

УТВЕРЖДАЮ
Руководитель ФКУ «ГБ МСЭ по
Республике Татарстан»

Минтруда России

Р.Х.Низамов

«03» 12 2013 г.



Политика информационной безопасности
Федерального казенного учреждения «Главное бюро
медико-социальной экспертизы по Республике Татарстан
(Татарстан)» Министерства труда и социальной защиты
Российской Федерации

1. Общие положения

1.1. Политика информационной безопасности Федерального казенного учреждения «Главное бюро медико-социальной экспертизы по Республике Татарстан (Татарстан)» Министерства труда и социальной защиты Российской Федерации (далее-Политика) разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов Министерства труда и социальной защиты Российской Федерации, ФГБУ «Федеральное бюро медико-социальной экспертизы», федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

1.2. Настоящая Политика является документом, доступным любому работнику Федерального казенного учреждения «Главное бюро медико-социальной экспертизы по Республике Татарстан (Татарстан)» Министерства труда и социальной защиты Российской Федерации (далее – Главное бюро) и пользователю его ресурсов, и представляет собой официально принятую руководством Главного бюро систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности.

1.3. Руководство Главного бюро осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства. Соблюдение требований информационной безопасности позволит обеспечить соответствие правовым, регулятивным требованиям и правилам оказания государственных услуг.

1.4. Требования информационной безопасности, которые предъявляются Главным бюро, соответствуют интересам (целям) деятельности Главного бюро и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.5. Стратегия Главного бюро в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности требований:

- российского законодательства в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных и других правовых актов;
- нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения физической безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности и приватности.

1.6. Необходимые требования обеспечения информационной безопасности Главного бюро должны неукоснительно соблюдаться работниками Главного бюро и другими сторонами как это определяется положениями внутренних нормативных документов Главного бюро.

1.7. Настоящая Политика обязательна для применения всеми работниками и руководством Главного бюро, а также пользователями его информационных ресурсов.

1.8. Положения настоящей Политики должны быть учтены при разработке политик информационной безопасности.

2. Список терминов и определений

2.1. **Информационная безопасность (ИБ)** - в настоящей Политике состояние защищенности технологических и процессов освидетельствования, объединяющих в своем составе работников Главного бюро, технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере.

2.2. **Информационная система Главного бюро** - совокупность программно-аппаратных комплексов Главного бюро.

2.3. **Инцидент информационной безопасности** - это появление одного или нескольких нежелательных рисков событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

2.4. **Модель угроз** - описательное представление свойств или характеристик угроз безопасности информации.

2.5. **Модель нарушителя** - описательное представление опыта, знаний, доступных ресурсов возможных нарушителей ИБ, необходимых им для реализации угрозы ИБ, и возможной мотивации действий.

2.6. Пользователь информационной системы - физическое лицо, обладающее возможностью доступа к информационной системе Главного бюро.

2.7. Угроза информационной безопасности - операционный риск, влияющий на нарушение одного (или нескольких) свойств информации - целостности, конфиденциальности, доступности объектов защиты.

3. Описание объекта защиты

Основными объектами защиты системы информационной безопасности в Главном бюро являются:

- информационные ресурсы, содержащие персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Главного бюро, независимо от формы и вида ее представления;
- информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы Главного бюро, независимо от формы и вида ее представления;
- работники Главного бюро, являющиеся разработчиками и пользователями информационных систем Главного бюро;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

4. Цели и задачи деятельности по обеспечению информационной безопасности

Целью деятельности по обеспечению информационной безопасности Главного бюро является снижение угроз информационной безопасности до приемлемого для Главного бюро уровня.

Основные задачи деятельности по обеспечению информационной безопасности Главного бюро:

- выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
- предотвращение инцидентов информационной безопасности;

- исключение либо минимизация выявленных угроз.

5. Угрозы информационной безопасности

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные).

5.1. Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т. п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

К антропогенным угрозам относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Главного бюро и контрольных органов, с действиями в руководстве и управлении, неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

5.2. Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

5.3. Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Источники угроз по отношению к инфраструктуре Главного бюро могут быть как внешними, так и внутренними.

6. Модель нарушителя информационной безопасности

По отношению к Главному бюро нарушители могут быть разделены на внешних и внутренних нарушителей.

6.1. Внутренние нарушители.

В качестве потенциальных внутренних нарушителей Главным бюро рассматриваются:

- зарегистрированные пользователи информационных систем Главного бюро;
- работники Главного бюро, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Банка, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства корпоративной информационной системы Главного бюро;
- руководители различных уровней.

6.2. Внешние нарушители.

В качестве потенциальных внешних нарушителей Главным бюро рассматриваются:

- бывшие работники Главного бюро;
- представители организаций, взаимодействующих по вопросам технического обеспечения Главного бюро;
- клиенты Главного бюро;
- посетители зданий и помещений Главного бюро;
- члены преступных организаций, работники спецслужб или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в корпоративную информационную систему Банка из внешних телекоммуникационных сетей (хакеры).

6.3. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

- нарушитель скрывает свои несанкционированные действия от других работников Банка;
- несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и

обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;

- внешний нарушитель может действовать в сговоре с внутренним нарушителем.

7. Основные положения по обеспечению информационной безопасности

7.1. Требования об обеспечении информационной безопасности Главного бюро обязательны к соблюдению всеми работниками Главного бюро и пользователями информационных систем.

7.2. Руководство Главного бюро приветствует и поощряет в установленном порядке деятельность работников Главного бюро и пользователей информационных систем по обеспечению информационной безопасности.

7.3. Неисполнение или некачественное исполнение работниками Главного бюро и пользователей информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в Главном бюро порядком либо требованиями действующего законодательства.

7.4. Стратегия Главного бюро в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Главного бюро, до специализированных мер информационной безопасности по каждому выявленному в Главном бюро риску, основанных на оценке рисков информационной безопасности.

7.5. С целью поддержки заданного уровня защищенности Главного бюро придерживается процессного подхода в построении системы менеджмента информационной безопасности. Система менеджмента

информационной безопасности Главного бюро основывается на осуществлении следующих основных процессов (планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование) и положениям международных стандартов по обеспечению информационной безопасности. На всех этапах жизненного цикла управление информационной безопасностью Главного бюро осуществляется с соблюдением нормативных документов.

7.6. При планировании мероприятий по обеспечению информационной безопасности в Главном бюро осуществляются:

7.6.1. Определение и распределение ролей персонала Главного бюро, связанного с обеспечением информационной безопасности (ролей информационной безопасности).

7.6.2. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.

7.6.3. Менеджмент рисков информационной безопасности, включающий:

- анализ влияния на информационную безопасность Главного бюро применяемых в деятельности Главного бюро технологий, а также внешних по отношению к Главному бюро событий;
- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
- определение моделей угроз информационной безопасности;
- выявление, анализ и оценка значимых для Главного бюро угроз информационной безопасности;
- выявление возможных негативных последствий для Главного бюро, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Главного бюро;
- идентификацию и анализ рисков событий информационной безопасности;
- оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для Главного бюро;
- обработку результатов оценки рисков информационной безопасности;

- оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Главного бюро в случае наступления рискованных событий;

- оценку затрат на реализацию защитных мер;
- рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;

- разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Главного бюро и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;

- документальное оформление целей и задач обеспечения информационной безопасности Главного бюро, поддержка в актуальном состоянии нормативно - методического обеспечения деятельности в сфере информационной безопасности.

7.7. В рамках реализации деятельности по обеспечению информационной безопасности в Главного бюро осуществляются:

7.7.1. Менеджмент инцидентов информационной безопасности, включающий:

- сбор информации о событиях информационной безопасности;
- выявление и анализ инцидентов информационной безопасности;

- расследование инцидентов информационной безопасности;

- оперативное реагирование на инцидент информационной безопасности;

- минимизация негативных последствий инцидентов информационной безопасности;

- оперативное доведение до руководства Главного бюро информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;

- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;

- контроль реализации и исполнения требований работниками Главного бюро действующих внутренних нормативных документов по обеспечению информационной безопасности Главного бюро;
- контроль деятельности работников и других пользователей информационных систем Главного бюро, направленный на выявление и предотвращение конфликтов интересов.

7.9. В целях совершенствования деятельности по обеспечению информационной безопасности в Главного бюро осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности

8. Организационная основа деятельности по обеспечению информационной безопасности

8.1. В целях выполнения задач по обеспечению информационной безопасности Главного бюро, в соответствии с рекомендациями международных и российских стандартов по безопасности в Главном бюро должны быть определены следующие роли:

- **Ответственное подразделение;**
- **Работник Главного бюро.**

При необходимости могут быть определены и другие роли по информационной безопасности.

8.2. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Главного бюро осуществляются и координируются **Ответственным подразделением**. Задачами **Ответственного подразделения** являются:

- установление потребностей Главного бюро в применении мер обеспечения информационной безопасности, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;
- соблюдение действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защите информации, нормативных актов по обеспечению информационной безопасности, приватности и неразглашению;
- разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Главного бюро, включая

планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;

- осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности Главного бюро;

- обучение, контроль и непосредственная работа с персоналом Главного бюро в области обеспечения информационной безопасности;

- планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объекты и системы в Главном бюро;

- выявление и предотвращение реализации угроз информационной безопасности;

- выявление и реагирование на инциденты информационной безопасности;

- прогнозирование и предупреждение инцидентов информационной безопасности;

- пресечение несанкционированных действий нарушителей информационной безопасности;

- поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение персонала;

- типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на структурные подразделения Главного бюро;

- обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;

- мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности;

- контроль обеспечения информационной безопасности, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;

- информирование руководства и руководителей его самостоятельных структурных подразделений об угрозах информационной безопасности, влияющих на деятельность.

8.3. **Ответственное подразделение** может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые работником **Ответственного подразделения**, и может, при наличии обоснованной необходимости по согласованию с руководителями соответствующих подразделений, привлекать для работы в них работников других самостоятельных структурных подразделений на основе совмещения работы в группе со своими основными должностными обязанностями.

8.4. Финансирование работ по реализации положений настоящей Политики осуществляется как в рамках целевого бюджета **Ответственного подразделения**, так и в рамках бюджетов бизнес - подразделений и подразделений ИТ-блока.

8.5. Основными задачами работников Главного бюро при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению информационной безопасности являются:

- соблюдение требований информационной безопасности, устанавливаемых нормативными документами;
- выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;
- выявление и реагирование на инциденты информационной безопасности;
- информирование в установленном порядке ответственных лиц о выявленных угрозах и рисковом событиях информационной безопасности;
- прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;
- мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;
- информирование своего руководства и **Ответственного подразделения** о выявленной угрозе в информационной среде Главного бюро.

9. Ответственность за соблюдение положений Политики

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение

изменений в процессы системы менеджмента информационной безопасности лежит на руководстве **Ответственного подразделения**.

Ответственность работников Главного бюро за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с работниками, а также положениями внутренних нормативных документов.

10. Контроль за соблюдением положений Политики

Текущий контроль соблюдения настоящей Политики осуществляет **Ответственное подразделение**. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

11. Заключительные положения

11.1. Требования настоящей Политики могут развиваться другим внутренними нормативными документами, которые дополняют и уточняют ее.

11.2. В случае изменения действующего законодательства и иных нормативных актов, а также Устава настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу. В этом случае **Ответственное подразделение** обязано незамедлительно инициировать внесение соответствующих изменений.

11.3. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

- периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 24 месяца;
- внеплановое внесение изменений в настоящую Политику может производиться 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.

11.4. Ответственным за внесение изменений в настоящую Политику является руководитель Главного бюро.

Ответственный	Начальник отдела информационно-статистического обеспечения		А.В.Лашуков
Исполнитель	Инженер-электроник		Д.И.Нафиков

Положение разработал:

Начальник отдела

информационно-статистического обеспечения

А. Лашуков