Некоммерческая организация
«Фонд развития городов»
(Фонд развития городов)
101000, Москва, Архангельский пер. 1/1/9, стр. 1А
ОГРН 1117799027422 ИНН/КПП: 7701168050/770101001

ПРИКАЗ

«06» марта 2020 года № 3-УП

Об утверждении и введении в действие
«Концепции информационной безопасности»
Некоммерческой организации «Фонд развития городов»

В соответствии с решением Комитета по безопасности Группы ВЭБ.РФ (протокол № 1 от 05 декабря 2019 года)

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с 06.03.2020 года «Концепцию информационной безопасности» некоммерческой организации «Фонд развития городов» (Приложение №1 к настоящему Приказу).
2. Утвердить и ввести в действие с 06.03.2020 года «Политику информационной безопасности» некоммерческой организации «Фонд развития городов» (Приложение №2 к настоящему Приказу).
3. Контроль за исполнением настоящего Приказа оставляю за собой.

Генеральный директор А.Л. Сорокин

Приложение №1 к
Приказу генерального директора
от 06 марта 2020 года № 3-УП

Концепция
информационной безопасности
некоммерческой организации «Фонд развития городов»

ОГЛАВЛЕНИЕ

1. Общие положения

1.1. Концепция информационной безопасности некоммерческой организации «Фонд развития городов» (далее – Концепция, Фонд) разработана в целях обеспечения реализации Стратегии Фонда (далее – Стратегия).

1.2. Деятельность по обеспечению информационной безопасности представляет собой взаимосвязанную совокупность процессов прогнозирования, выявления, предупреждения и пресечения внешних и внутренних угроз информационной безопасности, локализации и нейтрализации последствий их проявления.

1.3. Концепция представляет собой систему официальных взглядов на обеспечение безопасности Фонда в информационной сфере с учетом современных тенденций развития цифровой экономики, а также, методов защиты информации, информационной инфраструктуры.

В Концепции под информационной сферой понимается совокупность информации, информационной инфраструктуры, в том числе сайта Фонда в сети Интернет, работников Фонда, деятельность которых связана с формированием и обработкой информации, развитием и использованием информационных технологий, обеспечением информационной безопасности Фонда, а также совокупность механизмов регулирования соответствующих общественных отношений.

1.4. В Концепции на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели, задачи и основные направления обеспечения информационной безопасности с учетом стратегических приоритетов Фонда.

1.5. Концепция разработана на основе Концепции информационной безопасности государственной корпорации «Банк развития и внешнеэкономической деятельности (Внешэкономбанк)», Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646, Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274), руководящих документов ФСТЭК России и ФСБ России, а также с учетом иных документов в указанной сфере.

1.6. Настоящая Концепция является основой для совершенствования политики информационной безопасности Фонда, а также для выработки мер по развитию и совершенствованию системы обеспечения информационной безопасности.

1.7. Концепция призвана консолидировать усилия органов управления, коллегиальных рабочих органов, а также структурных подразделений Фонда во

взаимодействии с правоохранительными органами и иными органами государственной власти Российской Федерации, другими организациями по созданию благоприятных внутренних и внешних условий для обеспечения информационной безопасности Фонда.

2. Термины и определения

В настоящей Концепции используются следующие термины и определения:

- **интересы Фонда в информационной сфере** (далее – интересы в информационной сфере) – объективно значимые потребности Фонда в обеспечении их защищенности и долгосрочного устойчивого развития в части, касающейся информационной сферы;

- **угроза информационной безопасности Фонда** (далее – информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба интересам Фонда в информационной сфере;

- **инцидент информационной безопасности** – реализация угрозы информационной безопасности, наносящая ущерб и/или вызывающая любые другие непредвиденные или негативные для Фонда последствия;

- **информационная безопасность Фонда** (далее – информационная безопасность) – состояние защищенности Фонда от внутренних и внешних информационных угроз, при котором обеспечивается стабильное функционирование и долгосрочное устойчивое развитие Фонда;

- **обеспечение информационной безопасности Фонда** (далее – обеспечение информационной безопасности) – осуществление Фондом взаимоувязанных правовых, организационных, технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, предупреждению, обнаружению, предотвращению, отражению угроз информационной безопасности, локализации и ликвидации последствий их проявления;

- **силы обеспечения информационной безопасности Фонда** (далее – силы обеспечения информационной безопасности) – органы управления, коллегиальные рабочие органы, самостоятельные структурные подразделения и должностные лица Фонда, уполномоченные на решение задач по обеспечению информационной безопасности в соответствии с законодательством Российской Федерации и внутренними нормативными документами Фонда;

- **средства обеспечения информационной безопасности Фонда** (далее – средства обеспечения информационной безопасности) – правовые, организационные, технические, информационно-аналитические и другие средства, используемые силами обеспечения информационной безопасности;

- **система обеспечения информационной безопасности Фонда** (далее – система

обеспечения информационной безопасности) – совокупность сил обеспечения информационной безопасности, осуществляющих целенаправленную, скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

- **информационная инфраструктура Фонда** (далее – информационная инфраструктура) – совокупность объектов информатизации, информационных систем и сетей связи, расположенных на территории Фонда, в том числе систем обработки и анализа информации, технических и программных средств ее обработки, передачи, хранения и отображения, каналов информационного обмена и телекоммуникации, систем и средств защиты информации, объектов и помещений, в которых размещены такие системы, а также сайт Фонда в сети Интернет;

- **информация** – сведения (сообщения, данные) независимо от формы их представления;

- **информационные ресурсы Фонда** (далее – информационные ресурсы) – отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах Фонда (библиотеках, архивах, фондах, банках данных, информационных системах других видов);

- **объекты информационной безопасности** – все то, что защищается от информационных угроз.

Основными объектами обеспечения информационной безопасности Фонда являются:

1) работники Фонда;

2) финансовые, информационные, материально-технические и иные ресурсы;

3) информация ограниченного доступа и распространения, в том числе содержащая сведения, составляющие коммерческую и иную охраняемую законом тайну;

4) деловая репутация Фонда;

5) информационная инфраструктура, в том числе программно-аппаратные средства, информационные и телекоммуникационные системы, служебные помещения, а также сайт Фонда;

6) бизнес-процессы и системы управления (стратегического, корпоративного управления, управления безопасностью, рисками, персоналом и др.) Фонда;

7) производственные, социальные и другие отношения в информационной сфере, регулируемые международными договорами Российской Федерации, законодательством Российской Федерации, договорными, контрактными и внутренними нормативными документами Фонда.

3. Основные интересы Фонда в информационной сфере

3.1. Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности Фонда. Их эффективное применение является фактором реализации Стратегии.

Информационная сфера играет важную роль в обеспечении реализации стратегических приоритетов Фонда.

3.2. Основными интересами Фонда в информационной сфере являются:

1) создание благоприятных условий для реализации Указа Президента РФ от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»;

2) обеспечение результативного и эффективного участия Фонда в разработке национальных проектов (программ), планов мероприятий по их реализации, комплексного плана модернизации и расширения городской инфраструктуры;

3) соблюдение и защита прав и свобод работников Фонда в части, касающейся получения и использования информации;

4) обеспечение результативной и эффективной реализации Стратегии;

5) обеспечение информационной поддержки деятельности Фонда, механизмов взаимодействия с внешними и внутренними клиентами, с гражданским обществом;

6) применение информационных технологий в интересах сохранения, принятых и разделяемых работниками Фонда ценностей;

7) обеспечение информационной безопасности Фонда;

8) формирование и развитие системы информационной безопасности Фонда;

9) обеспечение защиты информации, содержащей сведения, составляющие коммерческую и иную охраняемую законом тайну, иной информации ограниченного доступа и распространения;

10) реализация системы мер по профилактике коррупционных и иных правонарушений в Фонде;

11) обеспечение деятельности Фонда по соблюдению работниками Фонда ограничений, запретов, обязанностей и требований к служебному поведению;

12) формирование и поддержание культуры информационной безопасности в Фонде;

13) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры Фонда;

14) обеспечение необходимого и достаточного уровня защищенности бизнес-процессов Фонда, в том числе в ходе их развития и совершенствования;

15) развитие в Фонде информационных технологий, информационной инфраструктуры, а также совершенствование деятельности сил обеспечения информационной

безопасности, в том числе по эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

3.3. Реализация интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам деструктивного воздействия на работников Фонда, на информационные ресурсы и информационную инфраструктуру в целях обеспечения стабильного функционирования и долгосрочного устойчивого развития Фонда.

4. Состояние информационной безопасности Фонда

4.1. Расширение областей применения информационных технологий, являясь фактором совершенствования функционирования и развития Фонда, одновременно порождает новые информационные угрозы.

Масштабное внедрение информационно-коммуникационных технологий и систем в органы государственной власти, в финансовые и иные организации приводит к возникновению новых форм коррупции.

Обострение конкуренции между системными интеграторами приводит в ряде случаев к росту коррупционных схем закупок информационно-коммуникационных технологий и систем.

4.2. Состояние информационной безопасности Фонда характеризуется:

- нарастанием угроз применения информационных технологий в целях нанесения ущерба Российской Федерации, в том числе финансовым и иным организациям;

- попытками подрыва деловой репутации и дискредитации деятельности российских организаций, ужесточением антироссийских санкций, обострением информационного противоборства;

- постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты информационной инфраструктуры;

- необходимостью дальнейшего повышения уровня использования конкурентоспособных информационных технологий, в том числе в области обеспечения информационной безопасности, для повышения результативности и эффективности деятельности Фонда;

- высоким уровнем зависимости информационной безопасности Фонда от зарубежных информационных технологий и программного обеспечения, вычислительной техники и средств связи, в том числе в области обеспечения информационной безопасности;

- необходимостью дальнейшего повышения уровня комплексного обеспечения безопасности информационных ресурсов и информационной инфраструктуры с использованием отечественных информационных технологий и отечественной продукции;

- наличием коррупционных проявлений со стороны внешних и внутренних клиентов

Фонда.

4.3. В Фонде планируется проводится регулярная (2 раза в год) оценка состояния информационной безопасности, оценка риска нарушения информационной безопасности и принимаемых мер, необходимых для управления этим риском.

Адекватный уровень защищенности информационных ресурсов и информационной инфраструктуры достигается обеспечением совокупности свойств информационной безопасности (конфиденциальность, целостность, доступность информационных ресурсов и информационной инфраструктуры в рамках установленных полномочий работников Фонда) в соответствии с законодательством Российской Федерации и внутренними нормативными документами.

Однако имеются и проблемы системного характера, требующие решения на всех уровнях управления информационной безопасностью, направленные:

- на снижение числа нарушений со стороны работников Фонда требований антикоррупционного законодательства, обеспечения информационной безопасности, в том числе в части сохранения конфиденциальности информации;

- на повышение уровня готовности Фонда к работе в условиях обострения информационного противоборства, в том числе роста масштабов компьютерной преступности;

- на повышение результативности и эффективности системы обеспечения информационной безопасности в условиях реализации Стратегии;

- на повышение качества документации в области обеспечения информационной безопасности, аудита и самооценки, ресурсного обеспечения информационной безопасности и др.

Решение этих и других проблем системного характера, связанных в том числе с развитием Фонда, с созданием новых требований к функционалу информационных систем, требует постоянного развития методов и средств обеспечения информационной безопасности, перехода на новый современный уровень управления информационной безопасностью.

4.4. Фонд активно внедряет новые информационные технологии. Вместе с тем, Фонд учитывает, что практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз. Исходя из этого, актуальной является задача развития и совершенствования взаимодействия Фонда по вопросам информационной безопасности, в том числе структурных подразделений по безопасности и информационным технологиям на всех этапах жизненного цикла информационных систем и технологий, элементов информационной инфраструктуры.

5. Основные угрозы информационной безопасности

Представленные в настоящей Концепции основные угрозы информационной безопасности Фонда включают в себя не только актуальные угрозы, но и угрозы, которые могут возникнуть в будущем при изменении условий деятельности, внешних и внутренних факторов, в том числе при оптимизации организационно-штатной структуры и ротации кадров.

5.1. Внешние угрозы

Основными внешними угрозами информационной безопасности являются:

1) ужесточение санкций в отношении Российской Федерации;

2) наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информацию и информационную инфраструктуру в деструктивных целях;

3) активизация деятельности иностранных технических разведок относительно российских организаций;

4) обострение информационного противоборства, в том числе расширение масштабов использования специальными службами некоторых государств средств оказания деструктивного информационно-психологического воздействия, в том числе с использованием возможностей информационных технологий в кредитно-финансовой сфере;

5) рост числа правонарушений, связанных с обработкой персональных данных с использованием информационных технологий;

6) широкое использование российскими организациями импортного оборудования, содержащего скрытые возможности;

7) сохранение значительной доли теневой экономики, условий для коррупции и криминализации хозяйственно-финансовых отношений, в том числе с использованием возможностей информационных технологий;

8) рост информационного пространства за счет новых сервисов и услуг, не обеспечивающих адекватный уровень информационной безопасности;

9) стихийные бедствия (землетрясения, наводнения и др.), аварии и катастрофы, в том числе связанные с ухудшением технического состояния объектов инфраструктуры и возникновением пожаров;

10) террористические акты, криминальные действия в отношении Фонда и их работников.

5.2. Внутренние угрозы

Основными внутренними угрозами информационной безопасности являются:

1) противоправные действия (бездействия) работников Фонда, приводящие к нарушению информационной безопасности;

2) нарушения работниками Фонда требований нормативных правовых актов Российской Федерации, внутренних нормативных документов Фонда при работе с информацией, содержащей сведения, составляющие коммерческую и иную охраняемую законом тайну, с иной информацией ограниченного доступа и распространения;

3) коррупционные и иные правонарушения в Фонде, в том числе с использованием возможностей информационных технологий;

4) нарушения работниками Фонда требований информационной безопасности при работе в сети Интернет;

5) утечка высококвалифицированных работников Фонда, составляющих основу человеческого капитала;

6) нарушения работниками Фонда установленных требований, приводящие к реализации угроз информационной безопасности с использованием легально предоставленных им прав и полномочий (внутренние нарушители информационной безопасности);

7) нарушения работниками Фонда установленных требований, приводящие к реализации угроз информационной безопасности, с использованием прав и полномочий, полученных нелегально (внутренние нарушители информационной безопасности);

8) несанкционированные устные выступления работников Фонда на семинарах, симпозиумах, конференциях, презентациях, пресс-конференциях и т.п., несогласованные публикации в СМИ, наносящие ущерб Фонду, ВЭБ.РФ и организациям ВЭБ.РФ, в том числе ущерб их деловой репутации;

9) не в полной мере соответствующие современным угрозам модели угроз и модели нарушителей информационной безопасности, информационная инфраструктура и меры защиты;

10) утечка по техническим каналам информации ограниченного доступа и распространения;

11) сбои, отказы, разрушения/повреждения программных и технических средств.

6. Принципы обеспечения информационной безопасности

Принципами обеспечения информационной безопасности Фонда являются:

1) соблюдение и защита прав и свобод работников Фонда;

2) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений;

3) соответствие целей и задач обеспечения информационной безопасности Фонда нормативным правовым актам Российской Федерации, регулирующим их деятельность, целям и задачам Стратегии;

4) соблюдение требований нормативных документов по защите информации, содержащей сведения, составляющие коммерческую тайну, иной информации ограниченного доступа и распространения;

5) системность и комплексность применения силами обеспечения информационной безопасности Фонда организационных, экономических, информационных, правовых, технических, специальных и иных мер обеспечения информационной безопасности;

6) приоритет предупредительных мер в целях обеспечения информационной безопасности;

7) координация и конструктивное взаимодействие сил обеспечения информационной безопасности при решении задач по обеспечению информационной безопасности;

8) соблюдение баланса между потребностью работников Фонда в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения информационной безопасности;

9) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз и аудита информационной безопасности;

10) специализация, стандартизация и унификация, лицензирование деятельности;

11) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

7. Цели, задачи и основные направления обеспечения информационной безопасности

7.1. Основные цели обеспечения информационной безопасности

Основными целями обеспечения информационной безопасности являются:

1) достижение надежной и своевременной защиты интересов Фонда в информационной сфере от внешних и внутренних угроз, обеспечивающей эффективную реализацию Стратегии;

2) достижение стабильного функционирования и долгосрочного устойчивого развития Фонда;

3) повышение результативности и эффективности комплексного обеспечения информационной безопасности Фонда.

7.2. Основные задачи обеспечения информационной безопасности

Основными задачами обеспечения информационной безопасности являются:

1) обеспечение защиты прав и законных интересов Фонда в информационной сфере;

2) постоянное развитие и совершенствование системы обеспечения информационной

безопасности Фонда;

3) разработка, реализация и оценка проектов и мероприятий по обеспечению информационной безопасности Фонда;

4) развитие системы подготовки работников Фонда в области обеспечения информационной безопасности.

7.3. **Основные направления обеспечения информационной безопасности**

Основными направлениями обеспечения информационной безопасности являются:

1) обеспечение защиты интересов Фонда в информационной сфере;

2) разработка и реализация политик информационной безопасности Фонда на основе настоящей Концепции;

3) своевременное и надежное прогнозирование, предупреждение, обнаружение, предотвращение, отражение информационных угроз, а также ликвидация последствий их проявления;

4) разработка и реализация мер по обеспечению необходимого уровня информационной безопасности с учетом ужесточения санкций в отношении Российской Федерации, обострения информационного противоборства, в том числе роста масштабов компьютерной преступности;

5) нейтрализация информационного воздействия, направленного на размывание ценностей Фонда;

6) предупреждение, выявление и пресечение коррупционных и иных правонарушений в Фонде, в том числе с использованием возможностей информационных технологий;

7) определение приоритетных направлений противодействия информационным угрозам;

8) разработка и реализация мер по защите информации, содержащей сведения, составляющие коммерческую и иную охраняемую законом тайну, иной информации ограниченного доступа и распространения, не содержащей сведений, составляющих государственную тайну;

9) развитие организационной структуры управления информационной безопасностью;

10) учет, категорирование и классификация информационных ресурсов;

11) управление инцидентами информационной безопасности и рисками в информационной сфере, в том числе операционными;

12) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, методологического, технического, информационно-аналитического, кадрового и иного обеспечения;

13) развитие системы взаимодействия с внешними и внутренними клиентами Фонда, органами государственной власти по вопросам информационной безопасности;

14) обеспечение информационной безопасности на всех стадиях жизненного цикла автоматизированных информационных систем и технологий Фонда, внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

15) совершенствование порядка использования сети Интернет в Фонде с учетом обеспечения информационной безопасности, обеспечение работников ключевыми документами для средств криптографической защиты информации, в том числе электронной подписью;

16) оценка и контроль состояния информационной безопасности, системы обеспечения информационной безопасности, деятельности структурных подразделений по обеспечению информационной безопасности;

17) обеспечение соблюдения законодательных, нормативных и договорных требований в области информационной безопасности, формирование и развитие внутренней нормативной базы в области обеспечения информационной безопасности;

18) управление доступом к информационным ресурсам Фонда;

19) инженерно-техническая и физическая защита информационных ресурсов Фонда;

20) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий, подготовка должностных лиц к выполнению требований обеспечения безопасности информации, формирование культуры информационной безопасности.

8. Организационные основы реализации Концепции

8.1. Система обеспечения информационной безопасности Фонда является частью системы обеспечения безопасности Фонда и строится на основе разграничения полномочий сил обеспечения информационной безопасности.

Обеспечение информационной безопасности осуществляется на основе сочетания правовых, организационных, технических, информационно-аналитических, кадровых, экономических и иных мер, реализуемых силами обеспечения информационной безопасности.

8.2. Реализация настоящей Концепции осуществляется под руководством Генерального директора Фонда при координирующем участии заместителя председателя ВЭБ.РФ, координирующего и контролирующего деятельность организаций ВЭБ.РФ по вопросам безопасности и соблюдения режима секретности в ВЭБ.РФ (далее – заместитель председателя ВЭБ.РФ), путем согласованных действий сил обеспечения информационной безопасности Фонда на плановой основе за счет консолидации усилий и их ресурсов,

комплексного использования системы мер, разработанных в рамках стратегического и оперативного планирования.

8.3. Положения настоящей Концепции обязательны для выполнения всеми работниками Фонда и являются основой для разработки и корректировки внутренних нормативных документов Фонда, в том числе планов в области обеспечения информационной безопасности, а также документов, касающихся деятельности коллегиальных рабочих органов, а также структурных подразделений Фонда.

8.4. Контроль за ходом реализации настоящей Концепции осуществляется в рамках мониторинга основных показателей состояния информационной безопасности Фонда, его результаты отражаются в ежегодном докладе заместителя председателя ВЭБ.РФ председателю ВЭБ.РФ о состоянии информационной безопасности организаций ВЭБ.РФ и мерах по ее укреплению.

8.5. Корректировка настоящей Концепции проводится с учетом Стратегии, результатов мониторинга основных показателей состояния информационной безопасности Фонда.

9. Основные показатели состояния информационной безопасности Фонда

9.1. Основными показателями, необходимыми для оценки состояния информационной безопасности Фонда, являются:

1) степень выполнения планов реализации настоящей Концепции;

2) наличие аттестатов соответствия защищаемых объектов информатизации Фонда требованиям безопасности информации;

3) наличие сертификатов на средства защиты информации;

4) наличие лицензий на отдельные виды деятельности в сфере обеспечения информационной безопасности Фонда.

9.2. Перечень основных показателей состояния информационной безопасности Фонда может уточняться по результатам его мониторинга, а также по результатам аудита и самооценки информационной безопасности.

Приложение №2 к
Приказу генерального директора
от 06 марта 2020 года № 3-УП

ПОЛИТИКА
информационной безопасности некоммерческой организации «Фонд развития городов»

Оглавление

1. Общие положения

1.1. Политика информационной безопасности Фонда развития городов (далее – Фонд) разработана в целях обеспечения реализации стратегии развития Фонда, а также в целях повышения эффективности функционирования системы обеспечения безопасности в области защиты информации.

1.2. Политика информационной безопасности Фонда (далее – Политика) представляет собой систему официальных взглядов Фонда на обеспечение информационной безопасности и определяет основные термины, цели, задачи и основные принципы обеспечения информационной безопасности, общий подход к построению модели угроз и нарушителей, требования к системе обеспечения информационной безопасности, а также порядок контроля реализации и пересмотра Политики.

1.3. Настоящая Политика разработана на основании Концепции информационной безопасности государственной корпорации развития ВЭБ.РФ и организаций ВЭБ.РФ, Концепции информационной безопасности Фонда, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями), Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями), Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской федерации» (с изменениями), Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646, Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденной Президентом Российской Федерации 12.12.2014 № К 1274, Федерального закона от 17.05.2007 № 82-ФЗ «О государственной корпорации развития «ВЭБ.РФ» (с изменениями), а также с учетом иных внутренних нормативных, регламентирующих и распорядительных документов Фонда и ВЭБ.РФ в указанной сфере.

1.4. Работники Фонда в своей деятельности обязаны руководствоваться положениями настоящей Политики.

1.5. Руководители структурных подразделений Фонда несут ответственность за обеспечение выполнения требований к информационной безопасности в своих структурных подразделениях.

2. Термины, определения и сокращения

2.1. В настоящей Политике используются следующие термины и определения:

автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

вредоносное программное обеспечение – компьютерная программа либо иная компьютерная информации, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

информация – сведения (сообщения, данные) независимо от формы их представления;

информация ограниченного распространения – информация ограниченного распространения (конфиденциального характера и для служебного пользования), не содержащих сведений, составляющих государственную тайну;

информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Фонда, находящаяся в распоряжении Фонда и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме;

информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационная безопасность – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность. Приоритетность свойств информационной безопасности определяется ценностью указанных ресурсов для интересов (целей) Фонда;

информационная сфера – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений;

информационная инфраструктура Фонда (далее – информационная инфраструктура) – совокупность объектов информатизации, автоматизированных систем и сетей связи, принадлежащих Фонду на законных основаниях, в том числе систем обработки и анализа информации, технических и программных средств ее обработки, передачи, хранения и отображения, каналов информационного обмена и телекоммуникации, систем и средств защиты информации, объектов и помещений, в которых размещены такие системы, а также сайт Фонда в сети Интернет, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия;

информационные ресурсы Фонда (далее – информационные ресурсы) – документы и массивы документов, содержащиеся в информационных системах Фонда, а также иные отдельные документы и отдельные массивы документов;

инцидент информационной безопасности – событие или комбинация событий, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, результатом которой являются:

1) нарушение или возможное нарушение работы средств защиты информации в составе системы обеспечения информационной безопасности Фонда;

2) нарушение или возможное нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних нормативных, регламентирующих и распорядительных документов Фонда в области обеспечения информационной безопасности, нарушение или возможное нарушение выполнения процессов системы обеспечения информационной безопасности Фонда;

3) нанесение или возможное нанесение ущерба Фонду, а также клиентам и партнерам Фонда.

модель нарушителя информационной безопасности – описание и классификация нарушителей информационной безопасности, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способов реализации угроз информационной безопасности со стороны указанных нарушителей;

модель угроз информационной безопасности – описание актуальных для Фонда источников угроз информационной безопасности; методов реализации утроз информационной безопасности; объектов, пригодных для реализации угроз информационной безопасности; уязвимостей, используемых источниками угроз информационной безопасности; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба;

нарушитель – субъект, реализующий угрозы информационной безопасности, нарушая предоставленные ему полномочия по доступу к активам Фонда или по распоряжению ими;

обеспечение информационной безопасности Фонда (далее – обеспечение информационной безопасности) – осуществление Фондом взаимоувязанных правовых, организационных, технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, предупреждению, обнаружению, предотвращению, отражению угроз информационной безопасности, локализации и ликвидации последствий их проявления;

объекты информационной безопасности – все то, что защищается от информационных угроз.

Основными объектами информационной безопасности Фонда в рамках данной Политики являются:

1) информационные ресурсы;

2) информация ограниченного доступа и распространения, в том числе содержащая сведения, составляющие коммерческую и иную охраняемую законом тайну;

3) информационная инфраструктура, в том числе программно-аппаратные средства, информационные и телекоммуникационные системы, служебные помещения;

4) бизнес-процессы и системы управления (стратегического, корпоративного управления, управления безопасностью, рисками, персоналом и др.);

5) производственные, социальные и другие отношения в информационной сфере, регулируемые международными договорами Российской Федерации, законодательством Российской Федерации, договорными, контрактными, внутренними нормативными, регламентирующими и распорядительными документами Фонда;

объекты критической информационной инфраструктуры (далее – объекты КИИ) – объекты информационной инфраструктуры, внесенные в перечень критических объектов информационной инфраструктуры;

персональные данные (далее – ПДн) – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

платежная информация – информация, на основании которой совершаются операции, связанные с осуществлением переводов денежных средств;

риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы;

система информационной безопасности (далее – СИБ) – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение;

система менеджмента информационной безопасности (далее – СМИБ) – часть менеджмента Фонда, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения информационной безопасности;

система обеспечения информационной безопасности (далее – СОИБ) – совокупность системы информационной безопасности и системы менеджмента информационной безопасности Фонда;

угроза информационной безопасности – совокупность действий и факторов, создающих опасность нанесения ущерба интересам Фонда в информационной сфере;

уязвимость – слабое место в инфраструктуре, включая систему обеспечения информационной безопасности, которое может быть использовано для реализации или способствовать реализации угрозы информационной безопасности;

2.2. В настоящей Политике используются следующие сокращения:

АС – автоматизированная система;

ЖЦ – жизненный цикл;

ИБ – информационная безопасность;

ИСПДн – информационная система персональных данных;

НРД – перегламентированные действия в рамках предоставленных полномочий;

НСД – несанкционированный доступ;

СКЗИ – средство криптографической защиты информации.

Иные термины, определения и сокращения, используемые в Политике, понимаются и толкуются в соответствии с тем значением, какое они имеют в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», других нормативных правовых актах Российской Федерации.

3. Цели и задачи обеспечения информационной безопасности Фонда

3.1 Основными целями обеспечения ИБ Фонда являются:

1) достижение высокого уровня защищенности интересов Фонда в информационной сфере от внешних и внутренних угроз, обеспечивающего эффективную реализацию стратегии развития Фонда;

2) обеспечение стабильного функционирования и долгосрочного устойчивого развития Фонда;

3) обеспечение непрерывности деятельности Фонда посредством гарантирования доступности информационных активов и информационной инфраструктуры;

4) предотвращение или снижение ущерба от инцидентов ИБ посредством обеспечения целостности информационных активов и информационной инфраструктуры Фонда, а также обеспечения конфиденциальности защищаемых информационных активов Фонда;

5) управление риском нарушения ИБ.

3.2 Основными задачами обеспечения ИБ Фонда являются:

1) разработка требований по обеспечению ИБ;

2) контроль выполнения установленных требований по обеспечению ИБ;

3) повышение эффективности проектов и мероприятий по обеспечению и поддержанию ИБ;

4) разработка и совершенствование нормативных документов Фонда по обеспечению ИБ;

5) развитие и совершенствование процессов прогнозирования, выявления, предупреждения и пресечения внешних и внутренних угроз ИБ, процессов локализации и нейтрализации последствий их проявления;

6) организация защиты информационных ресурсов от вредоносного программного обеспечения;

7) построение процесса управления уязвимостями информационной инфраструктуры;

8) защита информации от несанкционированного доступа и утечки по техническим каналам связи;

9) комплексное решение задач обеспечения защиты информации, содержащей сведения, составляющие коммерческую и иную охраняемую законом тайну, иной информации ограниченного доступа и информации, в отношении которой установлено законодательством Российской Федерации требование об обеспечении ее конфиденциальности.

4. Основные принципы обеспечения информационной безопасности Фонда

Основными принципами обеспечения ИБ Фонда являются:

1) соблюдение и защита прав и свобод работников Фонда;

2) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений;

3) соответствие целей и задач обеспечения ИБ Фонда нормативным правовым актам Российской Федерации, а также целям и задачам стратегии развития Фонда;

4) соблюдение требований нормативных документов по защите информации, составляющей коммерческую и иную охраняемую законом тайну, иной информации ограниченного доступа и информации, в отношении которой установлено требование об обеспечении ее конфиденциальности;

5) соблюдение требований законодательства, надзорных и регулирующих органов;

6) системность и комплексность применения организационных, экономических, информационных, правовых, технических, специальных и иных мер по обеспечению ИБ;

7) приоритет предупредительных мер в целях обеспечения ИБ;

8) координация и конструктивное взаимодействие структурных подразделений Фонда при решении задач по обеспечению ИБ;

9) соблюдение баланса между потребностью работников Фонда в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения ИБ;

10) достаточность средств по обеспечению ИБ, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз и аудита ИБ;

11) специализация, стандартизация и унификация методов и подходов, лицензирование деятельности;

12) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

5. Система обеспечения информационной безопасности Фонда

Для управления риском нарушения ИБ и поддержания ИБ на должном уровне в Фонде реализуется четыре группы процессов в виде циклической модели:

1) планирование СОИБ;
2) реализация СОИБ;
3) мониторинг и анализ СОИБ;
4) совершенствование СОИБ.

Данные группы процессов составляют СМИБ Фонда. Совокупность СИБ Фонда и СМИБ Фонда составляет СОИБ Фонда.

Основой для построения СОИБ Фонда являются требования законодательства Российской Федерации, надзорных и регулирующих органов, а также условия ведения деятельности Фонда, выраженные в идентификации активов, подлежащих защите, построении моделей угроз и нарушителей.

6. Модели угроз и нарушителей информационной безопасности Фонда

6.1. Модели угроз и нарушителей ИБ должны быть основным инструментом Фонда при развертывании, поддержании и совершенствовании СОИБ.

6.2. Модели угроз и нарушителей ИБ должны быть разработаны в целом для Фонда, а также при необходимости для отдельных процессов и систем.

6.3. Модели угроз и нарушителей ИБ разрабатываются на основе опыта и фактов прошлого, но ориентированы на будущее.

6.4. Чем более обоснован и точен прогноз в отношении актуальных для Фонда рисков нарушения требований к ИБ, тем адекватнее и эффективнее будут планируемые и принимаемые меры по обеспечению требуемого уровня ИБ. При этом следует учитывать, что со временем угрозы, их источники и риски могут изменяться, поэтому модели следует периодически пересматривать.

6.5. Модели угроз и нарушителей ИБ должны учитывать требования законодательства Российской Федерации в области ИБ, разработки ведущих специалистов институтов развития, а также международный опыт в этой сфере.

6.6. При разработке моделей угроз и нарушителей ИБ необходимо учитывать, что из всех возможных объектов атак с наибольшей вероятностью нарушитель выберет наиболее слабо контролируемый объект, где его деятельность будет оставаться необнаруженной максимально долго. Поэтому все операции, где осуществляется взаимодействие работников Фонда со средствами и системами автоматизации, должны особенно тщательно контролироваться.

6.7. Защита информационных ресурсов Фонда должна быть обеспечена как от нарушителей (внутренних и внешних), так и от естественных (природных и техногенных) угроз.

6.8. При построении адекватной модели нарушителя необходимо классифицировать нарушителя по следующим параметрам:

1) по отношению к системе (внутренний, внешний нарушитель);

2) по правам доступа;

3) по мотивам нарушения;

4) по уровню знаний о системе;

5) по уровню возможностей (используемым методам и средствам);

6) по времени действия;

7) по месту действия.

6.9. При построении адекватной модели угроз необходимо исходить из того, что основными угрозами ИБ являются:

6.9.1. Внешние угрозы:

1) ужесточение санкций в отношении Российской Федерации;

2) наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информацию и информационную инфраструктуру в деструктивных целях;

3) активизация деятельности иностранных технических разведок относительно российских организаций;

4) обострение информационного противоборства, в том числе расширение масштабов использования специальными службами некоторых государств средств оказания деструктивного информационно-психологического воздействия, в том числе с использованием возможностей информационных технологий и в целях размывания традиционных российских духовно-нравственных ценностей;

5) рост попыток подрыва деловой репутации и дискредитации деятельности Фонда, в том числе в средствах массовой информации;

6) рост масштабов компьютерной преступности;

7) рост числа правонарушений, связанных с обработкой персональных данных с использованием информационных технологий;

8) широкое использование российскими организациями импортного оборудования, содержащего скрытые возможности;

9) сохранение значительной доли теневой экономики, условий для коррупции и криминализации хозяйственно-финансовых отношений, в том числе с использованием возможностей информационных технологий;

10) рост информационного пространства за счет новых сервисов и услуг, не обеспечивающих адекватный уровень ИБ;

11) стихийные бедствия (землетрясения, наводнения и др.), аварии и катастрофы, в том числе связанные с ухудшением технического состояния объектов инфраструктуры и возникновением пожаров;

12) террористические акты, криминальные действия в отношении Фонда и работников Фонда.

6.9.2. Внутренние угрозы:

1) противоправные действия (бездействия) работников Фонда, приводящие к нарушению ИБ;

2) нарушения работниками Фонда требований нормативных правовых актов Российской Федерации, нормативных документов Фонда при работе с информацией, содержащей сведения, составляющие коммерческую и иную охраняемую законом тайну, с иной информацией ограниченного доступа и распространения;

3) коррупционные и иные правонарушения в Фонде, в том числе с использованием возможностей информационных технологий;

4) нарушения работниками Фонда требований информационной безопасности при работе в сети «Интернет»;

5) нарушения работниками Фонда установленных требований, приводящие к реализации угроз ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);

6) нарушения работниками Фонда установленных требований, приводящие к реализации угроз ИБ, с использованием прав и полномочий, полученных нелегально (внутренние нарушители ИБ);

7) несанкционированные устные выступления работников Фонда на семинарах, симпозиумах, конференциях, презентациях, пресс-конференциях и т.п., несогласованные

публикации в СМИ, наносящие ущерб Фонду и/или ВЭБ.РФ, в том числе ущерб их деловой репутации;

8) утечка по техническим каналам информации ограниченного доступа и распространения;

9) сбои, отказы, разрушения/повреждения программных и технических средств.

7. Система информационной безопасности Фонда

7.1. Выполнение требований к СИБ является ключевым процессом для обеспечения должного уровня ИБ Фонда. Формирование требований к СИБ проводится на основе:

1) положений настоящей Политики;

2) выполнения деятельности в рамках СМИБ.

7.2. Требования к СИБ формируются для следующих областей:

1) назначение и распределение ролей и обеспечение доверия к персоналу;

2) обеспечение ИБ на стадиях ЖЦ АС;

3) защита от НСД и НРД, управление доступом и регистрацией всех действий в АС, телекоммуникационном оборудовании, автоматических телефонных станциях и т.д.;

4) защита от вредоносного программного обеспечения;

5) использование ресурсов сети Интернет;

6) использование СКЗИ;

7) защита информационных технологических процессов;

8) защита технологических процессов и информационных систем, в которых обрабатываются персональные данные;

7.3. При распределении прав доступа работников и клиентов к информационным ресурсам Фонда руководствуется следующими принципами:

1) «Знать своего клиента» (Know your Customer) – принцип, используемый регулирующими органами для выражения отношения к организациям с точки зрения знания деятельности их клиентов;

2) «Знать своего служащего» (Know your Employee) – принцип, демонстрирующий озабоченность организации отношением служащих к своим обязанностям и возможными проблемами, такими как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью;

3) «Необходимо знать» (Need to Know) – принцип, ограничивающий полномочия по доступу к информации и ресурсам по обработке информации на уровне, минимально необходимом для выполнения определенных обязанностей;

4) «Двойное управление» (Dual Control) – принцип сохранения целостности процесса и борьбы с искажением функций системы, требующий дублирования (алгоритмического, временного, ресурсного или иного) действий до завершения определенных транзакций.

7.4. Формирование ролей осуществляется на основании существующих бизнес-процессов и проводится с целью исключения концентрации полномочий и снижения риска инцидентов ИБ, связанных с потерей информационными ресурсами свойств доступности, целостности или конфиденциальности.

7.5. Для обеспечения ИБ и контроля за качеством обеспечения ИБ должны быть определены роли, связанные с деятельностью по обеспечению ИБ.

7.6. ИБ АС должна обеспечиваться на всех стадиях ЖЦ АС с учетом интересов всех сторон, вовлеченных в процессы ЖЦ АС (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих подразделений).

7.7. При принятии решений об использовании сети Интернет, при формировании документов, регламентирующих порядок использования сети Интернет, а также иных документов, связанных с обеспечением ИБ при использовании сети Интернет, учитываются следующие положения:

1) сеть Интернет не имеет единого органа управления и не является юридическим лицом, с которым можно заключить договор. Провайдеры сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;

2) существует вероятность НСД, потери и искажения информации, передаваемой посредством сети Интернет;

3) существует вероятность атаки на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные к/из сети Интернет;

4) гарантии по обеспечению ИБ при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются.

7.8. В целях соблюдения лицензионных требований при осуществлении деятельности, связанной с шифровальными (криптографическими) средствами, Фонд получает и поддерживает в актуальном состоянии лицензию на осуществление данного вида деятельности и осуществляет взаимодействие с структурными подразделениями Фонда по вопросам настройки и эксплуатации АС.

7.9. В Фонде должна быть определена, выполняться и контролироваться политика в отношении обработки ПДн, а также в случае необходимости должны быть установлены порядки обработки ПДн для отдельных ресурсов ПДн. Должны быть определены цели обработки, перечень лиц, допущенных к обработке ПДн, а также соблюдаться требования по обеспечению защиты ПДн в соответствии с необходимым уровнем защищенности ИСПДн.

7.10. Детальные требования для областей, указанных в пункте 7.2 настоящей Политики, формируются в частных политиках второго и третьего уровней.

8. Система менеджмента информационной безопасности Фонда

8.1. Целью выполнения деятельности в рамках группы процессов «планирование» является запуск «цикла» СМИБ путем определения первоначальных планов построения, а также планов совершенствования СОИБ на основании решений, принятых на этапе «совершенствование».

8.2. Этап «реализация» выполняется по результатам выполнения этапов «планирование» и (или) «совершенствование» и заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СОИБ, определенных на этапе «планирование» и (или) реализации решений, принятых на этапе «совершенствование».

8.3. Целью выполнения деятельности в рамках группы процессов «проверка» является обеспечение достаточной уверенности в том, что СОИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ, а также внутренним и (или) внешним условиям функционирования Фонда, связанным с ИБ.

8.4. Группа процессов «совершенствование» включает в себя деятельность по принятию решений о реализации тактических и (или) стратегических улучшений СОИБ. Указанная деятельность, то есть переход к этапу «совершенствование», реализуется только тогда, когда выполнение процессов этапа «проверка» дало результат, требующий совершенствования СОИБ.

8.5. Необходимо накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения.

8.6. Для функционирования СМИБ выполняются следующие требования:

1) требования к организации и функционированию структурного подразделения, обеспечивающего ИБ;

2) требования к определению/коррекции области действия СОИБ;

3) требования к выбору/коррекции подхода к оценке рисков нарушения ИБ и проведению оценки рисков нарушения ИБ;

4) требования к разработке планов обработки рисков нарушения ИБ;

5) требования к разработке/коррекции внутренних документов, регламентирующих деятельность в области обеспечения ИБ;

6) требования к принятию руководством решений о реализации и эксплуатации СОИБ;

7) требования к организации реализации планов обработки рисков нарушения ИБ;

8) требования к разработке и организации реализации программ по обучению работников Фонда и повышению их осведомленности в области ИБ;

9) требования к организации обнаружения и реагирования на инциденты безопасности;

10) требования к организации обеспечения непрерывности бизнес-процессов и их восстановления после прерываний;

11) требования к мониторингу СОИБ и контролю защитных мер;

12) требования к анализу функционирования СОИБ;

13) требования к принятию решений по тактическим улучшениям СОИБ;

14) требования к принятию решений по стратегическим улучшениям СОИБ.

8.7. Детализация требований, указанных в пункте 8.6 настоящей Политики, формируется в частных политиках второго и третьего уровней.

9. Контроль реализации Политики информационной безопасности Фонда

Контроль реализации настоящей Политики осуществляется назначенными Генеральным директором Фонда ответственными работниками Фонда.

10. Порядок пересмотра Политики информационной безопасности Фонда

10.1. Настоящая Политика и соответствующие частные политики/положения/порядки/регламенты должны пересматриваться и при необходимости обновляться, при этом ответственность за их пересмотр и обновление возлагается на ответственных за ИБ работников Фонда, в должностные обязанности которых входит выполнение функций в области обеспечения ИБ.

10.2. В случае изменения действующего законодательства Российской Федерации, внесения изменений во внутренние нормативные, регламентирующие и распорядительные документы Фонда настоящая Политика действует в части, не противоречащей действующему законодательству и действующим внутренним нормативным, регламентирующим и распорядительным документам Фонда, до приведения ее в соответствие с такими изменениями.