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.