# Концепция и Политика информационной безопасности

# Обзор

1. Зачем нужна политика безопасности
2. Цели политики безопасности
3. Формирование политики безопасности
4. Характеристики и компоненты политики безопасности
5. Методы обеспечения информационной безопасности. Классификация методов защиты
6. Базовые принципы политики информационной безопасности
7. Конфигурация сети и услуг
8. Структура документа «Концепция информационной безопасности»

# *Зачем нужна политика безопасности*

Решения, сопряженные с безопасностью определяют в заметной мере, *насколько безопасна* ваша сеть, какой *уровень функциональности* может она предложить, и *насколько легко работать* в этой сети. Однако вы не можете принять хорошее решение, касающиеся безопасности, без определения того, каковы ваши *конечные цели*. Пока вы не определите, каковы ваши цели обеспечения безопасности, вы не можете эффективно использовать любую комбинацию средств, так как вы не знаете, что проверять и какие ограничения ввести. Например, ваши цели будут, вероятно, сильно отличаться от целей поставщика продукта. Поставщики пытаются сделать конфигурирование и работу продукта как можно проще, это предполагает, что конфигурация по умолчанию будет максимально открытой (т. е., небезопасной). В то время как это облегчает инсталляцию новых продуктов, такой подход оставляет свободным доступ к этим системам и через них к другим системам.

Ваши цели будут в основном определены следующими ключевыми компромиссами:

- ***предлагаемые услуги против предоставляемой безопасности*** - каждая услуга, предлагаемая пользователям, несет в себе определенные риски безопасности. Для некоторых услуг риск перевешивает привлекательные их стороны, и администратор может принять решение их запретить, а не защищать;
- ***простота использования против безопасности*** - простейшая система использования позволит доступ любому пользователю и не потребует пароля; то есть, лишена какой-либо безопасности. Требование пароля делает систему менее удобной, но более безопасной. Требование одноразового пароля, формируемого аппаратно еще менее удобно для использования, но много безопаснее;

# *Зачем нужна политика безопасности*

- ***стоимость безопасности против риска потери*** - существует много различных издержек безопасности: денежные (т. е., цену покупки оборудования и программ, обеспечивающих безопасность, например, firewall и генератора одноразовых паролей), рабочие характеристики (т. е., время необходимое для шифрования и дешифрования), а также простота использования (как упомянуто выше). Существует также много уровней риска: потеря конфиденциальности (т. е., чтение информации неавторизованными лицами), потеря данных (т. е., искажение или стирание информации), и потеря услуги (например, заполнение памяти, использование вычислительных ресурсов, и отказ в доступе к сети). Каждый тип издержек должен быть оценен и сопоставлен каждым типом потерь.

Эти цели следует довести до сведения всех пользователей, оперативного персонала и менеджеров в виде *набора правил безопасности*, называемых "политикой безопасности". Здесь использован этот термин, а не более близкое выражение "политика компьютерной безопасности", так как данная сфера включает в себя все типы информационных технологий и информацию, хранимую и обрабатываемую этой технологией.

Политика безопасности является формальным объявлением правил, которым должны подчиняться лица, получившие доступ к технологии и информации организации.

# *Цели политики безопасности*

Политика безопасности оформляется в виде *концепции информационной безопасности* информационных ресурсов компании, а также схем безопасности сетевого комплекса.

Главной целью политики безопасности является информирование пользователей, персонала и менеджеров об их обязанностях по защите технологии и информации. Политика должна специфицировать механизмы, через которые могут быть реализованы соответствующие требования.

Другой целью является обеспечение базиса при конфигурировании и аудите компьютерных систем и сетей в соответствии с политикой. Следовательно, попытка использовать набор средств безопасности в отсутствии определенной политики безопасности является бессмысленным.

Политика использования AUP (Appropriate Use Policy) может также быть частью политики безопасности. Она должна определять, что можно и чего нельзя делать с различными компонентами системы, включая типы трафика, разрешенные в сетях. AUP должна быть максимально прозрачной (заданной явно), чтобы избежать неопределенности и недоразумений. Например, AUP может перечислить какие-то запрещенные группы новостей USENET. (Заметим: AUP для некоторых узлов является приемлемой политикой использования (Acceptable Use Policy)).

# *Формирование политики безопасности*

Для того чтобы политика безопасности была адекватной и эффективной, она должна быть приемлемой и поддерживаемой на всех уровнях для сотрудников организации. Особенно важно, чтобы корпоративный менеджмент безоговорочно поддерживал политику безопасности. Ниже представлен список лиц, которые должны быть вовлечены в создание и подготовку документов по политике безопасности:

1) администратор безопасности компании (узла);
2) технический персонал информационной технологии (например, персонал вычислительного центра);
3) администраторы больших групп пользователей организации (например, коммерческие подразделения, отдел компьютерной информатики в университете и т. д.);
4) команда ликвидации инцидентов нарушения безопасности;
5) представители групп пользователей, имеющие отношения к политике безопасности;
6) ответственные управленцы;
7) юрист (если таковой имеется).

Выше в списке приведены представители многих организаций, но перечень не является исчерпывающим. Идея заключается во включении в список ключевых лиц, работающих в сети и имеющих распорядительные функции, лица, определяющие политику, технический персонал, кто знает основные разветвления политического выбора. В некоторых организациях, может быть разумным включить персонал EDP-аудита. Включение этой группы является важным, если результирующие политические заявления должны быть восприняты как можно более широким кругом лиц. Роль юриста может сильно варьироваться от страны к стране.

# *Характеристики и компоненты политики безопасности*

Характеристиками хорошей политики безопасности являются:

- она должна быть реализуема через процедуры системной администрации, публикацию приемлемых руководств по использованию, или другими приемлемыми способами;
- она должна быть, где возможно, внедряема посредством специальных устройств и программ и через санкции, где предотвращение угроз технически невозможно;
- она должна ясно определять области ответственности пользователей, администраторов и менеджмента.

Хорошая политика безопасности включает в себя следующие компоненты:

- инструкции по технологии приобретения компьютерного оборудования, которые разъясняют требования или предпочтения, связанные с безопасностью. Эта инструкция должна прилагаться к существующим рекомендациям по закупкам и закупочной политике;
- политику конфиденциальности, которая определяет разумные требования по обеспечению закрытости частной информации, включая мониторинг электронной почты, контроль операций, выполняемых пользователями и доступ к их файлам;

# *Характеристики и компоненты политики безопасности*

- политику доступа, которая определяет права доступа и привилегии с целью защиты определенных объектов от утраты или раскрытия для пользователей оперативного персонала и менеджмента. Она должна предоставить инструкции для внешнего подключения, передачи данных, устройств подключения к сети и для добавления нового программного обеспечения к системе. Она должна также специфицировать любые необходимые сообщения уведомления (например, сообщения подключения должны предоставлять предупреждения об авторизованном использовании и мониторинге канала, а не просто выдавать строку типа "Welcome");
- политику аккаунтинга, которая определяет ответственность пользователей, операционного персонала и менеджмента. Она должна специфицировать возможность аудита и предоставлять инструкции обработки инцидентов (т.е., что делать и с кем связаться, если зарегистрировано вторжение);
- политику аутентификации, которая устанавливает эффективную политику паролей и устанавливает инструкции для удаленной аутентификации и использования аутентификационных устройств (например, одноразовых паролей и устройств их генерирующих);
- заявление доступности, которое устанавливает пожелания пользователей о доступности определенных ресурсов. Оно должно относиться к избыточности и восстановлению объектов, а также специфицировать часы работы и периоды остановок для обслуживания. Оно должно также включать контактную информацию для информирования о состоянии системы и об отказах;

# *Характеристики и компоненты политики безопасности*

- политику поддержки сети и информационных систем, которая описывает, как персоналу, отвечающему за поддержку внутренней сети и внешних каналов, разрешено использовать технологию доступа. Важный вопрос, который здесь должен быть задан, заключается в том, должен ли быть разрешен внешний доступ и как такой доступ следует контролировать. Другой областью, рассматриваемой здесь, является организация работ с субподрядными фирмами и способ ее управления;
- политику сообщений о нарушениях, которая указывает, какой тип нарушений (например, конфиденциальности и безопасности, внутренней или внешней) должен докладываться и кто готовит такие доклады. Доброжелательная атмосфера и возможность анонимного доклада приведет к тому, что вероятность сообщения в случае нарушения будет выше;
- поддерживающую информацию, которая предоставляет пользователям, персоналу и менеджменту контактные данные для каждого типа нарушений политики безопасности; инструкции о том, как обрабатывать внешние запросы об инцидентах, сопряженных с нарушением безопасности, или информацию, которая может рассматриваться как конфиденциальная или частная; и перекрестные ссылки на процедуры безопасности и сопряженную с ними данные, такие как политика компании и правительственные законы и постановления.

# *Характеристики и компоненты политики безопасности*

Могут существовать регулирующие требования, которые влияют на некоторые аспекты вашей политики безопасности (например, мониторирование линий). Создатели политики безопасности должны рассматривать возможности сотрудничества в ее формировании. Как минимум, политика должна быть рассмотрена юристом.

Раз ваша политика безопасности установлена, она должна быть четко доведена до сведения пользователей, персонала и менеджмента. Важной частью процесса является подписание всем персоналом регулирующего безопасность документа, которое указывает, что люди читали, поняли и согласны с требованиями политики там содержащимися. Наконец, ваша политика должна рассматриваться на регулярной основе с целью выяснения того, поддерживает ли она эффективно требования безопасности.

Для того чтобы политика безопасности была жизнеспособна в долгосрочном плане, она требует большой доли *гибкости*, основанной на концепции архитектурной безопасности. Политика безопасности должна быть по большей части независимой от специфического оборудования и программного обеспечения. Механизмы актуализации политики должны быть четкими и понятными. Это включает процесс, вовлеченных людей и лиц, кто должен реализовать изменения.

Всякий раз, когда возможно, политика должна разъяснять, какие *исключения* существуют для общей политики. Например, при каких условиях системному администратору позволено просматривать файлы пользователя. Могут также существовать случаи, когда несколько пользователей имеют доступ к одному и тому же идентификатору userid. Например, в системах с пользователем **root**, несколько системных администраторов могут знать пароль и использовать аккаунт root.

# *Методы обеспечения информационной безопасности. Классификация методов защиты*

**Обеспечение информационной безопасности** — это деятельность, направленная на достижение состояния защищенности (целостности, конфиденциальности и доступности) информационной среды, а также на прогнозирование, предотвращение и смягчение последствий любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Сегодня существует большой арсенал методов обеспечения информационной безопасности, к которым мы, прежде всего, отнесем *технические средства защиты*, такие как системы шифрования, аутентификации, авторизации, аудита, антивирусной защиты, межсетевые экраны и др.

Однако помимо технических средств, не меньшее, а иногда и большее влияние на безопасность системы оказывают средства, построенные на качественно другой основе. К таким «не техническим» мерам защиты относятся соответствующие *сфера законодательства, морально-этические нормы, просветительная работа и административные меры*. Например, именно ужесточением наказаний за преступления в области нарушения информационной безопасности эксперты объясняют резкое снижение за последние два года количества вирусных атак. Примером эффективных административных мер может служить запрет сотрудникам пользоваться в пределах предприятия собственными ноутбуками; такой запрет сокращает случаи утечки конфиденциальной информации и заражения корпоративных данных новыми вирусами.

# *Методы обеспечения информационной безопасности. Классификация методов защиты*

Важную роль играют также, *физические средства защиты*, к которым относят замки, камеры наблюдения, охранные системы. Данные, записанные на съемный носитель, помещенный в сейф в хорошо охраняемом помещении, очевидно, более защищены, чем данные, хранящиеся на диске работающего в сети компьютера, защищенного самым совершенным сетевым экраном.

Универсальным средством противодействия атакам, имеющим целью нарушение целостности данных, а в некоторых случаях и их доступности, является резервное копирование. **Резервное копирование** — это набор автоматизированных процедур создания и поддержания копий данных, которые могут быть использованы для восстановления исходных данных в случае их потери или искажения. Резервные копии записывают на сменные носители большой емкости, например магнитные ленты, которые для повышения отказоустойчивости размещают в местах, территориально разнесенных с местонахождением исходных данных. Понятно, что при этом возрастает вероятность их потери или кражи. Чтобы смягчить возможные последствия этих угроз, копируемые данные записываются на сменные носители в зашифрованном виде.

Для эффективного поддержания информационной безопасности необходим *системный подход*. Это означает, что различные средства защиты (технические, юридические, административные, физические и т. д.) должны применяться совместно и под централизованным управлением.

# *Базовые принципы политики информационной безопасности*

Одним из таких принципов является предоставление каждому сотруднику предприятия того *минимального уровня привилегий* на доступ к данным, который необходим ему для выполнения его должностных обязанностей.

Следующий принцип — использование *многоуровневого подхода* к обеспечению безопасности. Система защиты с многократным резервированием средств безопасности увеличивает вероятность сохранности данных. Так, например, физические средства защиты (закрытые помещения, блокировочные ключи), ограничивающие непосредственный контакт пользователя только приписанным ему компьютером, дополняют и усиливают эффективность централизованной системы авторизации пользователей.

Принцип *единого контрольно-пропускного пункта* заключается в том, что весь входящий во внутреннюю сеть и выходящий во внешнюю сеть трафик проходит через единственный узел сети, например через сетевой экран. Только это позволяет в достаточной степени контролировать трафик. В противном случае, когда в сети имеется множество пользовательских станций, имеющих независимый выход во внешнюю сеть, очень трудно скоординировать правила, ограничивающие права пользователей внутренней сети на доступ к серверам внешней сети и обратно — права внешних клиентов на доступ к ресурсам внутренней сети.

# *Базовые принципы политики информационной безопасности*

Используя многоуровневую систему защиты, важно обеспечивать *баланс надежности защиты всех уровней*. Если в сети все сообщения шифруются, но ключи легкодоступны, то эффект от шифрования нулевой. Если внешний трафик сети, подключенной к Интернету, проходит через мощный сетевой экран, но пользователи имеют возможность связываться с узлами Интернета по коммутируемым линиям через локально установленные модемы, то деньги (как правило, немалые), потраченные на сетевой экран, можно считать выброшенными на ветер.

Следующим универсальным принципом является использование только таких средств, которые при отказе переходят в состояние *максимальной защиты*. Это касается самых различных средств безопасности. Если в сети имеется устройство, которое анализирует весь входной трафик и отбрасывает кадры с определенным, заранее заданным обратным адресом, то при отказе оно должно полностью блокировать вход в сеть. Неприемлемым следовало бы признать устройство, которое при отказе просто отключается, начиная пропускать в сеть весь внешний трафик.

Следующим является принцип *баланса возможного ущерба от реализации угрозы и затрат на ее предотвращение*. Ни одна система безопасности не гарантирует защиту данных на уровне 100 %, поскольку является результатом компромисса между возможными рисками и возможными затратами. Определяя политику безопасности, администратор должен взвесить величину ущерба, которую может понести предприятие в результате нарушения защиты данных, и соотнести ее с величиной затрат, требуемых на обеспечение безопасности этих данных. Так, в некоторых случаях можно отказаться от дорогостоящего межсетевого экрана в пользу стандартных средств фильтрации обычного маршрутизатора, в других же приходится идти на беспрецедентные затраты. Главное, чтобы принятое решение было обосновано экономически.

## Защита инфраструктуры

Многие сетевые администраторы готовы идти на большие издержки, чтобы защитить ЭВМ их сети. Немногие администраторы делают что-либо, чтобы защитить сами сети. К этому есть определенные предпосылки. Например, ЭВМ защитить много легче чем сеть. Кроме того, атакеров скорее интересуют конкретные машины, а нанесение ущерба сети в их планы не входит. Тем не менее, существуют причины защиты сетей. Например, атакер может перенаправить сетевой трафик через ЭВМ вне сети, чтобы просмотреть интересующие его данные (например, перехватить пароли). Инфраструктура включает в себя сетевое управление (например, SNMP), услуги (например, DNS, NFS, NTP, WWW) и безопасность (т.е., аутентификация пользователей и ограничения доступа).

Инфраструктура также нуждается в защите от человеческих ошибок. Когда администратор неверно конфигурирует ЭВМ, сервис, предоставляемый машиной, может деградировать. Это существенно только для пользователей этой ЭВМ, если только эта машине не является первичным сервером, число пострадавших пользователей при этом ограничено. Однако если маршрутизатор некорректно сконфигурирован, все пользователи, кто нуждается в доступе к сети, пострадают. Очевидно, что число пользователей несравненно большее, чем число людей, зависящих от услуг одной ЭВМ.

## Защита сети

Существует несколько проблем, которые актуальны для сетей. Классической проблемой является атака "denial of service" (отказ в обслуживании). В этом случае, сеть попадает в состояние, при котором она не может более передавать данные пользователя. Существует два способа реализации такого состояния: путем атаки маршрутизаторов и с помощью перегрузки сети избыточным трафиком. Заметим, что термин маршрутизатор в этом разделе используется как активное сетевое устройство самого широкого класса, сюда могут относиться сетевые экраны (firewall), прокси-серверы, и т. д.

Атака на маршрутизатор заключается в блокировке им передачи пакетов или в переадресации их некорректным образом. В первом случае может иметь место не верная конфигурация, произвольная *модификация маршрутной таблицы*, или "атака перегрузки" (т.е., маршрутизатор забрасывается немаршрутизуемыми пакетами, что вызывает деградацию его рабочих характеристик). Атака перегрузки на сеть аналогична подобной атаке на маршрутизатор, за исключением того, что пакеты являются обычно широковещательными. Идеальной атакой перегрузки являлась бы такая, при которой посылка одного пакета, использующего известную уязвимость, вызывала посылку лавины пакетов.

Другой классической проблемой является фальсификация (spoofing). В этом случае маршрутизатору посылается запрос произвольной модификации маршрутов, заставляя его послать одному или нескольким маршрутизаторам данные, искажающие маршрутизацию пакетов. Это отличается от атаки отказа обслуживания только целью модификации маршрута. При отказе обслуживания, целью является выведение из строя маршрутизатора; что будет быстро замечено пользователями сети. При фальсификации, ложный путь вынудит пакеты двигаться к ЭВМ, где атакер мониторирует передаваемую информацию. Эти пакеты переадресуются затем по их правильному месту назначения. Однако атакер может менять или не менять при этом содержимое пакетов.

Решением большинства этих проблем является предотвращение посылки пакетов модификации маршрутов протоколами маршрутизации (например, RIP-2, OSPF). Существует три уровня защиты: пароль с открытым текстом, криптографическая контрольная сумма и шифрование. Пароли предоставляют минимальную защиту от атакеров, которые не имеют непосредственного физического доступа к сети. Пароли также предлагают некоторую защиту от некорректного конфигурирования маршрутизаторов. Преимуществом паролей является малая избыточность в отношении полосы и ресурсов CPU. Контрольные суммы защищают от присылки ложных пакетов, даже в случае, когда атакер имеет физический доступ к сети. В сочетании с номером по порядку или другим уникальным идентификатором контрольная сумма может защитить также от атак "откликов", когда атакером или “сошедшим с ума” маршрутизатором повторно присылается старое (но корректное) обновление маршрута. Большая безопасность достигается пересылкой закодированной маршрутной информации. Это мешает атакеру определить топологию сети. Недостатком шифрования является избыточность, связанная с обработкой зашифрованных сообщений.

RIP-2 (RFC 1723) и OSPF (RFC 1583) оба поддерживают пароли с открытым текстом в своей основной спецификации. Кроме того, существует расширения этих базовых протоколов, поддерживающие MD5-шифрование.

К сожалению, не существует приемлемой защиты от атак перегрузки (flooding), или некорректного поведения ЭВМ или маршрутизатора, перегружающих сеть. К счастью, этот тип атак является очевидным и по этой причине хорошо диагностируемым и устраняемым.

**Защита услуг**

Существует много типов услуг и каждая из них имеет свой уровень требований безопасности. Эти требования будут варьироваться в зависимости от назначения услуги. Например, услуга, которая предназначена для применения исключительно внутри узла (например, NFS) может требовать механизмов защиты, отличных от используемых в случае внешних приложений. Может быть достаточно защитить внутренний сервер от внешнего. Однако, WWW-сервер, который должен быть доступен из любой точки Интернет, требует встроенной защиты. То есть, сервис/протокол/сервер должны обеспечивать любую безопасность, необходимую для предотвращения неавторизованного доступа и модификации базы данных Web.

# *Конфигурация сети и услуг*

Внутренние услуги (т. е., услуги, используемые в пределах узла) и внешние услуги (т. е., услуги, преднамеренно сделанные доступными для пользователей за пределами узла) будут, вообще говоря, иметь требования безопасности, которые существенно отличаются. Следовательно, разумно ограничить внутренние услуги набором ЭВМ, подключенных к серверу, а внешние услуги должны быть доступны на других серверах. То есть, внутренние и внешние серверы не должны размещаться на одном и том же компьютере. Фактически, многие узлы имеют один набор субсетей (или даже сетей), которые доступны извне, и другой набор, который доступен изнутри. Эти две области соединяются через firewall. Должно уделяться большое внимание для обеспечения корректной работы такого firewall.

Усиливается интерес к использованию Интранет для соединения различных частей организации (например, отделения компании). В то время как данный документ делает четкое различие между внешними и внутренними частями (общедоступные и частные), узлы, использующие Интранет, должны позаботиться о рассмотрении трех зон и предпринять соответствующие действия, проектируя сеть и предоставляя услуги. Услуга, предлагаемая в Интранет, не является ни общедоступной, ни в полной мере частной. Следовательно, услуга требует своей собственной системы поддержки, отделенной от внешних и внутренних услуг и сетей.

# *Конфигурация сети и услуг*

Один вид внешних услуг достоин специального рассмотрения, это анонимный или гостевой доступ. Это может быть анонимное FTP или гостевой (не аутентифицированный) login. Особенно важно гарантировать, чтобы анонимные серверы FTP и гостевые аккаунты были тщательно изолированы от любых ЭВМ и файловых систем, куда не следует пускать внешних пользователей. Другой областью специального внимания должен быть анонимный доступ с возможностью записи. Узел может быть юридически ответственен за общедоступную информацию, поэтому рекомендуется мониторировать данные, заносимые анонимными пользователями.

В дальнейшем будут рассмотрены некоторые наиболее популярные услуги: служба имен, служба паролей/ключей, служба аутентификации, электронная почта, WWW, пересылка файлов и NFS. Так как эти услуги наиболее часто используются, они являются объектами атак. Успешная атака на одну из услуг может привести к катастрофе всей системы в целом.

# *Структура документа «Концепция информационной безопасности»*

## 1. Введение

Настоящая Концепция информационной безопасности (далее – Концепция) является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности (далее – ИБ) компании…

Необходимость разработки Концепции обусловлена расширением сферы применения новейших информационных технологий и процессов при обработке информации.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (далее – СЗПДн) в _____. Концепция определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня защищенности для автоматизированных информационных систем (далее - ИС) в _____.

Концепция разработана в соответствии с системным подходом к обеспечению ИБ. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз ИБ и разработку СЗПДн с позиции комплексного применения технических и организационных мер и средств защиты.

Под ИБ _____ понимается защищённость информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в том числе персональные данные (далее – информация) и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам (субъектам) или инфраструктуре. Задачи ИБ сводятся  минимизации ущерба от возможной реализации угроз безопасности информации, а также к прогнозированию и предотвращению таких воздействий.

# *Структура документа «Концепция информационной безопасности»*

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению ИБ в _____, а также нормативных и методических документов, обеспечивающих её реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности информации в _____;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности, и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз;
- координации деятельности структурных подразделений при проведении работ по развитию и эксплуатации ИС с соблюдением требований обеспечения безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности в ИС.

Область применения Концепции распространяется на все подразделения _____, эксплуатирующие технические и программные средства ИС, в которых осуществляется автоматизированная обработка информации, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИС.

Правовой базой для разработки настоящей Концепции служат требования действующих в РФ законодательных и нормативных актов по вопросам информационной безопасности.

## 2. Общие положения

Система защиты персональных данных (СЗПДн) представляет собой совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ними.

Безопасность информации достигается путём исключения несанкционированного, в том числе случайного, доступа к ней, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий.

Структура, состав и основные функции СЗПДн определяются исходя из класса защищенности ИС и уровня значимости информации. СЗПДн включает в себя организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки информации), а также используемые в ИС информационные технологии.

Эти меры призваны обеспечить:

- конфиденциальность информации;
- целостность информации;
- доступность информации

Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИС, разработку технического (частного технического) задания на создание СЗПДн;
- стадия проектирования и реализации СЗПДн, включающая разработку Технического проекта на построение системы защиты информации;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приёмо-сдаточные испытания СЗПДн, а также оценку соответствия ИС требованиям ИБ.

Организационные меры предусматривают создание и поддержание правовой базы безопасности информации и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИС организационно- технические меры защиты реализуются при помощи соответствующих программно-технических средств защиты информации.

Перечень необходимых мер защиты информации определяется по результатам обследования ИС.

## 3. Задачи СЗПДн

Основной целью создания СЗПДн является минимизация ущерба от возможной реализации угроз безопасности информации.

# Структура документа «Концепция информационной безопасности»

Для достижения основной цели система безопасности информации ИС должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИС посторонних лиц (возможность использования ИС и доступ к её ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИС для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:
- к информации, циркулирующей в ИС;
- средствам вычислительной техники ИС;
-аппаратным, программным и криптографическим средствам защиты, используемым в ИС;
-регистрацию действий пользователей при использовании защищаемых ресурсов ИС в системных журналах и периодический контроль корректности действий пользователей системы путём анализа содержимого этих журналов;
-контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;
-защиту от несанкционированной модификации и контроль целостности используемых в ИС программных средств, а также защиту системы от внедрения несанкционированных программ;
-защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

-защиту информации, хранимую, обрабатываемую и передаваемую по каналам связи, от несанкционированного разглашения или искажения;
-обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
-своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба субъектам, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
-создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

## 4. Объекты защиты

### 4.1 Перечень информационных систем

В _____ производится обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

Перечень ИС, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, определяется на основании «Отчёта по результатам обследования».

### 4.2 Перечень объектов защиты

Объектами защиты являются информация, обрабатываемая в ИС, и технические средства ее обработки и защиты. Информации, подлежащая защите, определяется на основании «Отчёта по результатам обследования».

# *Структура документа «Концепция информационной безопасности»*

К объекты защиты относятся:

- обрабатываемая информация;
- технологическая информация;
- программно-технические средства обработки;
- средства защиты информации;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИС.

**5. Классификация пользователей ИС**

Пользователем ИС является лицо, участвующее в функционировании информационной системы или использующее результаты её функционирования. Также пользователем ИС является любой сотрудник _____, имеющий доступ к ИС и её ресурсам в соответствии с установленным порядком и в соответствии с его функциональными обязанностями.

Пользователи ИС делятся на три основные категории (роли).

1. Администратор ИС - сотрудники _____, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИС обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном ПО ИС;
- обладает полной информацией о технических средствах и конфигурации ИС;
- имеет доступ ко всем техническим средствам обработки информации и данным ИС;
- обладает правами конфигурирования и административной настройки технических средств ИС.

# *Структура документа «Концепция информационной безопасности»*

2. Разработчик ИС - сотрудники _____ или сторонних организаций, которые занимаются разработкой ПО ИС. Программист-разработчик ИС обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации ИС;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИС на стадиях её разработки, внедрения и сопровождения;
-может располагать любыми фрагментами информации о топологии ИС и технических средствах обработки и защиты информации, обрабатываемой в ИС.

3. Оператор ИС- сотрудники ИС, участвующих в процессе эксплуатации ИС. Оператор ИС обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, идентификатором и паролем), обеспечивающими доступ к некоторому подмножеству информации;
- располагает конфиденциальными данными, к которым имеет доступ.

Категории пользователей должны быть определены для каждой ИС. При построении СЗПДн требуется уточнение разделения сотрудников _____ внутри категорий, в соответствии с типами пользователей, определёнными в Политике информационной безопасности ИС.

Все выявленные группы (роли) пользователей отражаются в «Отчёте по результатам обследования». На основании Отчёта выявляются права доступа к элементам ИС для всех групп (ролей) пользователей и отражаются в Матрице доступа в Положении о разграничении прав доступа к обрабатываемой информации.

# *Структура документа «Концепция информационной безопасности»*

## 6. Основные принципы построения системы защиты информации

Построение системы обеспечения безопасности информации ИС в _____ и её функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
-простота применения средств защиты;
-научная обоснованность и техническая реализуемость;
-специализация и профессионализм;
-обязательность контроля.

# Структура документа «Концепция информационной безопасности»

**6.1 Законность**

Предполагает осуществление защитных мероприятий и разработку СЗПДн в _____ в соответствии с действующим законодательством в области защиты информации и другими нормативными актами по ИБ, утверждёнными органами государственной власти в пределах их компетенции.

Пользователи и обслуживающий персонал ИС должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение безопасности информации.

**6.2 Системность**

Системный подход к построению СЗПДн в _____ предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения ИБ.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места ИС, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределённые системы и НСД к информации. СЗПДн должна строиться с учётом не только всех известных каналов проникновения и НСД к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.

**6.3 Комплексность**

Комплексное использование методов и средств защиты в _____ предполагает согласованное применение разнородных средств при построении целостной СЗПДн, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов.

# *Структура документа «Концепция информационной безопасности»*

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учётом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укреплённых рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

**6.4 Непрерывность защиты информации**

Защита информации – не разовое мероприятие и не простая совокупность проведённых мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС.

ИС должна находиться в защищённом состоянии на протяжении всего времени функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИС в незащищённое состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей, ключей шифрования, переопределение полномочий и т.п.).

Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления её функционирования.

**6.5 Своевременность**

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите ИС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки ИС в целом и СЗПДн в частности. Разработка СЗПДн должна вестись параллельно с разработкой и развитием самой ИС. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счёте, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищённые системы.

**6.6 Преемственность и совершенствование**

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС и СЗПДн с учётом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

**6.7 Персональная ответственность**

Предполагает возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого сотрудника _____ в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников _____ строится таким образом, чтобы в случае любого противоправного действия круг нарушителей был чётко известен или сведен к минимуму.

**6.8 Принцип минимизации полномочий**

Означает предоставление пользователям ИС минимальных прав доступа в соответствии с производственной необходимостью на основе принципа «всё, что не разрешено, запрещено».

Доступ к информации должен предоставляться только в том случае и объёме, в которых необходимо сотруднику _____ для выполнения его должностных обязанностей.

**6.9 Взаимодействие и сотрудничество**

Предполагает создание благоприятной атмосферы в коллективах подразделений _____, обеспечивающих деятельность ИС, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

В такой обстановке сотрудники _____ должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений технической защиты информации.

**6.10 Гибкость системы защиты информации**

Принятые меры и установленные СЗИ, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности СЗИ должны обладать определённой гибкостью. Особенно важным это свойство является в тех случаях, когда установку СЗИ необходимо осуществлять на работающую систему, не нарушая процесса её нормального функционирования.

**6.11 Открытость алгоритмов и механизмов защиты**

Суть принципа открытости алгоритмов и механизмов СЗПДн состоит в том, что защита не должна обеспечиваться только за счёт секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы СЗПДн не должно давать возможности её преодоления (даже авторам). Однако это не означает, что информация о СЗПДн должна быть общедоступна.

**6.12 Простота применения средств защиты**

Механизмы работы СЗПДн должны быть интуитивно понятны и просты в использовании. Применение СЗИ не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных и малопонятных ему операций (ввод нескольких паролей и имён и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИС.

**6.13 Научная обоснованность и техническая реализуемость**

Информационные технологии, технические и программные средства, средства и меры защиты информации в СЗПДн должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

СЗПДН должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

**6.14 Специализация и профессионализм**

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информации, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация СЗИ должна осуществляться профессионально подготовленными специалистами.

**6.15 Обязательность контроля**

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и СЗИ при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль над деятельностью любого пользователя, каждого СЗИ и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

# Структура документа «Концепция информационной безопасности»

## 7. Меры, методы и средства обеспечения требуемого уровня защищённости

Обеспечение требуемого уровня защищённости ИС должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИС подразделяются на:

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

### 7.1 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 их 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.

### 7.2 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 утверждённые нормативные акты, однако, их несоблюдение ведёт 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 коллективе _____. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

**7.3 Организационные (административные) меры защиты**

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования ИС, использование ресурсов ИС, деятельность сотрудников _____ и сторонних организаций, а также порядок взаимодействия пользователей с ИС таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз ИБ или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику информационной безопасности ИС, отражающую подходы к защите информации, и обеспечить её выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности в ИС состоит из мер административного уровня и организационных (процедурных) мер защиты информации. К административному уровню относятся решения руководства, затрагивающие деятельность ИС в целом.

# *Структура документа «Концепция информационной безопасности»*

Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности информации, определение ответственных за её реализацию;
- формулирование целей, постановка задач, определение направлений деятельности _____ в области безопасности информации;
- принятие решений по вопросам реализации программы безопасности;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна чётко очертить сферу влияния и ограничения при определении целей безопасности информации, определить, какими ресурсами (материальные, персонал) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИС.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности информации в _____.

Эти правила определяют:

- какова область применения политики безопасности информации;
- каковы роли и обязанности должностных лиц, отвечающих за проведение политики безопасности информации, а также их ответственность;
- кто имеет права доступа к информации;
- какими мерами и средствами обеспечивается защита информации;
- какими мерами и средствами обеспечивается контроль соблюдения введённого режима безопасности.

# *Структура документа «Концепция информационной безопасности»*

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к информации;
- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов СЗПДн;
- организовать меры противодействия НСД к информации пользователями на этапах идентификации, аутентификации и авторизации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

- регламента доступа в помещения _____;
- порядок допуска сотрудников к ИС;
- регламента процессов ведения БД и осуществления модификации информационных ресурсов;
- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИС;
- инструкций пользователей ИС (администратора ИС, администратора безопасности ИС, операторов ИС);
- инструкции пользователя при возникновении нештатных ситуаций.

## 7.4 Физические меры 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.
Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путём установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

## 7.5 Аппаратно-программные средства защиты информации

Технические (аппаратно-программные) меры защиты информации основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, обеспечение целостности и т.д.).

С учётом всех требований и принципов обеспечения безопасности информации в ИС по всем направлениям защиты в состав СЗПДн могут быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей;
- средства разграничения доступа зарегистрированных пользователей к ресурсам;
- средства обеспечения и контроля целостности программных и информационных ресурсов;

# *Структура документа «Концепция информационной безопасности»*

-средства оперативного контроля и регистрации событий безопасности;
-средства обнаружения и предотвращения вторжений;
-средства анализ защищённости;
-средства межсетевого экранирования;
-антивирусные средства;
-СКЗИ.

Успешное применение технических средств защиты на основании принципов предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИС;
- каждый сотрудник (пользователь ИС) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- в ИС разработка и отладка программ осуществляется за пределами ИС, на испытательных стендах;
- все изменения конфигурации технических и программных средств ИС производятся строго в установленном порядке (регистрируются и контролируются) только на основании распоряжений руководства;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, не доступных для посторонних (специальных помещениях, шкафах, и т.п.).
- специалистами по ИБ осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

**8. Контроль эффективности системы защиты ИС**

Контроль эффективности СЗПДн должен осуществляться на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы системы защиты (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности информации.

Контроль СЗПДн может проводиться как администратором безопасности ИС (оперативный контроль в процессе информационного взаимодействия в ИС), а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором безопасности ИС как с помощью штатных средств СЗПДн, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на соответствие установленным требованиям.

**9. Сферы ответственности за безопасность информации**

Ответственным за разработку мер и контроль над обеспечением безопасности информации является директор _____ (далее – Руководитель). Руководитель может делегировать часть полномочий по обеспечению безопасности информации.

Сфера ответственности Руководителя включает следующие направления обеспечения безопасности информации:

-планирование и реализация мер по обеспечению безопасности информации;
-анализ угроз безопасности информации;
-разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;

-контроль защищённости информационной инфраструктуры от угроз ИБ;
-обучение и информирование пользователей ИС о порядке работы с техническими средствами;
-предотвращение, выявление, реагирование и расследование нарушений безопасности информации.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты, с этими организациями должно быть заключено «Соглашение о конфиденциальности» либо «Соглашение о соблюдении режима безопасности информации при выполнении работ».

**10. Модель нарушителя безопасности**

Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты .

Нарушители подразделяются по признаку принадлежности к ИС. Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории КЗ, в пределах которой размещается оборудование ИС;
- внутренние нарушители – физические лица, имеющие право пребывания на территории КЗ, в пределах которой размещается оборудование ИС.

# *Структура документа «Концепция информационной безопасности»*

**11. Модель угроз безопасности**

Для ИС выделяются следующие основные категории угроз безопасности информации:

- угрозы от утечки по техническим канала;
- угрозы несанкционированного доступа к информации:
  - угрозы уничтожения, хищения аппаратных средств ИС, носителей информации путем физического доступа к элементам ИС;
  - угрозы хищения, несанкционированной модификации или блокирования информации за счёт НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
  - угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИС;
  - в результате сбоев ПО, а также угрозы неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;
  - угрозы преднамеренных действий внутренних нарушителей;
  - угрозы НСД по каналам связи.

# *Структура документа «Концепция информационной безопасности»*

**12. Механизм реализации Концепции**

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения ИБ и защиты информации;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России и ФСБ России;
- потребностей ИС в средствах обеспечения безопасности информации.

**13. Ожидаемый эффект от реализации Концепции**

Реализация Концепции информационной безопасности в ИС позволит:

- оценить состояние безопасности информации в ИС, выявить источники внутренних и внешних угроз ИБ, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
- разработать распорядительные и нормативно-методические документы, применительно к ИС;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности информации в ИС;
- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной СЗПДн и создаст условия для её дальнейшего совершенствования.

# *Структура документа «Концепция информационной безопасности»*

**Список использованных источников**

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Концепция, являются:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
3. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
4. Постановление Правительства РФ от 24 октября 2011 г. № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)»;
5. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
6. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
7. Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

# *Структура документа «Концепция информационной безопасности»*

8. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
9. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
0. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
1. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая Заместителем директора ФСТЭК России 15 февраля 2008 г.;
2. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая Заместителем директора ФСТЭК России 15 февраля 2008 г.