МИНИСТЕРСТВО ЮСТИЦИИ КИРОВСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

03.03.2016 № 15

г. Киров

Об утверждении политики информационной безопасности министерства юстиции Кировской области

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», пунктом 2 части 1 и частью 2 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»:

1. Утвердить политику информационной безопасности министерства юстиции Кировской области (далее - политика) (прилагается).

2. Назначить лицом, ответственным за организацию информационной безопасности министерства юстиции заместителя министра юстиции Игнатюк Юлию Владимировну.

3. Определить ответственным подразделением за информационную безопасность отдел по вопросам регистрации актов гражданского состояния, оказания государственных услуг министерства юстиции.

4. Отделу организационно-кадровой и аналитической работы министерства юстиции ознакомить с политикой сотрудников (работников) министерства и подведомственных учреждений.

5. Настоящее распоряжение подлежит опубликованию на официальном сайте министерства юстиции Кировской области.

Заместитель Председателя
Правительства области, министр
юстиции Кировской области Р.А. Береснев

ПОДГОТОВЛЕНО:

заместитель министра Ю.В. Игнатюк

СОГЛАСОВАНО:

заместитель министра В.Г. Жилин

начальник отдела по вопросам актов
гражданского состояния, оказания
государственных услуг В.Д. Токарев

ведущий консультант
государственно-правового
управления Ю.А. Сколова

Приложение

УТВЕРЖДЕНА

распоряжением министерства
юстиции Кировской области
от 03.03.2016 № 15

**Политика информационной безопасности
министерства юстиции Кировской области**

1. Общие положения.

1.1. Понятия и термины, применяемые в настоящей политике, используются в значениях, установленных:

Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 № Пр-1895;

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

ГОСТ 34.003-90. «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;

ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения»;

ГОСТ Р ИСО/МЭК 27000-2012 «Национальный стандарт. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

1.2. Политика информационной безопасности министерства юстиции Кировской области (далее – политика) разработана в соответствии с

законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов Российской Федерации и Кировской области, требованиями федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

1.3. Министерство юстиции Кировской области (далее – министерство) является исполнительным органом государственной власти Кировской области межотраслевой компетенции, проводящим государственную политику и осуществляющим управление в сферах правового обеспечения деятельности Губернатора Кировской области, Правительства Кировской области и администрации Правительства Кировской области, организационного обеспечения деятельности мировых судей Кировской области и аппаратов мировых судей, организации деятельности по государственной регистрации актов гражданского состояния, ведение регистра муниципальных нормативных правовых актов.

1.4. Настоящая политика является документом, доступным любому сотруднику министерства и пользователю его ресурсов, и представляет собой официально принятую министерством 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 министерства.

1.5. Министерство осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования деятельности органов исполнительной власти, а также развития реализуемых информационных технологий и ожиданий потребителей государственных услуг и других заинтересованных лиц.

1.6. Требования информационной безопасности, которые предъявляются министерством, соответствуют целям деятельности министерства и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.7. Политика министерства 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, служебной тайны и других правовых актов;

нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности;

государственных стандартов Российской Федерации по обеспечению информационной безопасности.

1.8. Требования обеспечения информационной безопасности министерства должны неукоснительно соблюдаться сотрудниками министерства и другими сторонами как это определяется положениями нормативных правовых актов министерства, а также требованиями договоров и соглашений, стороной которых является министерство.

1.9. Настоящая политика распространяется на деятельность министерства и обязательна для применения всеми сотрудниками (работниками) министерства, а также пользователями его информационных ресурсов.

1.10. Положения настоящей политики должны быть учтены при разработке политик информационной безопасности в подведомственных учреждениях.

2. Объекты защиты.

Основными объектами защиты системы информационной безопасности в министерстве являются:

информационные ресурсы, содержащие охраняемую нормативными актами Российской Федерации и Кировской области тайну, служебную тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы министерства, независимо от формы и вида ее представления;

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.

3. Цели и задачи деятельности по обеспечению информационной безопасности.

Целью деятельности по обеспечению информационной безопасности министерства является снижение угроз информационной безопасности до приемлемого уровня.

Основные задачи деятельности по обеспечению информационной безопасности министерства:

выявление, оценка и прогнозирование потенциальных угроз информационной безопасности;

принятие мер по предотвращению инцидентов информационной безопасности;

создание условий для исключения или минимизации выявленных угроз информационной безопасности.

4. Угрозы информационной безопасности

По методам воздействия на информацию угрозы подразделяются на естественные и искусственные.

К естественным угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия и другие явления, не зависящие от человека.

Искусственные угрозы состоят из угроз, возникающих вследствие непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях сотрудников, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

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

5. Модель нарушителя информационной безопасности.

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

5.1. Внутренние нарушители.

В качестве потенциальных внутренних нарушителей министерством рассматриваются:

зарегистрированные пользователи информационных систем министерства;

сотрудники министерства, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем министерства, но имеющие доступ в здания и помещения;

персонал, обслуживающий технические средства информационных систем министерства;

сотрудники структурных подразделений министерства, задействованные в разработке и сопровождении программного обеспечения;

сотрудники структурных подразделений, обеспечивающие безопасность министерства;

руководители различных уровней.

5.2. Внешние нарушители.

В качестве потенциальных внешних нарушителей министерством рассматриваются:

бывшие сотрудники министерства;

представители организаций, взаимодействующих с министерством по вопросам технического обеспечения министерства;

заявители, обратившиеся за предоставлением государственных услуг в министерство;

иные посетители зданий и помещений министерства;

иные лица, случайно или умышленно проникшие в информационную систему министерства из внешних телекоммуникационных сетей.

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

нарушитель скрывает свои несанкционированные действия от других сотрудников министерства;

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, финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей.

6. Основные принципы информационной безопасности.

6.1. При построении системы информационной безопасности министерство руководствуется следующими основными принципами:

6.1.1. Законность (осуществление защитных мероприятий и разработки системы информационной министерства в соответствии с законодательством в области защиты информации).

6.1.2. Системность (учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности).

6.1.3. Комплексность (согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов).

6.1.4. Непрерывность (постоянная работа и организационная поддержка мер и средств защиты для эффективного обеспечения информационной безопасности).

6.1.5. Своевременность (постановка задач по комплексной защите информации и реализация мер обеспечения информационной безопасности на ранних стадиях разработки информационных систем в целом и их систем защиты информации в частности).

6.1.6. Преемственность и непрерывность совершенствования (совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и систем их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите).

6.1.7. Разумная достаточность (выбор достаточного уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми);

6.1.8. Персональная ответственность (ответственность за обеспечение информационной безопасности для каждого сотрудника в пределах его полномочий).

6.1.9. Минимизация полномочий (предоставление пользователям информационных систем министерства минимальных прав в соответствии с должностными регламентами, инструкциями сотрудников министерства).

6.1.10 Исключение конфликта интересов (четкое разделение обязанностей сотрудников министерства и исключение ситуаций, когда сфера ответственности допускает конфликт интересов).

6.1.11. Взаимодействие и сотрудничество (сотрудники министерства должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделения, ответственного за информационную безопасность).

6.1.12 Гибкость системы защиты (способность реагировать на изменения внешней среды и условий осуществления министерством своих функций).

6.1.13 Простота применения средств защиты (применение не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при работе пользователей информационных систем, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций).

6.1.14 Обоснованность и техническая реализуемость (реализация на современном уровне развития науки и техники, обоснованность с точки зрения достижения заданного уровня безопасности информации, а также соответствие установленным нормам и требованиям по безопасности информации).

6.1.15 Специализация и профессионализм (реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными сотрудниками).

6.1.16 Обязательность контроля (обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности на основе используемых систем и

средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств).

7. Основные положения по обеспечению информационной безопасности.

7.1. Требования об обеспечении информационной безопасности министерства обязательны к соблюдению всеми сотрудниками министерства и пользователями информационных систем.

7.2. Неисполнение или некачественное исполнение сотрудниками министерства и пользователей информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным мер административного воздействия, степень которых определяется действующим законодательством.

7.3. Политика министерства в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне лица, ответственного за защиту информации в министерстве, до специализированных мер информационной безопасности по каждому выявленному в министерстве риску, основанных на оценке рисков информационной безопасности.

7.4. С целью поддержки заданного уровня защищенности министерство придерживается процессного подхода в построении системы менеджмента информационной безопасности.

Система менеджмента информационной безопасности министерства основывается на осуществлении следующих основных процессов (планирование, реализация и эксплуатация защитных мер, проверка, совершенствование) соответствующих требованиям нормативных актов в области защиты информации.

7.5. При планировании мероприятий по обеспечению информационной безопасности в министерстве осуществляются:

7.5.1. Определение и распределение ролей сотрудников министерства, связанных с обеспечением информационной безопасности (ролей информационной безопасности).

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

7.5.3. Менеджмент рисков информационной безопасности, включающий:

анализ влияния на информационную безопасность министерства применяемых в деятельности министерства технологий, а также внешних по отношению к министерству 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 министерства угроз информационной безопасности;

выявление возможных негативных последствий, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных систем министерства;

идентификацию и анализ возможности деструктивных событий информационной безопасности;

оценку возможной величины угроз информационной безопасности и определение среди них угроз, неприемлемых для министерства;

обработку результатов оценки угроз информационной безопасности;

минимизацию возможности последствий угроз информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для информации министерства в случае наступления угроз;

оценку влияния защитных мер на цели основной деятельности министерства;

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 министерства и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;

документальное оформление целей и задач обеспечения информационной безопасности министерства, поддержка в актуальном состоянии нормативно – методического обеспечения деятельности в сфере информационной безопасности.

7.6. В рамках реализации деятельности по обеспечению информационной безопасности в министерстве осуществляются:

7.6.1. 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 лица, ответственного за организацию информационной безопасности министерства, 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;

пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;

повышение уровня знаний сотрудников министерства в вопросах обеспечения информационной безопасности;

обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем министерства и информации, обрабатываемой в них;

применение средств криптографической защиты информации;

обеспечение бесперебойной работы автоматизированных систем и сетей связи;

обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;

применение средств защиты от вредоносных программ;

обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем министерства, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);

обеспечение информационной безопасности при использовании доступа в сеть Интернет;

контроль доступа в здания и помещения министерства.

7.6.2. Обеспечение защиты информации от утечки по техническим каналам, включающее:

применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита;

применение мер и технических средств, создающих помехи при несанкционированном получении информации - активная защита;

применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

7.7. В целях проверки деятельности по обеспечению информационной безопасности в министерстве осуществляются:

контроль правильности реализации и эксплуатации защитных мер;

контроль изменений конфигурации информационных систем и подсистем министерства;

мониторинг факторов рисков и соответствующий их пересмотр;

контроль реализации и исполнения требований сотрудниками министерства действующих внутренних нормативных документов по обеспечению информационной безопасности министерства;

контроль деятельности сотрудников и других пользователей информационных систем министерства, направленный на выявление и предотвращение конфликтов интересов.

7.8. В целях совершенствования деятельности по обеспечению информационной безопасности в министерстве 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 министерства, в министерстве определены следующие роли:

лицо, ответственное за организацию защиты информации;

ответственное подразделение;

сотрудник (работник) министерства.

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

8.2. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности министерства осуществляются и

координируются ответственным подразделением. Задачами ответственного подразделения являются:

8.2.1. Установление потребностей министерства в применении мер обеспечения информационной безопасности, определяемых как внутренними требованиями, так и требованиями нормативных актов.

8.2.2. Соблюдение действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации, государственных стандартов России по обеспечению информационной безопасности, нормативных актов по обеспечению информационной безопасности, принятых федеральными органами, контролирующими деятельность министерства, нормативных актов Кировской области в области безопасности информации.

8.2.3. Разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности министерства, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов.

8.2.4. Осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности министерства.

8.2.5. Обучение, контроль и непосредственная работа с сотрудниками министерства в области обеспечения информационной безопасности.

8.2.6. Планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объекты и системы в министерстве.

8.2.7. Выявление и предотвращение реализации угроз информационной безопасности.

8.2.8. Выявление и реагирование на инциденты информационной безопасности.

8.2.9. Информирование в установленном порядке ответственных лиц об угрозах и событиях информационной безопасности.

8.2.10. Прогнозирование и предупреждение инцидентов информационной безопасности.

8.2.11. Пресечение несанкционированных действий нарушителей информационной безопасности.

8.2.12. Поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение сотрудников.

8.2.13. Типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на подведомственные учреждения.

8.2.14. Обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности.

8.2.15. Мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности министерства.

8.2.16. Контроль обеспечения информационной безопасности министерства, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности.

8.2.17. Информирование лица, ответственного за организацию информационной безопасности министерства и руководителей подведомственных учреждений министерства об угрозах информационной безопасности, влияющих на деятельность министерства.

8.3. Ответственное подразделение может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые сотрудником ответственного подразделения, и может, при наличии обоснованной необходимости по согласованию с руководителями соответствующих подразделений, привлекать для работы в них сотрудников

других самостоятельных структурных подразделений министерства на основе совмещения работы в группе со своими основными должностными обязанностями.

8.5. Основными функциями лица, ответственного за организацию защиты информации являются:

назначение ответственных лиц в области информационной безопасности,

координация и внедрение информационной безопасности в министерстве.

8.6. Основными задачами сотрудников министерства, при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению информационной безопасности министерства являются:

соблюдение требований информационной безопасности, устанавливаемых нормативными документами министерства;

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 возможности наступления угроз 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 министерства.

9. Ответственность за соблюдение положений политики.

Общее руководство обеспечением информационной безопасности министерства осуществляет лицо, ответственное за организацию защиты информации.

Ответственность за поддержание положений настоящей политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности министерства лежит на руководстве ответственного подразделения.

Ответственность сотрудников министерства за невыполнение настоящей политики определяется соответствующими положениями, включаемыми в служебные регламенты и иные трудовые соглашения с сотрудниками министерства, а также положениями внутренних нормативных документов министерства.

10. Контроль за соблюдением положений политики

Общий контроль состояния информационной безопасности министерства осуществляется лицом, ответственным за организацию информационной безопасности.

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