«УТВЕРЖДЕНА»
решением Правления
Акционерного общества
«Фонд развития предпринимательства «Даму»
от 17 марта 2011 года, протокол № 11/2011

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «Фонд развития предпринимательства «Даму»

(с изменениями и дополнениями по состоянию на 03.07.2015 г.)

Алматы, 2015

Содержание:

Введение

Настоящая Политика информационной безопасности (далее - Политика) АО «Фонд развития предпринимательства Даму» (далее - Фонд) определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих Положений, Правил, Инструкций.

Нормативно-правовую основу Политики составляет законодательство Республики Казахстан по вопросам использования информационных систем, нормативные правовые акты Республики Казахстан, требования международных стандартов управления информационной безопасностью, а именно СТ РК ИСО/МЭК 27001:2008.

Обеспечение информационной безопасности - необходимое условие для успешного осуществления коммерческой деятельности Фонда. Фонд рассматривает информацию как один из важнейших активов. Информационная безопасность является элементом общей политики Фонда в сфере обеспечения безопасности бизнеса. Нарушения в данной области

могут привести к серьезным последствиям, включая потерю доверия со стороны клиентов и снижению конкурентоспособности.

Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информации и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Фонд. Положения настоящего документа относятся ко всем штатным работникам и временным работникам, имеющим доступ к автоматизированным и телекоммуникационным системам Фонда.

Неотъемлемой частью организации защиты информации является непрерывный контроль эффективности предпринимаемых мер, определение для работников Фонда перечня недопустимых действий, возможных последствий и ответственности.

Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их системное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий.

1. Термины и определения

В настоящей Политике используются следующие понятия:

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации - защищенность информации от ее нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного ее тиражирования.

Доступность - возможность для авторизованного пользователя информационной системы за приемлемое время получить информационную услугу, предусмотренную функциональностью.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность (ИБ) - комплекс административно-правовых, организационно-распорядительных и технических мер, направленных на обеспечение конфиденциальности, целостности и санкционированной доступности информации в процессе ее сбора, обработки, передачи и хранения.

Информационная система (ИС) обработки информации - организационно-техническая структура, представляющая собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных;
- методов и алгоритмов обработки в виде соответствующего программного обеспечения;
- баз данных на различных носителях;
- персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных.

Конфиденциальность - защита от несанкционированного ознакомления.

Несанкционированное действие - действие субъекта в нарушение установленных в системе правил обработки информации.

Пользователь - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Сеть (локальная сеть, ЛВС, LAN) - группа точек, узлов или других устройств, соединенных коммуникационным набором оборудования, обеспечивающее соединение станций и передачу между ними информации.

Угроза - реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного нарушения режима функционирования объекта.

Уязвимость - любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

Целостность информации - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому ее состоянию).

Шифрование - это преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки.

2. Цели, задачи и основополагающие принципы

2.1 Основной целью системы информационной безопасности является защита корпоративной ИС Фонда от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня рисков.

2.2 Основными задачами системы информационной безопасности являются:

2.2.1 отнесение информации к категории несекретной, ограниченного распространения, банковской, коммерческой и другим видам тайн, иной конфиденциальной информации, подлежащей защите от неправомерного использования;

2.2.2 прогнозирование и своевременное выявление угроз безопасности информационным ресурсам Фонда, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

2.2.3 создание условий функционирования Фонда с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения ущерба;

2.2.4 создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Фонда, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности;

2.2.5 создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц.

2.3 Построение системы обеспечения безопасности информации Фонда и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

2.3.1 законности - соблюдение законодательства по защите информации и законных интересов всех участников информационного обмена;

2.3.2 системности - подход к вопросам организации информационной безопасности должен быть логическим и последовательным: в первую очередь оценка риска информационной безопасности исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику Фонда;

2.3.3 эффективности - реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению ИБ должны сводить риски к минимуму, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;

2.3.4 целесообразности - соблюдение соразмерности затрат на обеспечение защиты информации и потенциальных потерь при реализации угроз;

2.3.5 непрерывности - принцип функционирования системы информационной безопасности, учитывающий, что злоумышленники в любой момент времени ищут возможность обхода защитных мер, прибегая для этого к легальным и нелегальным методам;

2.3.6 взаимодействии и координации - осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи подразделений службы безопасности, информационных технологий и подразделений-пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания информационных систем, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными государственными органами. Эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными специалистами ответственных подразделений Фонда;

2.3.7 совершенствовании - совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;

2.3.8 приоритетности - категорирование (ранжирование) всех информационных ресурсов Фонда по степени важности и оценка реальных, а также потенциальных угроз информационной безопасности;

2.3.9 информированности и персональной ответственности - пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации, информационные сервисы индивидуально идентифицирует пользователей и инициируемые ими процессы;

2.3.10 соответствие стандартам - система информационной безопасности соответствует международным стандартам в данной области;

2.3.11 обязательность контроля - контроль за деятельностью пользователей, а также мониторинг работы ИС должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия.

3. Объекты обеспечения информационной безопасности

3.1 Автоматизированная система обработки информации Фонда является распределенной структурой, объединяющей в единую ИС подсистемы центрального аппарата, региональных филиалов. Основными объектами обеспечения информационной безопасности в Фонде признаются следующие элементы:

3.1.1 информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством к государственной тайне, коммерческой тайне Фонда, открытая информация, необходимая для обеспечения нормального функционирования Фонда (в дальнейшем - защищаемая информация);

3.1.2 средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;

3.1.3 программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы Фонда, с помощью которых производится обработка защищаемой информации;

3.1.4 помещения, предназначенные для ведения закрытых переговоров и совещаний;

3.1.5 помещения, в которых расположены средства обработки защищаемой информации;

3.1.6 технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

3.2 Подлежащая защите информация может находиться:

3.2.1 на бумажных носителях;

3.2.2 в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);

3.2.3 передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;

3.2.4 в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;

3.2.5 записываться и воспроизводиться с помощью технических средств (диктофоны, видеомагнитофоны и др.).

4. Меры обеспечения безопасности

4.1 Меры обеспечения безопасности. Все меры обеспечения безопасности компьютерных систем подразделяются на:

- правовые (законодательные);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратурные и программные).

4.2 Законодательные (правовые) меры защиты. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

4.3 Морально-этические меры защиты. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

4.4 Организационные (административные) меры защиты. Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных,

использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

4.5 Физические средства защиты. Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

4.6 Технические (программно-аппаратные) средства защиты. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав информационных систем Фонда и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

5. Угрозы информационной безопасности

5.1 Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

5.1.1 утрата сведений, составляющих банковскую тайну, коммерческую тайну Фонда и иную защищаемую информацию, а также искажение (несанкционированная модификация, подделка) такой информации;

5.1.2 утечка - несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.), а также утечка информации по каналам связи и за счет побочных электромагнитных излучений;

5.1.3 недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;

5.1.4 отсутствие планирования и контроля;

5.1.5 низкая степень надежности программного обеспечения;

5.1.6 недостаточная осведомленность персонала, низкая квалификация персонала и пользователей в области информационных технологий.

5.2 В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Фонда и его нормальное функционирование:

5.2.1 финансовые потери, связанные с утечкой или разглашением защищаемой информации;

5.2.2 финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;

5.2.3 ущерб от дезорганизации деятельности Фонда и потери, связанные с невозможностью выполнения им своих обязательств;

5.2.4 моральные потери (ущерб репутации Фонда).

6. Техническое обеспечение информационной безопасности Фонда

6.1 Техническое обеспечение информационной безопасности должно базироваться:

6.1.1 на системе унификации и взаимного дополнения применяемых средств защиты;

6.1.2 на системе лицензирования деятельности;

6.1.3 на системах сертификации всего программного обеспечения и средств защиты.

6.2 Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, технических, программных и криптографических средств и мер по защите информации в процессе документооборота, при работе работников с конфиденциальными документами и сведениями, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров.

6.3 Предоставление прав доступа работникам Фонда к соответствующей информации определяется в порядке, определяемом внутренними документами Фонда.

6.4 Одним из направлений обеспечения информационной безопасности является реализация технической политики, то есть защита информационных ресурсов от хищения, утраты, уничтожения, разглашения, утечки, искажения и подделки за счет несанкционированного доступа и иных воздействий.

6.5 В рамках обеспечения информационной безопасности, техническая политика предусматривает:

6.5.1 реализацию единой разрешительной системы допуска работников к работам, документам и информации конфиденциального характера;

6.5.2 ограничение доступа работников и посторонних лиц в здания, помещения, где обрабатывается (хранится) информация конфиденциального характера, в том числе на объекты информатики;

6.5.3 разграничение доступа пользователей к данным автоматизированных систем различного уровня и назначения;

6.5.4 учет документов, информационных массивов, регистрация действий пользователей ИС, контроль за несанкционированным доступом и действиями пользователей;

6.5.5 криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;

6.5.6 предотвращение внедрения в автоматизированные ИС программ вирусного характера.

6.6 Защита информационных ресурсов от несанкционированного доступа предусматривает:

6.6.1 единую централизованную политику обеспечения безопасности автоматизированных систем, регистрации и проверки прав доступа работников Фонда;

6.6.2 обоснованность доступа, предполагающую наличие соответствующей формы допуска работника для ознакомления с информацией (документацией) определенного уровня конфиденциальности при необходимости ознакомления с данной информацией или действий с ней для выполнения производственных функций;

6.6.3 персональную ответственность, предполагающую ответственность работника за использование и сохранность доверенной информации (документов, носителей информации, информационных массивов), за свои действия в автоматизированной системе;

6.6.4 надежность хранения, предполагающую хранение информации (документов, носителей информации, информационных массивов) в условиях, исключающих несанкционированное ознакомление, ее уничтожение, подделку или искажение;

6.6.5 централизованный контроль за действиями работников с конфиденциальными документами, а также конфиденциальной информацией в автоматизированных системах;

6.6.6 целостность технической и программной среды, обрабатываемой информации и средств защиты, предполагающую физическую сохранность средств информатизации, неизменность программной среды, определяемую предусмотренной технологией

обработки информации, выполнение средствами защиты предусмотренных функций, изолированность средств защиты от пользователей.

6.7 Обеспечение безопасности ИС предполагает разработку необходимых мер защиты на этапе формирования будущей автоматизированной системы, что заключается в составлении спецификаций на приобретаемое оборудование и программное обеспечение с учетом предъявляемых требований по безопасности.

6.8 В процессе формирования заказа на построение ИС необходимо учитывать не только основной набор функциональных сервисов (бухгалтерские системы, системы автоматизации процедур, делопроизводства и тому подобные), но и ряд необходимых вспомогательных сервисов, обеспечивающих надежное функционирование системы и требуемый уровень безопасности. При этом необходимо учитывать, что в защите нуждаются все сервисы и коммуникационные пути между ними. В случае, если не все функционально законченные сервисы обладают полным набором механизмов безопасности, они требуют объединения в составные сервисы, в совокупности, обладающие таким набором и с внешней точки зрения представляющих собой единое целое.

6.9 Обеспечение единой политики процедур регистрации и предоставления доступа, а также требование обоснованности доступа реализуется в рамках разрешительной системы допуска к работам, документам и сведениям, которая предполагает определение для всех пользователей автоматизированных систем доступные им информационные и программные ресурсы, а также конкретные операции (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

6.10 Условие надежности хранения информации реализуется с помощью:

6.10.1 оборудования помещений, в которых ведется обработка конфиденциальной информации сейфами и металлическими шкафами для хранения документов, а также техническими средствами разграничения и контроля доступа;

6.10.2 использования криптографического преобразования информации в автоматизированных системах.

6.11 Система контроля за действиями работников реализуется с помощью:

6.11.1 организационных мер и технических средств контроля при работе с конфиденциальными документами и сведениями;

6.11.2 регистрации (протоколирования средствами системного аудита) действий пользователей с информационными и программными ресурсами автоматизированных систем с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата, включая запрещенные попытки доступа;

6.11.3 сигнализации о несанкционированных действиях пользователей.

6.12 Целостность автоматизированных систем достигается комплексом программно-технических средств и организационных мероприятий, осуществляемых уполномоченными подразделениями Фонда.

6.13 При необходимости передачи по внешним линиям связи конфиденциальной информации, основным направлением защиты информации от перехвата, искажения и навязывания ложной информации является использование криптографического преобразования информации, а на небольших расстояниях, использование защищенных волоконно-оптических линий связи.

6.14 Для защиты информации должны использоваться средства криптографической защиты данных гарантированной стойкости для определенного уровня конфиденциальности передаваемой информации и соответствующая ключевая система, обеспечивающая надежный обмен информацией и аутентификацию (подтверждение подлинности) сообщений.

6.15 Необходимой составляющей системы безопасности должно быть обеспечение качества работ и используемых средств и мер защиты, нормативной базой которого является система стандартов и других нормативных правовых актов по безопасности,

утвержденных органами государственного управления в соответствии с их компетенцией и определяющие нормы защищенности информации и требования в различных направлениях защиты информации.

6.16 В целях обеспечения заданного качества функционирования системы информационной безопасности, должно проводиться предпроектное обследование и проектирование ИС, выработка требований по средствам защиты информации и контроля, предполагаемых к использованию в этих системах, а также контроль защищенности информационных ресурсов.

6.17 Применение аутентификации в автоматизированных системах обусловлено необходимостью гарантированного сопоставления участников информационного обмена учетным записям в системе в целях предоставления им законно предоставленных прав на реализацию системных процедур. Аутентификация в вычислительных сетях призвана обеспечить заданную степень уверенности получателя в том, что полученная информация была передана отправителем и при этом не была заменена или искажена.

6.18 Целью аутентификации является защита участников информационного обмена от стороннего вмешательства путем взаимной идентификации. Важной мерой защиты передаваемых в электронном виде данных, является шифрование.

7. Организационное обеспечение информационной безопасности

7.1 Задачи обеспечения безопасности информационных ресурсов решаются следующими организационными методами:

7.1.1 разработкой и осуществлением разрешительной системы допуска работников к работам с документами и сведениями конфиденциального характера;

7.1.2 установлением единого порядка хранения и обращения конфиденциальной информации (документов, носителей информации);

7.1.3 координацией работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи.

7.2 В работе с работником Фонда основными организационными мерами в плане достижения информационной безопасности являются:

7.2.1 заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности и сохранность конфиденциальной информации;

7.2.2 проведение первоначального инструктажа, периодического обучения и повышения квалификации работников Фонда в области информационной безопасности.

7.3 Система распределения обязанностей между отдельными работниками может в значительной мере способствовать повышению общего уровня информационной безопасности. Этого можно достичь следующими методами:

7.3.1 минимизация данных, доступных работникам. Каждый работник должен знать только те детали процедур обработки данных, которые необходимы ему для выполнения своих обязанностей. Организация технологического процесса сбора и обработки информации и планирование помещений должны по мере возможности исключать или сводить к минимуму контакты персонала в процессе выполнения работ. Каждый работник должен знать все о своей работе и связанных с нею ограничениях, а также четко представлять последствия нарушения этих ограничений;

7.3.2 разделение полномочий и дублирование контроля. В системах с высокими требованиями по обеспечению сохранности данных ответственная работа или процедура (например, изменение статуса электронного документа) выполняется после подтверждения ее необходимости двумя работниками. Временные или вновь принятые работники, а также работники, проходящие обучение, стажировку, практику не должны самостоятельно выполнять ответственные задания.

7.4 Административные меры защиты информации предполагают:

7.4.1 обеспечение физической сохранности автоматизированной системы и дополнительного оборудования;

7.4.2 организацию контроля доступа и режима выполнения работ персоналом подразделения информационных технологий;

7.4.3 инспектирование правильности и полноты выполнения персоналом подразделения информационных технологий мер по обеспечению сохранности необходимых дубликатов файлов, библиотеки программ, оборудования системы;

7.4.4 практическую проверку функционирования отдельных мер защиты: предотвращения недозволенных изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;

7.4.5 проверку машинных и ручных протоколов выполнения работ со стороны пользователей;

7.4.6 ознакомление работников Департамента информационных технологий со всеми новыми разработками по обеспечению сохранности данных.

8. Программа создания системы безопасности

8.1 Политика служит методологической основой для формирования и реализации программы создания системы информационной безопасности Фонда. В целом для функционирования системы информационной безопасности с учетом положений Политики должны быть разработаны и приняты (с учетом необходимого обновления) следующие документы:

8.1.1 классификация (анализ) рисков информационной безопасности;

8.1.2 внутренний документ Фонда о порядке отнесения сведений к конфиденциальной информации;

8.1.3 перечень сведений, составляющих конфиденциальную информацию;

8.1.4 организационно-распорядительные документы, регламентирующие порядок и правила обеспечения сохранности конфиденциальной информации в рамках каждой функциональной задачи и соответствующей ей автоматизированной системы.

8.2 Для осуществления технической политики в области обеспечения информационной безопасности необходимо разработать и реализовать комплекс мероприятий:

8.2.1 по обеспечению технической, программной и криптографической защиты информации в автоматизированных системах;

8.2.2 по оснащению важнейших объектов и помещений средствами и системами защиты и контроля.

8.3 В процессе создания системы безопасности необходимо предусмотреть приоритеты реализации наиболее важных и актуальных направлений обеспечения безопасности, с учетом выделяемых финансовых ресурсов.

8.4 В целях достижения оптимального уровня информационной безопасности следует:

8.4.1 иметь в наличие внутренний документ, определяющий порядок определения сведений, составляющих конфиденциальную информацию Фонда и требования к организации их защиты, включающие описание процедур отнесения сведений к категории конфиденциальных и, в случае необходимости, в установленном порядке вносить в него изменения и дополнения;

8.4.2 регулярно проводить анализ принятой технологии обработки конфиденциальной информации, включая категорирование ресурсов по степени критичности обрабатываемых с их помощью данных;

8.4.3 определять полный перечень и возможные угрозы нарушения конфиденциальности информации и классифицировать их по вероятности возникновения исходя из принятой типовой модели нарушителя;

8.4.4 с учетом действующих мер и средств защиты проводить оценку риска утечки конфиденциальной информации;

8.4.5 разработать и внедрить систему обеспечения безопасности информации в Фонде (систему защиты информации), направленную на снижение уровня риска, включающую комплекс организационных мер и технических средств;

8.4.6 на постоянной основе проводить обучение и повышение квалификации персонала Фонда в области информационной безопасности;

8.4.7 проводить периодический контроль эффективности и адекватности принимаемых мер защиты информации.

9. Разделение полномочий и ответственность

9.1 Руководство Фонда осуществляет координацию деятельности всех подразделений для организации и поддержания соответствующего уровня информационной безопасности.

9.2 Решение вопросов стратегического планирования по информационной безопасности, а также контроль нештатных ситуаций и инцидентов в области защиты информации, осуществляет Департамент безопасности совместно с Департаментом информационных технологий.

9.3 В рамках исполнения настоящей политики Фонд проводит регулярный мониторинг и аудит программно-аппаратного комплекса, обеспечивающего функционирование норм и правил настоящей политики. Аудит проводится силами и средствами Департамента информационных технологий при общем участии Департамента безопасности, на регулярной основе, по согласованному и утвержденному план-графику, с представлением отчетности руководству курирующих департаментов. Независимый аудит информационной безопасности может быть проведен по решению Совета Директоров Фонда с привлечением независимой аудиторской компании.

9.4 Департамент безопасности выполняет мониторинг защищенности информационных ресурсов, разрабатывает правила и инструкции, контролирует соблюдение требований информационной безопасности всеми участниками информационного обмена. Расследование инцидентов осуществляет Департамент безопасности Фонда совместно с Департаментом информационных технологий.

9.5 Директора департаментов и филиалов Фонда несут ответственность за ознакомление работников с требованиями информационной безопасности.

9.6 Администраторы ресурсов ИС обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.

9.7 Задачей каждого пользователя ИС является соблюдение правил, инструкций, рекомендаций по обеспечению безопасной работы ИС, извещение руководства обо всех подозрительных ситуациях при работе с информационными ресурсами.

9.8 За несоблюдение порядка и правил использования информационных ресурсов к виновным могут быть применены меры, предусмотренные трудовыми договорами, заключенными между Фондом и работником, а также действующим законодательством Республики Казахстан и настоящей Политикой.

10. Порядок пересмотра Политики, документы, регламентирующие Политику

10.1 Департаментом безопасности ежегодно пересматриваются основные принципы, направления и требования по защите информации в Фонде. Пересмотр Политики осуществляется в соответствии с изменениями, влияющими на первоначальную оценку риска, путем выявления существенных инцидентов нарушения информационной безопасности, появления новых уязвимостей или изменения организационной, или технологической инфраструктуры Фонда.

10.2 Настоящая Политика регламентируется дополнительными документами, предусмотренными пунктом 8.1. настоящей Политики и соответствующими Правилами информационной безопасности по конкретным областям ее применения.