Приложение № 1 к распоряжению

министерства управления финансами

Самарской области

от «03» сентября 2018 № 01-08/30

# Политика информационной безопасности министерства управления финансами Самарской области

## 1. Общие положения

1.1. Политика информационной безопасности министерства управления финансами Самарской области (далее - ПИБ) разработана в соответствии с нормами действующего законодательства Российской Федерации в области обеспечения информационной безопасности и учитывает требования нормативных документов Министерства финансов Российской Федерации, Федерального казначейства, Центрального Банка Российской Федерации, Федеральной службы безопасности Российской Федерации (ФСБ России), Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

ПИБ разработана в целях соблюдения норм следующих нормативных правовых актов:

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
5. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
6. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
7. Указ Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»;
8. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»;
9. Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
10. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
11. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
12. Распоряжение Правительства РФ от 17.07.2006 № 1024-р «О концепции региональной информатизации до 2010 года»;
13. Распоряжение Правительства Российской Федерации от 20.07.2011 № 1275-р «О Концепции создания и развития государственной интегрированной информационной системы управления общественными финансами «Электронный бюджет»;
14. Решение Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;
15. Приказ Федеральной службы по техническому и экспортному контролю России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
16. Методические рекомендации «Меры защиты информации в государственных информационных системах», утвержденные приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 11.02.2014;
17. Приказ Федеральной службы безопасности России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
18. Приказ Федеральной службы безопасности России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
19. Приказ Федеральной службы охраны Российской Федерации от 07.08.2009 № 487 «Об утверждении Положения о сегменте информационно-телекоммуникационной сети «Интернет» для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации»;
20. Приказ Федеральной службы по техническому и экспортному контролю России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
21. Приказ Минкомсвязи России от 25.08.2009 № 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»;
22. Приказ Федеральной службы безопасности России и Федеральной службы по техническому и экспортному контролю России № 416/489 от 31.08.2010 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

1.2. ПИБ является общедоступным документом, который отражает цели, задачи, принципы и основные направления обеспечения информационной безопасности в министерстве управления финансами Самарской области (далее - министерство).

1.3. Действие настоящей ПИБ распространяется на деятельность всех сотрудников министерства.

1.4. Действие настоящей ПИБ не распространяется на информационные ресурсы и иные виды информации, содержащей сведения, составляющие государственную тайну.

## 2. Цели, задачи и принцип обеспечения информационной безопасности в министерстве

2.1. Цель обеспечения информационной безопасности в министерстве – защита информационных ресурсов от возможного несанкционированного доступа к ним, которое может привести к нанесению ущерба министерству и его сотрудникам, государственным органам и учреждениям Самарской области, а также ограничить возможность выполнения министерством своих полномочий.

2.2. Для достижения поставленной цели в министерстве решаются следующие задачи:

анализ и оценка актуальных угроз и нарушителей информационной безопасности;

оценка рисков информационной безопасности;

внедрение организационных, программно-аппаратных и технических мер защиты информации;

создание условий для оперативного реагирования на угрозы информационной безопасности.

2.3. Принципы обеспечения информационной безопасности в министерстве:

законность;

процессный подход;

непрерывность функционирования;

персональная ответственность.

2.4. Законность функционирования системы обеспечения информационной безопасности в министерстве достигается путем соответствия внедряемых защитных мер требованиям:

действующего законодательства РФ в сфере информационной безопасности и стандартов безопасности;

действующего бюджетного законодательства РФ;

законодательства РФ в области обработки персональных данных и нормативных документов ФСБ России и ФСТЭК России, регламентирующих вопросы обеспечения безопасности персональных данных при их обработке в информационных системах министерства.

2.5. Процессный подход к обеспечению информационной безопасности достигается путем построения системы обеспечения информационной безопасности с учетом результатов анализа всех рабочих процессов, функционирующих в министерстве.

2.6. Непрерывность функционирования системы обеспечения информационной безопасности достигается министерством путем применения циклической модели Деминга (ГОСТ Р ИСО/МЭК 27001-2006) к процессу обеспечения информационной безопасности «….планирование – осуществление – проверка – действие….».

2.7. Персональная ответственность достигается путем установления ответственности каждого сотрудника министерства, участвующего в процессе обеспечения информационной безопасности.

## 3. Общие сведения об информационных ресурсах, подлежащих защите в министерстве

3.1. К категории информационных ресурсов министерства, информационную безопасность которых необходимо обеспечивать, рассматриваются следующие типы ресурсов:

информационные ресурсы – информация ограниченного доступа и распространения; информация, содержащая сведения, относящиеся к персональным данным субъектов персональных данных; информация о расположении каналов передачи данных на основе волоконно-оптических линий связи, информация об инфраструктуре компьютерной сети министерства, общедоступная информация, включая общедоступную информацию ограниченного распространения, а так же информация, определяющая параметры конфигурирования и эксплуатации средств защиты информации, независимо от формы представления такой информации;

программные ресурсы – прикладное и системное программное обеспечение, а также среда разработки прикладного программного обеспечения;

физические ресурсы – автоматизированные рабочие места (персональные компьютеры, серверы), коммуникационное оборудование (маршрутизаторы, коммутаторы, модемы), периферийная техника (принтеры, сканеры) и иная организационная техника.

## 4. Модель угроз и нарушителей информационной безопасности

4.1. В качестве возможных угроз нарушения информационной безопасности в министерстве рассматриваются три основных класса угроз:

угрозы нарушения конфиденциальности информации;

угрозы нарушения целостности информации;

 угрозы нарушения доступности информации.

4.2. Каждая угроза информационной безопасности расписывается и анализируется следующим образом: «источник угрозы информационной безопасности» - «способ несанкционированного доступа к ресурсу» - «несанкционированные действия с ресурсом» - «уровень реализации угрозы информационной безопасности» - «нарушение характеристики безопасности ресурса».

4.3. В качестве одного из основных источников угроз информационной безопасности в министерстве рассматриваются лица, которые могут получить несанкционированный доступ к ресурсам министерства (нарушители информационной безопасности).

4.4. С учетом разделения нарушителей информационной безопасности на внешних, внутренних и комбинированных в качестве возможных потенциальных нарушителей информационной безопасности могут выступать:

4.4.1. Внешние нарушители информационной безопасности:

сотрудники государственных и муниципальных органов, учреждений или иные физические лица, прибывающие в министерство в качестве посетителей;

лица, случайно или намеренно, получившие доступ к информационным ресурсам министерства через внешние телекоммуникационные каналы связи;

программисты-разработчики программных компонент информационных систем, не являющиеся сотрудниками министерства;

сотрудники компаний, обеспечивающих поставку, настройку и ремонт компьютерной техники;

сотрудники компаний, обеспечивающих обслуживание компьютерной сети министерства или обслуживание средств защиты информации в министерстве;

сотрудники спецслужб и представители силовых ведомств, имеющие возможность применять специальные средства и способы атак на информационные ресурсы министерства;

4.4.2. Внутренние нарушители информационной безопасности:

сотрудники министерства, имеющие санкционированный доступ к ресурсам информационных систем министерства;

сотрудники министерства, осуществляющие доступ к информационным ресурсам с использованием технологии удаленного доступа;

сотрудники министерства, имеющие полномочия администратора базы (баз) данных, системного администратора или администратора информационной безопасности.

4.4.3. Комбинированные нарушители информационной безопасности – внешние и внутренние нарушители информационной безопасности, действующие в сговоре.

4.5. В зависимости от цели, квалификации, технического оснащения и прав доступа к информационным системам министерства нарушители информационной безопасности могут реализовывать атаки на уровне сетевого оборудования, операционных систем, систем управления базами данных, сетевых приложений и сервисов, приложений и сервисов министерства, используя следующие способы несанкционированного доступа:

внедрение вредоносного программного обеспечения;

кража носителей информационных ресурсов;

кража технических средств обработки информационных ресурсов;

несанкционированное повышение привилегий сотрудника министерства в информационной системе;

несанкционированные действия сотрудников министерства в информационной системе;

физическое подключение к каналу связи с целью перехвата информации;

внесение недекларированных возможностей и/или программных закладок;

внедрение ложных сетевых сервисов;

подмена доверенного объекта;

навязывание ложного сетевого маршрута;

удаленный запуск приложений и т.д.

4.6. Все способы несанкционированного доступа к информационным ресурсам могут быть направлены на преднамеренное или случайное копирование, модификацию, удаление, передачу по каналам связи и/или передачу на материальных носителях, с целью нарушения конфиденциальности, целостности и/или доступности ресурса.

4.7. Детальная модель угроз и нарушителей информационной безопасности для информационных систем министерства регламентируется отдельными внутренними документами министерства.

## 5. Процесс обеспечения информационной безопасности

5.1. Построение системы обеспечения информационной безопасности (далее по тексту - СОИБ) с использованием модели Деминга заключается в цикличном выполнении следующей группы процессов:

планирование СОИБ;

реализация СОИБ;

проверка СОИБ;

совершенствование СОИБ.

5.2. На этапе планирования СОИБ в министерстве осуществляется:

5.2.1. Анализ требований законодательства РФ и нормативных правовых документов РФ в области обеспечения информационной безопасности.

5.2.2. Определение и распределение ролей сотрудников министерства в области обеспечения информационной безопасности.

5.2.3. Анализ и оценка рисков информационной безопасности:

идентификация информационных, программных и физических ресурсов министерства;

определение потенциальных нарушителей информационной безопасности для министерства (модель нарушителя);

определение значимых для министерства угроз информационной безопасности (модель угроз информационной безопасности);

оценка вероятности возникновения угроз информационной безопасности;

оценка степени влияния угроз информационной безопасности на деятельность министерства;

оценка рисков нарушения информационной безопасности в министерстве;

рассмотрение различных вариантов применения средств защиты информации, в целях минимизации выявленных рисков информационной безопасности;

оценка затрат на реализацию средств защиты.

5.2.4. Формирование требований к СОИБ по следующим направлениям:

комплексная антивирусная защита информационных систем министерства;

обработка персональных данных и информации ограниченного распространения;

управление сетями министерства;

управление логическим доступом к ресурсам министерства;

управление средствами криптографической защиты и их ключевыми системами;

использование сотрудниками министерства сети Интернет и корпоративной электронной почты;

парольная политика;

межсетевое взаимодействие информационных систем министерства;

управление физическим доступом сотрудников в помещения министерства;

аудит событий информационной безопасности.

5.2.5. Определение и закрепление ответственности сотрудников министерства, принимающих участие в процессе обеспечения информационной безопасности.

5.3. На этапе реализации СОИБ в министерстве осуществляется:

5.3.1. Внедрение внутренних распорядительных документов, регламентирующих требования к системе обеспечения информационной безопасности в технологических процессах министерства по направлениям, указанным в п.5.2.4 настоящей ПИБ:

положение о защищенной сети передачи данных министерства;

положение об обеспечении информационной безопасности при использовании информационно-телекоммуникационной сети Интернет в министерстве;

положение о порядке обработки персональных данных в информационных системах персональных данных министерства и т.д.

5.3.2. Внедрение и конфигурирование программных, программно-аппаратных и технических средств защиты информации.

5.3.3. Внедрение процедур управления инцидентами информационной безопасности.

5.3.4. Повышение осведомленности сотрудников министерства в вопросах обеспечения информационной безопасности.

5.3.5. Обеспечение непрерывности функционирования информационных систем министерства и возможности восстановления их после сбоя.

5.4. На этапе проверки СОИБ в министерстве осуществляется:

5.4.1. Контроль корректности и бесперебойности функционирования программных, программно-аппаратных и технических средств защиты информации;

5.4.2. Контроль исполнения сотрудниками министерства внутренних документов министерства, регламентирующих вопросы обеспечения информационной безопасности.

5.4.3. Проведение оценки соответствия системы обеспечения информационной безопасности требованиям к защите информационных ресурсов министерства, установленных законодательством РФ, нормативными документами Министерства финансов РФ, Федерального казначейства, Центрального Банка Российской Федерации, ФСБ России, ФСТЭК России.

5.5. На этапе совершенствования СОИБ в министерстве осуществляется:

анализ результатов проверки СОИБ;

внесение оперативных изменений в состав и конфигурацию средств защиты информации;

внесение изменений в документы, регламентирующие деятельность по обеспечению информационной безопасности;

разработка планов по тактическим улучшениям СОИБ.

## 6. Организационная составляющая процесса обеспечения информационной безопасности

6.1. Для достижения цели обеспечения информационной безопасности в министерстве выделены следующие ответственные лица:

Куратор – руководитель управления автоматизации бюджетного процесса министерства;

Уполномоченные сотрудники управления автоматизации бюджетного процесса министерства в части обеспечения выполнения работ по информационной безопасности;

Ответственные сотрудники территориальных отделов министерства;

Сотрудники министерства.

6.2. К основным задачам, решаемым Куратором, относятся:

координация работ по построению системы обеспечения информационной безопасности;

согласование внутренних документов в сфере обеспечения информационной безопасности министерства.

6.3. К основным задачам, решаемым Уполномоченными сотрудниками управления автоматизации бюджетного процесса министерства в части обеспечения выполнения работ по информационной безопасности, относятся:

организация и выполнение работ по соблюдению требований законодательства Российской Федерации в области обеспечения информационной безопасности, нормативных документов Министерства финансов РФ, Федерального казначейства России, Центрального Банка Российской Федерации, ФСБ России, ФСТЭК России;

анализ и оценка рисков нарушения информационной безопасности, в разрезе технологических процессов министерства;

выработка требований и механизмов защиты данных, используемых в технологических процессах министерства;

определение состава внутренних документов министерства, регламентирующих деятельность по обеспечению информационной безопасности, а также внесение в них изменений и/или дополнений;

работа с сотрудниками министерства, в части повышения их уровня осведомленности в вопросах обеспечения информационной безопасности;

выявление и реагирование на инциденты информационной безопасности;

мониторинг, контроль и оценка эффективности принятых мер по обеспечению информационной безопасности и применяемых средств защиты информации.

6.4. Уполномоченные сотрудники управления автоматизации бюджетного процесса министерства в части обеспечения выполнения работ по информационной безопасности утверждаются распоряжением министерства.

6.5. К основным задачам, решаемым ответственными сотрудниками территориальных отделов министерства, относятся:

организация работ по выполнению требований внутренних документов министерства, в области обеспечения информационной безопасности;

регистрация и информирование, в установленном порядке, об инцидентах информационной безопасности.

6.6. Ответственные сотрудники территориальных отделов министерства утверждаются распоряжением министерства.

6.7. К основным задачам, решаемым сотрудниками министерства, в рамках выполнения требований по информационной безопасности относятся:

соблюдение требований законодательства и внутренних документов министерства по информационной безопасности;

выявление и информирование, в установленном порядке, об инцидентах информационной безопасности на своем участке работ.

## 7. Контроль и ответственность

7.1. Общее руководством процессом обеспечения информационной безопасности осуществляет министр управления финансами Самарской области.

7.2. Сотрудники министерства несут ответственность за несоблюдение требований настоящей ПИБ.

7.3. Ответственность за поддержание ПИБ в актуальном состоянии несет руководитель управления автоматизации бюджетного процесса.

7.4. Контроль за выполнением требований ПИБ осуществляется:

сотрудниками управления автоматизации бюджетного процесса, уполномоченными на выполнение работ по информационной безопасности - постоянно, в рамках мероприятий по мониторингу и контролю защитных мер, а так же в рамках проведения внутренних проверок, оценки соответствия требований законодательства Российской Федерации в области обеспечения информационной безопасности, нормативных документов Министерства финансов РФ, Федерального казначейства России, Центрального Банка РФ, ФСБ России, ФСТЭК России и стандартов безопасности;

ответственными сотрудниками территориальных отделов министерства - постоянно, в рамках мероприятий по соблюдению процедур обеспечения информационной безопасности территориальных отделов министерства.

##

## 8. Заключительные положения

8.1. Требования настоящей ПИБ могут дополняться и уточняться другими внутренними документами министерства.

8.2. В случае изменения действующего законодательства и иных нормативных актов, а также Положения о министерстве управления финансами Самарской области, утвержденным Постановлением Правительства Самарской области от 21.11.2008 № 447 (далее – Положение о министерстве) настоящая ПИБ и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным правовым актам, а также Положению о министерстве. В этом случае управление автоматизации бюджетного процессаобязано незамедлительно инициировать внесение соответствующих изменений в ПИБ.

8.3. Внесение изменений в действующую ПИБ осуществляется на внеплановой основе. Внеплановое внесение изменений в действующую ПИБ 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.