УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБЩИЕ ТРЕБОВАНИЯ

[СОИБ-100]

2018г.

Оглавление

1. Общие положения

1.1. Выполнение требований к Системе обеспечения информационной безопасности (далее – СОИБ) ООО «Сатурн» (далее - Компания) является основой для обеспечения необходимого и достаточного уровня информационной безопасности (далее - ИБ). Формирование требований к СОИБ Компании проводится на основе:

- положений настоящего документа;
- выполнения деятельности в рамках СМИБ Компании.

Требования к СОИБ Компании оформляются документально.

1.2. Положения раздела 2 настоящего документа образуют базовый набор требований к СОИБ Компании. Данный базовый набор требований может быть расширен по результатам анализа и оценки рисков нарушения ИБ.

1.3. Требования к СОИБ должны быть сформированы по следующим направлениям:

- назначение и распределения ролей и обеспечение доверия к персоналу;
- обеспечение ИБ на стадиях жизненного цикла информационных систем (далее - ИС);
- защита от несанкционированного доступа (далее – НСД), управление доступом и регистрацией всех действий в ИС, в телекоммуникационном оборудовании, автоматических телефонных станциях и т.д.;
- антивирусная защита;
- использование ресурсов сети Интернет;
- использование средств криптографической защиты информации (далее – СКЗИ);
- защита информационных технологических процессов, в том числе бизнес-процессов, в рамках которых обрабатываются персональные данные.

В отдельных подразделениях Компании требования к СОИБ могут формироваться и для других областей и направлений деятельности.

1.4. Для обеспечения ИБ и контроля за качеством обеспечения ИБ в Компании должна быть реализована Система менеджмента информационной безопасности (далее - СМИБ). Руководство Компании должно осуществлять координацию своевременности и качества выполнения ролей в рамках СМИБ.

1.5. Формирование ролей должно осуществляться на основании существующих бизнес-процессов Компании и проводиться с целями:

- исключения концентрации полномочий;
- снижения риска инцидентов ИБ, связанных с потерей информационными активами свойств доступности, целостности и конфиденциальности.

Формирование ролей не должно выполняться по принципу фиксации фактически сложившихся прав и полномочий персонала Компании.

1.6. ИБ Компании должна обеспечиваться на всех стадиях жизненного цикла (далее – ЖЦ) информационных систем, автоматизирующих информационные технологические процессы, с учетом интересов всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений Компании).

1.7. В рамках информационных технологических процессов в качестве активов, защищаемых в первую очередь, следует рассматривать:

- производственный процесс;

- финансовую и тендерную информацию.

2. Общие требования обеспечения информационной безопасности

2.1. Общие требования по обеспечению информационной безопасности при назначении и распределении ролей, и обеспечении доверия к персоналу

2.1.1. Должны быть выделены и документально определены роли ее работников.

Формирование ролей, связанных с выполнением деятельности по обеспечению ИБ среди прочего должно осуществляться на основании требований СМИБ Компании.

2.1.2. Роли следует персонифицировать с установлением ответственности за их выполнение. Ответственность должна быть документально зафиксирована в должностных инструкциях.

2.1.3. С целью снижения рисков нарушения ИБ не допускается, чтобы в рамках одной роли совмещались следующие функции:

- разработки и сопровождения системы/ПО;
- эксплуатации системы/ПО;
- администратора системы;
- администратора ИБ;
- выполнения операций в системе и контроля их выполнения.

2.1.4. Должны быть документально определены и выполняться процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом Компании.

2.1.5. Должны быть документально определены процедуры приема на работу по отношению к должностям, влияющим на обеспечение ИБ, включающие:

- проверку подлинности предоставленных документов;
- заявляемой квалификации;
- точности и полноты биографических фактов;
- проверку в части профессиональных навыков и оценку профессиональной пригодности.

Указанные процедуры должны предусматривать документальную фиксацию результатов проводимых проверок.

2.1.6. Необходимо документально определить процедуры регулярной проверки (с документальной фиксацией результатов) в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки (с документальной фиксацией результатов) — при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии.

2.1.7. Все работники Компании должны давать письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов.

2.1.8. При взаимодействии с внешними организациями и клиентами требования по обеспечению ИБ должны регламентироваться положениями, включаемыми в договоры (соглашения) с ними.

2.1.9. Обязанности персонала по выполнению требований по обеспечению ИБ должны включаться в трудовые контракты (соглашения, договоры) и (или) должностные

инструкции.

2.1.10. Невыполнение работниками Компании требований по обеспечению ИБ должно приравниваться к невыполнению должностных обязанностей и приводить как минимум к дисциплинарной ответственности.

2.2. Общие требования по обеспечению информационной безопасности ИС на стадиях жизненного цикла

2.2.1. При формировании требований по обеспечению ИБ рассматриваются следующие общие стадии модели ЖЦ ИС:

1) разработка технических заданий;
2) проектирование;
3) создание и тестирование;
4) приемка и ввод в действие;
5) эксплуатация;
6) сопровождение и модернизация;
7) снятие с эксплуатации.

В случае самостоятельной разработки ИС в Компании рекомендуется рассматривать все стадии ЖЦ ИС, а в случае внедрения готовых ИС рекомендуется рассматривать стадии 4—7 ЖЦ ИС.

2.2.2. Разработка технических заданий и приемка ИС должны осуществляться по согласованию и при участии подразделения (лиц) в Компании, ответственного за обеспечение ИБ.

2.2.3. Ввод в действие, эксплуатация и сопровождение (модернизация), снятие с эксплуатации ИС должны осуществляться под контролем подразделения (лиц) в организации, ответственного за обеспечение ИБ.

2.2.4. Привлекаемые для разработки и (или) производства средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ. При заключении договоров в них должны включаться согласованные политики информационного взаимодействия.

2.2.5. Разрабатываемые ИС и (или) их компоненты должны быть снабжены документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз Компании. Приобретаемые Компанией готовые ИС и (или) их компоненты рекомендуется снабжать указанной документацией.

Также документация на разрабатываемые ИС или приобретаемые готовые ИС и их компоненты должна содержать описание реализованных защитных мер, предпринятых разработчиком относительно безопасности разработки и безопасности поставки.

В договор (контракт) о разработке ИС или поставке готовых ИС и их компонентов должны включаться положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных положений должен быть приобретен полный комплект рабочей конструкторской документации, обеспечивающий возможность сопровождения ИС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости или позиции фирмы-поставщика (разработчика), руководство необходимо оценить и документально оформить допустимость риска нарушения ИБ, возникающего при невозможности сопровождения ИС и их компонентов.

2.2.6. При разработке технических заданий на системы дистанционного обслуживания должно

быть учтено, что защита данных должна обеспечиваться в условиях:

- попыток доступа к защищаемой информации анонимных, неавторизованных злоумышленников при использовании сетей общего пользования;
- возможности ошибок авторизованных пользователей систем;
- возможности ненамеренного или неадекватного использования конфиденциальных данных авторизованными пользователями.

2.2.7. На стадии тестирования должны обеспечиваться анонимность данных, и проверка адекватности разграничения доступа.

2.2.8. На стадии эксплуатации ИС должны быть документально определены и выполняться процедуры контроля работоспособности (функционирования, эффективности) реализованных в ИС защитных мер. Результаты выполнения контроля должны документироваться.

2.2.9. На стадии сопровождения (модернизации) должны быть документально определены и выполняться процедуры контроля, обеспечивающие защиту от:

- умышленного несанкционированного раскрытия, модификации или уничтожения информации;
- неумышленной модификации, раскрытия или уничтожения информации;
- отказа в обслуживании или ухудшения обслуживания.

Результаты выполнения контроля должны документироваться.

2.2.10. На стадии сопровождения (модернизации) при любом внесении изменения в ИС должны проводиться процедуры проверки функциональности, результаты которой должны документально фиксироваться.

2.2.11. На стадии снятия с эксплуатации должны быть документально определены и выполняться процедуры, обеспечивающие удаление информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности Компании, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС и с внешних носителей, за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами. Результаты выполнения процедур должны документироваться.

2.3. Общие требования по обеспечению информационной безопасности при управлении доступом и регистрации

2.3.1. Должен быть документально определен перечень информационных активов (их типов) Компании. Права доступа работников и контрагентов Компании к данным активам должны быть документально зафиксированы.

2.3.2. В составе ИС должны применяться встроенные защитные меры, а также дополнительные (при необходимости) средства защиты информации от НСД.

2.3.3. Должны быть документально определены и утверждены руководством, выполняться и контролироваться следующие процедуры:

- идентификации;
- аутентификации;
- авторизации;
- управления доступом;

- контроля целостности;
- регистрации событий и действий пользователей.

Процедуры управления доступом должны исключать возможность «самосанкционирования». Результаты контроля процедур должны документироваться.

2.3.4. Необходимо документально определить процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные действия. Для проведения процедур мониторинга и анализа данных регистрации, действий и операций рекомендуется использовать специализированные программные и (или) технические средства.

Процедуры мониторинга и анализа должны использовать документально определенные критерии выявления неправомерных или подозрительных действий. Указанные процедуры мониторинга и анализа должны применяться на регулярной основе, например, ежедневно, ко всем выполненным операциям и транзакциям.

2.3.5. Порядок доступа работников Компании в помещения, в которых размещаются объекты информационных активов, должен быть регламентирован во внутренних документах, а его выполнение должно контролироваться.

Результаты контроля выполнения порядка доступа должны оформляться документально.

2.3.6. Используемые в Компании ИС, в том числе системы дистанционного обслуживания, должны обеспечивать среди прочего возможность регистрации:

- операций с данными;
- проводимых транзакций, имеющих финансовые последствия;
- операций, связанных с назначением и распределением прав пользователей.

2.3.7. Системы дистанционного обслуживания должны реализовывать защитные меры, обеспечивающие невозможность отказа от авторства проводимых операций и транзакций, например, многофакторная аутентификация или использование электронной подписи.

Протоколам операций, выполняемых посредством систем дистанционного обслуживания, рекомендуется придать свойство юридической значимости, например, путем внесения соответствующих положений в договоры на дистанционное обслуживание.

2.3.8. При заключении договоров со сторонними организациями рекомендуется юридическое оформление договоренностей, предусматривающих необходимый уровень взаимодействия, в случае выхода инцидента ИБ за рамки отдельной Компании.

2.3.9. Должны быть документально оформлены и доведены до сведения работников и клиентов Компании процедуры, определяющие действия в случае компрометации информации, необходимой для их идентификации, аутентификации и (или) авторизации, в том числе произошедшей по их вине, включая информацию о способах распознавания таких случаев.

Эти процедуры должны предусматривать документирование работниками и клиентами всех своих действий и их результатов.

2.3.10. В системах дистанционного обслуживания должны быть реализованы механизмы информирования (регулярного, непрерывного или по требованию) обо всех совершаемых операциях.

2.3.11. Должны применяться защитные меры, направленные на обеспечение защиты от несанкционированного доступа (далее – НСД), повреждения или нарушения целостности

информации, необходимой для регистрации, идентификации, аутентификации и (или) авторизации контрагентов и работников Компании. Все попытки НСД к такой информации должны регистрироваться. При увольнении или изменении должностных обязанностей работников Компании, имевших доступ к указанной информации, необходимо выполнить документированные процедуры соответствующего пересмотра прав доступа.

2.3.12. Работа всех пользователей ИС должна осуществляться под уникальными учетными записями.

2.4. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты

2.4.1. На всех автоматизированных рабочих местах, серверах ИС Компании и средствах контроля трафика сети Интернет, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты.

Процедуры установки, настройки и регулярного обновления средств антивирусной защиты (версий и баз данных) должны быть документированы и осуществляться администраторами ИС или иными официально уполномоченными лицами.

Рекомендуется организовать автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных.

Установка и обновление антивирусных средств должны контролироваться представителями подразделения (лицами) в организации, ответственными за обеспечение ИБ.

2.4.2. Должны быть разработаны и введены в действие инструкции по антивирусной защите.

2.4.3. Должна быть организована антивирусная фильтрация всего трафика электронного почтового обмена.

Рекомендуется организовать построение эшелонированной централизованной системы антивирусной защиты, предусматривающей использование средств антивирусной защиты различных производителей и их раздельную установку на рабочих станциях, почтовых серверах и межсетевых экранах.

2.4.4. Должны быть документально определены и выполняться процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка. Результаты установки, изменения программного обеспечения и антивирусной проверки должны документироваться.

2.4.5. Должны быть документально определены процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, необходимо зафиксировать:

- необходимые меры по отражению и устранению последствий вирусной атаки;
- порядок официального информирования руководства;
- порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки).

2.4.6. Должны быть документально определены и выполняться процедуры контроля за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах ИС. Результаты контроля должны документироваться.

2.4.7. Ответственность за выполнение требований по антивирусной защите должна быть возложена на руководителя функционального подразделения Компании, а обязанности по

выполнению предписанных мер антивирусной защиты должны быть возложены на каждого работника организации, имеющего доступ к АРМ и (или) ИС.

2.5. Общие требования по обеспечению информационной безопасности при использовании сети Интернет

2.5.1. Решение об использовании сети Интернет для производственной и (или) собственной хозяйственной деятельности должно документально приниматься руководством Компании и внутри отдельных подразделений руководителями подразделений. При этом цели использования сети Интернет должны быть явно перечислены, например, сеть Интернет в Компании/подразделении может использоваться для:

- ведения дистанционного обслуживания;
- получения и распространения информации, связанной с производственной деятельностью;
- информационно-аналитической работы в интересах Компании;
- обмена электронными сообщениями, например, почтовыми.

Использование сети Интернет в неустановленных целях должно быть запрещено.

С целью ограничения использования сети Интернет в неустановленных целях рекомендуется провести выделение ограниченного числа пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей. Наделение работников Компании правами пользователя конкретного пакета должно оформляться документально и выполняться в соответствии с его должностными обязанностями, в частности, в соответствии с назначенными ему ролями.

2.5.2. Должен быть документально определен порядок подключения и использования ресурсов сети Интернет, включающий в том числе положение о контроле со стороны подразделения (лиц) в организации, ответственного за обеспечение ИБ.

2.5.3. При необходимости осуществлять дистанционное использование ресурсов Компании, в связи с повышенными рисками нарушения ИБ при взаимодействии с сетью Интернет должны применяться средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

Рекомендуется выполнить выделение и организовать физическую изоляцию от внутренних сетей тех ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line.

2.5.4. При осуществлении дистанционного обслуживания должны применяться защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы. Все попытки таких подмен должны регистрироваться регламентированным образом.

2.5.5. Все операции пользователей в течение всего сеанса работы с системами дистанционного обслуживания должны выполняться только после выполнения процедур идентификации, аутентификации и авторизации. В случаях нарушения или разрыва соединения необходимо обеспечить повторное выполнение указанных процедур.

Для доступа пользователей к системам дистанционного обслуживания рекомендуется использовать многофакторную аутентификацию.

2.5.6. Почтовый обмен через сеть Интернет должен осуществляться с использованием защитных

мер. Перечень защитных мер и порядок их использования должны быть определены документально.

Рекомендуется организовать почтовый обмен с сетью Интернет через ограниченное количество точек, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации) почтовых серверов с безопасной системой репликации почтовых сообщений между ними (интернет-киоски).

2.5.7. Электронная почта должна архивироваться. Архив должен быть доступен подразделению (лицу) в организации, ответственному за обеспечение ИБ. Изменения в архиве не допускаются. Порядок доступа к информации архива должен быть документально определен.

2.5.8. Рекомендуется не применять практику хранения и обработки банковской информации (в т.ч. открытой) на ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line. Наличие банковской информации на таких ЭВМ должно определяться бизнес-целями Компании и документально санкционироваться руководством.

2.5.9. При взаимодействии с сетью Интернет должны быть документально определены и использоваться защитные меры противодействия атакам хакеров и распространению спама.

2.6. Общие требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации

2.6.1. Средства криптографической защиты информации, или шифровальные (криптографические) средства (далее — СКЗИ), предназначены для защиты информации при ее обработке, хранении и передаче по каналам связи.

Необходимость использования СКЗИ определяется самостоятельно, если иное не предусмотрено законодательством РФ.

Применение СКЗИ в Компании должно проводиться в соответствии с моделью угроз ИБ и моделью нарушителя ИБ, принятыми Компанией.

Рекомендуется утвердить частную политику ИБ, касающуюся применения СКЗИ в Компании.

СКЗИ, применяемые для защиты персональных данных, должны иметь класс не ниже КС2.

Работы по обеспечению с помощью СКЗИ безопасности информации проводятся в соответствии с действующими в настоящее время нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России.

2.6.2. Для обеспечения безопасности рекомендуется использовать СКЗИ, которые:

- допускают встраивание в технологические процессы обработки электронных сообщений, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;
- поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
- сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ России.

2.6.3. Установка и ввод в эксплуатацию, а также эксплуатация СКЗИ должны осуществляться в соответствии с эксплуатационной и технической документацией к этим средствам.

2.6.4. При применении СКЗИ должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющую собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

2.6.5. Информационная безопасность процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты.

2.6.6. Для повышения уровня безопасности при эксплуатации СКЗИ и их ключевых систем рекомендуется реализовать процедуры мониторинга, регистрирующего все значимые события, состоявшиеся в процессе обмена криптографически защищенными данными, и все инциденты ИБ.

2.6.7. Порядок применения СКЗИ определяется руководством Компании на основании указанных выше в данном разделе документов и должен включать:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой системой;
- порядок обращения с носителями ключевой информации, включая действия при смене и компрометации ключей.

2.7. Общие требования по обеспечению информационной безопасности информационных технологических процессов

2.7.1. Информационные технологические процессы должны быть документирован в Компании.

2.7.2. Должны быть документально определены:

- состав и схемы размещения и подключения аппаратных средств Компании (ЭВМ, серверов, сетевого и каналообразующего оборудования, АТС и т.п.);
- перечни программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и ИС и необходимого для выполнения конкретных информационных технологических процессов;
- состав информационных систем (их размещение, архитектура построения и т.п.);
- основные информационные потоки.

Выполнение данных требований должно документироваться, поддерживаться актуальным и контролироваться руководством Компании.

2.7.3. Порядок обмена информацией с контрагентами должен быть зафиксирован в договорах между участниками, осуществляющими обмен информацией.

2.7.4. Работники Компании, в том числе администраторы ИС и средств защиты информации, не должны обладать полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения информации, а также проведения несанкционированных операций.

2.7.5. Результаты технологических операций по обработке информации должны контролироваться (проверяться) и удостоверяться лицами/автоматизированными процессами.

Рекомендуется, чтобы обработку информации и контроль (проверку) результатов обработки осуществляли разные работники / автоматизированные процессы.

2.7.6. Обязанности по администрированию средств защиты информации рекомендуется возлагать приказом или распоряжением по Компании на администраторов ИБ с отражением этих обязанностей в их должностных инструкциях.

2.7.7. Комплекс мер по обеспечению ИБ должен предусматривать в том числе:

- защиту информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных сообщений;
- доступ работника Компании только к тем ресурсам, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения информации;
- аутентификацию входящих электронных сообщений;
- двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными сообщениями;
- возможность ввода информации в ИС только для авторизованных пользователей;
- восстановление информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов.

2.7.8. При проектировании, разработке и эксплуатации систем дистанционного обслуживания должны быть документально определены и выполняться процедуры, реализующие в том числе механизмы снижения вероятности выполнения непреднамеренных или случайных операций.

2.7.9. Клиенты систем дистанционного обслуживания должны быть обеспечены детальными инструкциями, описывающими процедуры выполнения операций.

2.7.10. Должны быть документально определены процедуры обслуживания средств вычислительной техники ИС, включая замену их программных и (или) аппаратных частей.

2.7.11. Должна осуществляться и быть регламентирована процедура периодического контроля всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ. Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в Компании за обеспечение ИБ.

2.7.12. Должна осуществляться и быть регламентирована процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ. Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в Компании за обеспечение ИБ.

2.7.13. В Компании необходимо провести классификацию информации.

Классификацию информации следует проводить в соответствии со степенью тяжести последствий потери ее свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности.

2.7.14. Для каждого из типов информационных активов (типов информации), полученных в результате классификации, должен быть документально определен набор требований по их защите.

2.7.15. Для каждой ИС должен быть документально определен порядок контроля ее функционирования со стороны лиц, отвечающих за ИБ.

2.7.16. Информационные технологические процессы должны быть документированы в Компании. Указанные документы должны быть согласованы со службой ИБ.

Указанные процессы должны быть реализованы в рамках, созданных для этих целей ИС.

Не входящие в состав данных ИС серверы, офисные ЭВМ и другое оборудование рекомендуется изолировать от ИС на уровне локальных вычислительных сетей способом, согласованным со службой либо лицом, отвечающим в организации за ИБ.

2.7.17. Должны быть документально определены перечни программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и ИС и необходимого для выполнения конкретных информационных технологических процессов. Состав установленного и используемого в ЭВМ и ИС программного обеспечения должен соответствовать определенному перечню.

Выполнение данных требований должно контролироваться с документированием результатов.

2.7.18. Должна быть регламентирована и осуществляться процедура периодического контроля всех реализованных программно-техническими средствами и организационными мерами функций (требований) по обеспечению ИБ.

Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в организации за ИБ.

2.7.19. Должна быть регламентирована и осуществляться процедура восстановления всех реализованных программно-техническими средствами и организационными мерами функций по обеспечению ИБ.

Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в организации за ИБ.

2.8. Общие требования по обработке персональных данных в Компании

2.8.1. Должны быть определены, документально зафиксированы и утверждены руководством Компании цели обработки персональных данных.

2.8.2. Должна быть определена необходимость уведомления Уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных.

2.8.3. Для каждой цели обработки персональных данных должны быть определены, документально зафиксированы и утверждены руководством Компании:

- объем и содержание персональных данных;
- сроки обработки, в том числе сроки хранения персональных данных;
- необходимость получения согласия субъектов персональных данных.

2.8.4. Рекомендуется использовать Обезличенные персональные данные. Процедуры обезличивания должны соответствовать рекомендациям по обезличиванию и быть документированы.

2.8.5. Рекомендуется проводить классификацию персональных данных в соответствии со степенью тяжести последствий потери свойств безопасности персональных данных для субъекта персональных данных.

Рекомендуется выделять следующие категории персональных данных:

- персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к специальным категориям персональных данных;
- персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к биометрическим персональным данным;
- персональные данные, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным;
- персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к общедоступным или обезличенным персональным данным.

2.8.6. Передача персональных данных Компанией третьему лицу должна осуществляться с согласия субъекта персональных данных за исключением случаев, предусмотренных законодательством РФ. В том случае, если Компания поручает обработку персональных данных третьему лицу на основании договора, существенным условием такого договора является обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

2.8.7. Компания должна прекратить обработку персональных данных и уничтожить собранные персональные данные, если иное не установлено законодательством РФ, в следующих случаях и в сроки, установленные законодательством РФ:

- по достижении целей обработки или при утрате необходимости в их достижении;
- по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных;
- если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с законодательством РФ;
- при невозможности устранения оператором допущенных нарушений при обработке персональных данных.

Должен быть определен и документально зафиксирован порядок уничтожения персональных данных (в том числе и материальных носителей персональных данных).

2.8.8. Должен быть определен и документально зафиксирован порядок обработки обращений субъектов персональных данных (или их законных представителей) по вопросам обработки их персональных данных.

2.8.9. Должен быть определен и документально зафиксирован порядок действий в случае запросов Уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных.

2.8.10. Должен быть определен и документально зафиксирован подход к отнесению ИС к информационным системам персональных данных (ИСПДн).

2.8.11. Должен быть определен и документально зафиксирован перечень ИСПДн. В перечень ИСПДн должны быть включены как минимум ИС, целью создания и использования которых является обработка персональных данных.

2.8.12. Для каждой ИСПДн должны быть определены и документально зафиксированы:

- цель обработки персональных данных;
- объем и содержание обрабатываемых персональных данных;
- перечень действий с персональными данными и способы их обработки.

Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать целям обработки. В том случае, если для выполнения информационного технологического процесса, реализацию которого поддерживает ИСПДн, нет необходимости в обработке определенных персональных данных, эти персональные данные должны быть удалены.

2.8.13. Информационные технологические процессы, в рамках которых обрабатываются персональные данные в ИСПДн, должны быть документированы.

При этом рекомендуется исключать фиксацию на одном материальном носителе и персональных данных, и иных видов информационных активов, а также персональных данных, цели обработки которых заведомо несовместимы.

При обработке различных категорий персональных данных для каждой категории персональных данных рекомендуется использовать отдельный материальный носитель.

2.8.14. Должен быть определен и документально зафиксирован перечень (список) работников (ролей), осуществляющих обработку персональных данных в ИСПДн либо имеющих доступ к персональным данным.

Доступ работников Компании к персональным данным, и обработка персональных данных работниками Компании должны осуществляться только для выполнения их должностных обязанностей.

2.8.15. Работники Компании, осуществляющие обработку персональных данных в ИСПДн, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности персональных данных в части, касающейся их должностных обязанностей.

2.8.16. Должен быть определен и документально зафиксирован порядок доступа работников Компании и иных лиц в помещения, в которых ведется обработка персональных данных.

2.8.17. Должен быть определен и документально зафиксирован порядок хранения материальных носителей персональных данных, устанавливающий:

- места хранения материальных носителей персональных данных;
- требования по обеспечению безопасности персональных данных при хранении их носителей;
- работников, ответственных за реализацию требований по обеспечению безопасности персональных данных;
- порядок контроля выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных.

2.8.18. При обработке персональных данных на бумажных носителях, в частности, при использовании в Компании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования, установленные «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15 сентября 2008 г. № 687.

2.8.19. Требования по обеспечению безопасности персональных данных при их обработке в ИСПДн определяются для каждого класса ИСПДн на основе требований Приказа ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. История изменений

№	Дата	Версия	Предмет изменений	Автор
1.				
2.				
3.				