Системные принципы защиты информации

Информационная безопасность (ИБ) – отсутствие недопустимого риска, связанного с причинением прямого или косвенного имущественного (финансового) ущерба предприятию (организации), который вызван нарушением конфиденциальности, целостности и доступности информации.

Угроза ИБ – наличие потенциальной возможности использования некоторой информации или воздействия на эту информацию, ведущей к прямому или косвенному ущербу для предприятия.

КСЗИ основана на принципах: (1)…

Комплексная система защиты информации (КСЗИ) основывается на следующих системных принципах:

- ***принцип системного подхода*** – необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени компонентов, условий и факторов, существенных для обеспечения безопасного функционирования информационной системы (ИС);
- ***принцип комплексности*** – согласованное применение разнородных средств и мероприятий для обеспечения безопасности всей совокупности информации, подлежащей защите, по отношению ко всему спектру угроз;

КСЗИ основана на принципах: (2)…

Комплексная система защиты информации основывается на следующих системных принципах:

- ***принцип адекватности*** – принимаемые решения должны выбираться так, чтобы обеспечить необходимый уровень ИБ при минимальных затратах на создание механизмов защиты и обеспечение их правильного функционирования;
- ***принцип адаптивности*** – СЗИ должна строиться с учетом возможного изменения конфигурации сети, числа пользователей и степени конфиденциальности и ценности информации. Введение каждого нового элемента сети или изменение действующих условий не должно снижать достигнутого уровня защищенности ИС;

КСЗИ основана на принципах: (3)…

Комплексная система защиты информации основывается на следующих системных принципах:

- ***принцип неопределенности*** – должна обеспечиваться эффективная защита информации в условиях неопределенности действия угроз, влияния человеческого фактора, отсутствия формальных математических моделей для описания информационных процессов и технологий и т.д.;
- ***принцип непрерывности*** – защита информации представляет собой непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС.

Методологические принципы изучения сложных проблем ЗИ (1)

В качестве важных методологических принципов, отмечаются :

- ***построение адекватных моделей изучаемых систем и процессов*** – необходима разработка методов, позволяющих адекватно моделировать системы и процессы, существенно зависящие от воздействия случайных и труднопредсказуемых факторов.
- Попытки моделирования с использованием традиционных методов приводят к тому, что создаваемые модели оказываются неадекватными моделируемым системам.

«… более трех принципов – это уже беспринципность»

Методологические принципы изучения сложных проблем ЗИ (2)

В качестве важных методологических принципов, отмечаются :

- ***унификация разрабатываемых решений*** – требуется разработка унифицированной концепции построения сложных систем, позволяющей представить решение проблемной ситуации «объект – среда – цели» в виде последовательности самостоятельных, относительно независимых проектных задач (этапов) и свести решение задачи проектирования к выбору типовых и стандартных проектных решений;

Методологические принципы изучения сложных проблем ЗИ (3)

В качестве важных методологических принципов, отмечаются :

- ***максимальная структуризация изучаемых систем и разрабатываемых решений*** – предполагает декомпозицию сложной системы и элементов ее среды на отдельные составляющие (компоненты), взаимодействующие друг с другом, анализ которых позволяет в конечном итоге сформировать такую архитектуру разрабатываемой системы, которая наилучшим образом удовлетворяет совокупности условий проектирования, эксплуатации;

Методологические принципы изучения сложных проблем ЗИ (4)

В качестве важных методологических принципов, отмечаются :

- ***радикальная эволюция в реализации разработанных предложений*** – необходимо стремиться к радикальным улучшениями архитектуры систем и процессов их организации и обеспечения функционирования, но реализовывать их постепенно, эволюционным путем.
- Непрерывная интеграция, спиральная модель жизненного цикла;

Современная система защиты информации

- **Современная система защиты информации** (СЗИ) – это сложная, динамическая, развивающаяся человеко-машинная система, неотделимая от объекта защиты – информационной системы предприятия (организации) и призванная обеспечить его нормальное и устойчивое функционирование в условиях действия возможных внутренних и внешних угроз.
- Угрозы характеризуются существенной **неопределенностью**, что требует использования для их описания, а равно, и для построения соответствующих алгоритмов принятия решений в СЗИ, адекватных угрозам, математических моделей и методов искусственного интеллекта.
- **Конкретная реализация** моделей, методов и алгоритмов определяется характером угроз, спецификой решаемых

Интегрированные системы защиты информации

Различают следующие уровни обеспечения ИБ:

- нормативно-законодательный;
- административный;
- процедурный;
- программно-технический.

Интегрированные системы защиты информации (1 уровень)

На **нормативно-законодательном уровне** разрабатываются законодательные меры обеспечения ИБ, регулирующие информационные отношения между различными субъектами (юридическими и физическими лицами) в пределах страны

- «Доктрина информационной безопасности»,
- ФЗ «Об информации, информационных технологиях и защите информации»,
- ФЗ «О государственной тайне»,
- ФЗ «О коммерческой тайне»,
- ФЗ «О персональных данных»
- национальные стандарты ГОСТ Р ИСО/МЭК

Интегрированные системы защиты информации (2 уровень)

К **административному уровню ИБ** относятся действия общего характера, предпринимаемые руководством предприятия.

Цель административного уровня – сформировать программу работ в области ИБ и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является **политика безопасности**, которая строится на основе анализа рисков и отражает принятый подход к защите информационных ресурсов предприятия.

Интегрированные системы защиты информации (3 уровень)

На **процедурном уровне ИБ** применяются главным образом организационные меры безопасности, ориентированные на людей, а не на технические средства. К данным мерам относятся:

- управление персоналом;
- физическая защита;
- поддержание работоспособности информационной системы;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

В качестве нормативно-методической базы ИБ использованы специализированные политики ИБ (по конкретным аспектам ИБ), правила и процедуры ИБ, инструкции администраторам и пользователям ИС.

Интегрированные системы защиты информации (4 уровень)

Программно-технический уровень ИБ – это уровень, на котором реализуются различные программно-технические меры, направленные на контроль работоспособности оборудования и программного обеспечения.

Поскольку из общего числа угроз в последние годы все больший удельный вес занимают внутренние угрозы со стороны персонала, по отношению к которым процедурные меры не дают большого эффекта, именно на программно-технические меры возлагаются большие надежды.

Наиболее распространенные сервисы безопасности

На программно-техническом уровне понятие сервиса (функции безопасности) включает:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

Интегрированные системы защиты информации

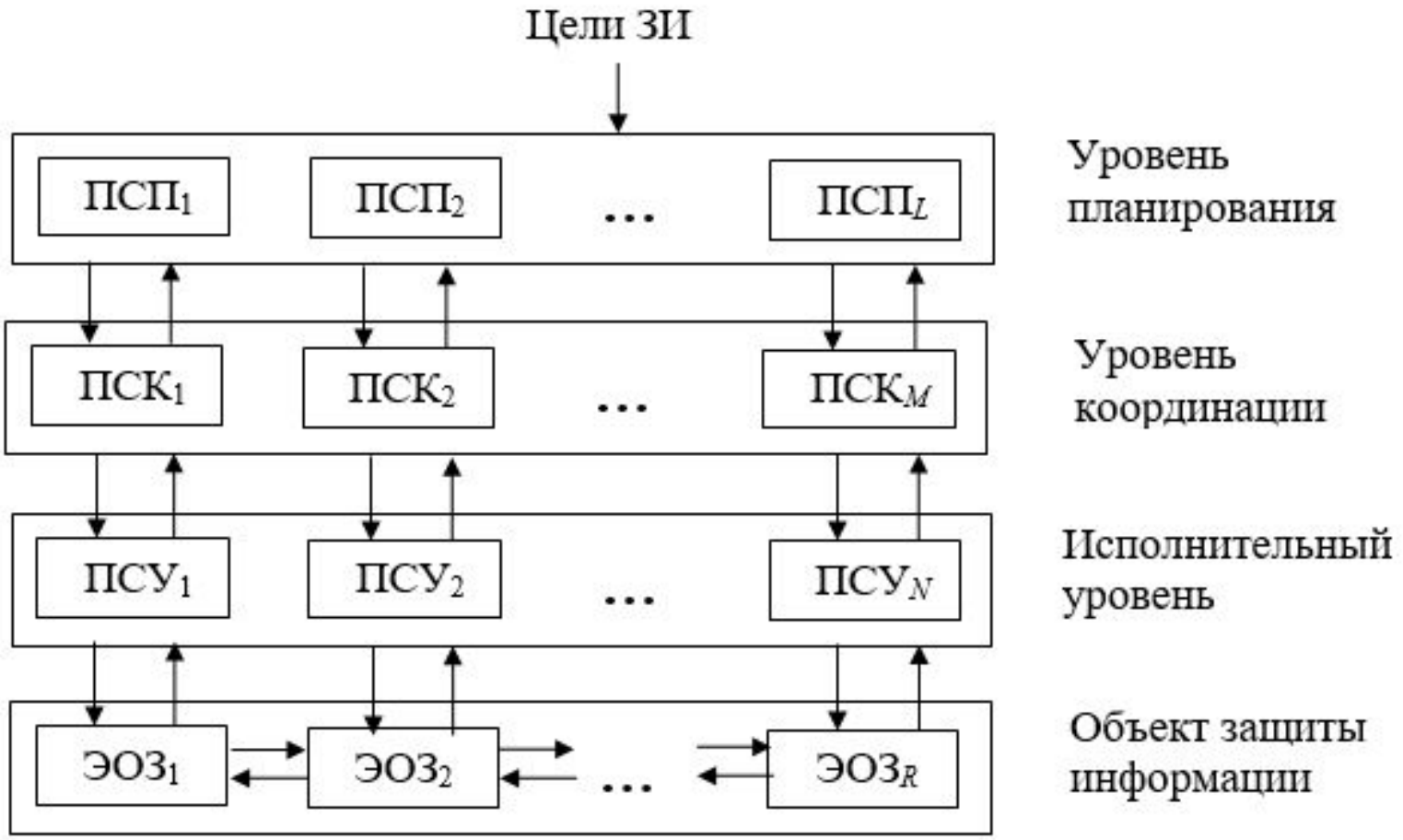
Необходимым условием эффективного функционирования комплексной СЗИ является согласованная работа всех подсистем в соответствии с политикой безопасности и нормативно-методическими документами, принятыми на предприятии.

В составе СЗИ:

- уровень управления СЗИ
  - уровень координации работы подсистем
  - уровень планирования СЗИ в целом.
- исполнительный уровень управления СЗИ - подсистема управления защитой ($ПСУ_1$, …, $ПСУ_N$), реализующая управление сервисами безопасности для отдельных элементов объекта защиты ($ЭОЗ_1$, …, $ЭОЗ_R$).

Системы, обладающие многоуровневой иерархической

Схема иерархической организации СЗИ



Интегрированные системы защиты информации (1)

Уровень координации, «ядро» СЗИ, реализует функции координированного управления работой подсистем защиты и включает в себя ряд подсистем управления ($ПСК_1$, …, $ПСК_М$), обеспечивающих:

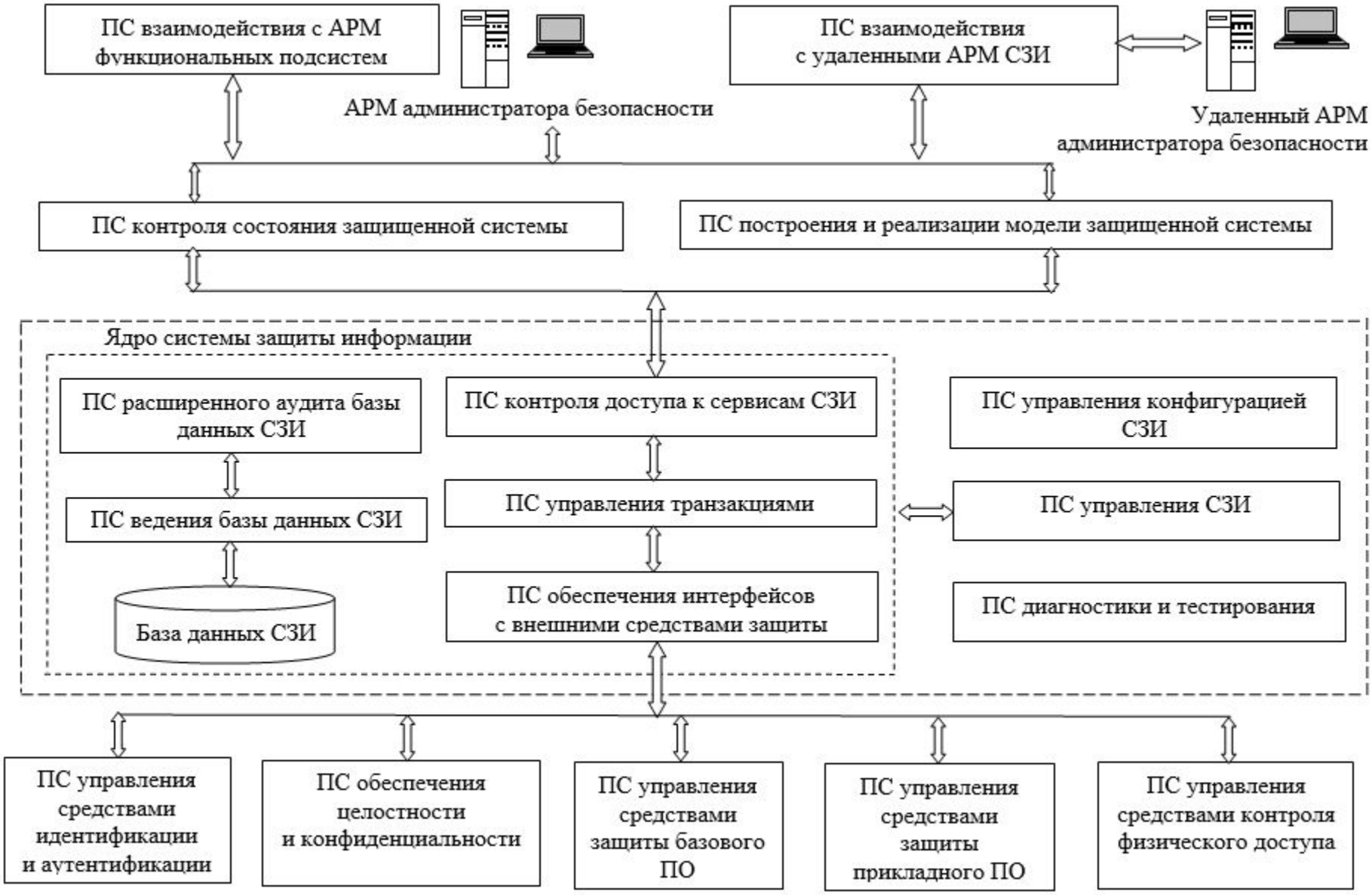
- включение в работу компонентов (подсистем) СЗИ при поступлении запросов на обработку защищаемых данных;
- управление работой СЗИ в процессе обработки защищаемых данных;
- организацию и обеспечение проверок правильности функционирования СЗИ;
- блокирование несанкционированного доступа (НСД) к защищаемым базам данных;
- обеспечение реагирования на сигналы о несанкционированных действиях;
- ведение протоколов СЗИ и др.

Интегрированные системы защиты информации (2)

На **уровень планирования СЗИ**, также состоящий из нескольких подсистем планирования ($ПСП_1$, …, $ПСП_L$), возлагаются функции контроля состояния безопасности информационной системы. Выполняются функции:

- контроль текущего уровня защищенности ИС;
- слежение за опасными ситуациями (непредвиденными обстоятельствами);
- анализ причин, которые привели к их возникновению, и устранение последствий;
- прогноз развития ситуаций;
- анализ рисков;
- перераспределение ресурсов (задача выбора оптимального набора средств защиты) при изменении состава ИС или характеристик среды.

Архитектура интегрированной системы



Функции управления в составе СЗИ

Все функции управления являются составляющими одной общей задачи – реализации политики безопасности:

- управление сервисами безопасности,
- координация их взаимодействия,
- осуществление контроля функционирования защищенной информационной системы

Достоинства и недостатки интегрированных СЗИ

Преимущества интегрированных СЗИ:

- возможность централизованного управления работой всех подсистем практически с одного пульта (консоли),
- координация и контроль правильности функционирования этих подсистем,
- минимизация избыточности (устранение дублирования функций),
- упрощение механизмов оценки ситуаций и принятия решений.

Достоинства и недостатки интегрированных СЗИ

В качестве недостатков можно отметить:

- недостаточную гибкость
  - возможные ошибочные реакции при появлении неизвестных угроз, затруднения при оценке сложных ситуаций,
  - снижение оперативности принятия решений при большом числе дестабилизирующих факторов – так называемое «проклятие размерности»,
- повышенная нагрузка на администратора безопасности,
- возможные «нестыковки» механизмов защиты (алгоритмов реализации сервисов безопасности) при использовании технических решений различных фирм-производителей и т.д.

Адаптивные интегрированные (интеллектуальных) СЗИ

Подобные затруднения в значительной степени теряют свою остроту в связи с появлением нового класса СЗИ – адаптивных интегрированных (интеллектуальных) систем защиты информации.