3.4. Программно-технические методы и средства обеспечения безопасности

Аппаратно - программные средства защиты информации предоставляются устройствами, встраиваемыми непосредственно в аппаратуру АИС, или устройствами, сопряженными с аппаратурой АИС по стандартному интерфейсу и предназначенными для реализации конкретных функций защиты. Они реализуют логическую оболочку АИС, ориентированную на обеспечение безопасности.

Программно-технические методы и средства могут быть систематизированы по характеру противостояния, по нашему мнению, в две группы - *активные* и *пассивные*. К первой группе относятся следующие (рис. 21).

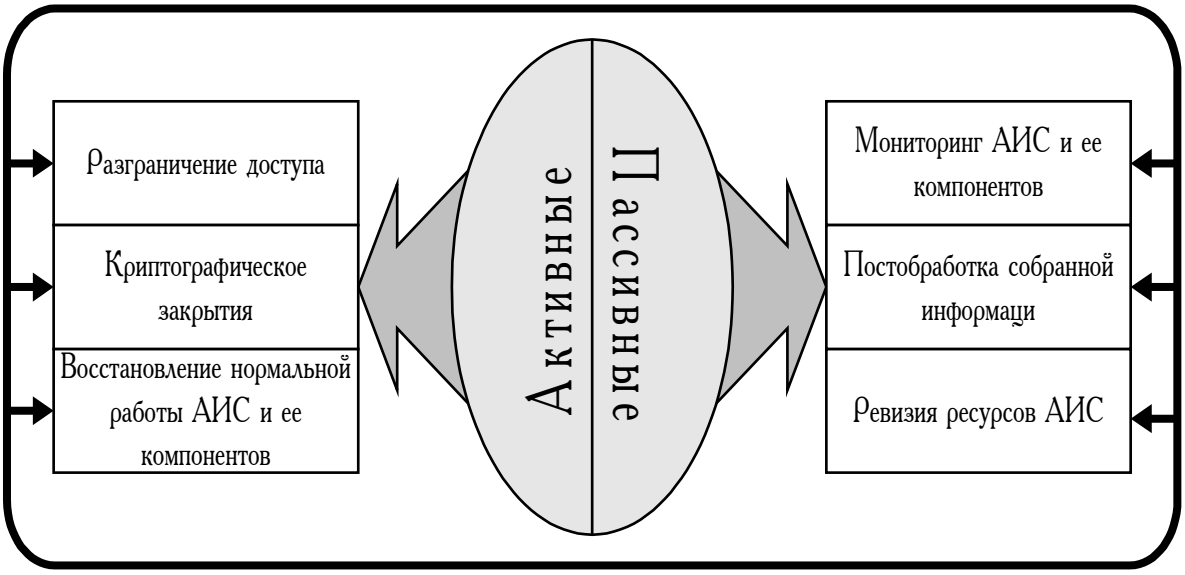

Рис 21. Классификация программно-технических методов и средств защиты информации по характеру противодействия.

- *методы и средства разграничения доступа*, способствующие защите информации с регулированием использования всех ресурсов системы (технических, программных, баз данных) [147,30,157].

- *методы криптографического закрытия*. Реализуют преобразование данных, в бесполезную информацию для злоумышленника [135,99,38].

- *методы и средства восстановления нормальной работы.* Это такая часть АИС, которая призвана обеспечить непрерывное функционирование объекта управления и уменьшения времени выхода из строя за счет привлечения дополнительных ресурсов.

Необходимо иметь ввиду, что криптографические методы используются в сочетании со средствами разграничения доступа, что значительно повышает качество защиты [135,74 и др.].

Пассивные программно-технические методы и средства обеспечения информационной безопасности призваны выполнять функции, связанные с контролем состояния системы, а также подготовкой необходимой информации для активных элементов системы защиты. К ним относятся следующие из этих методов и средств:

- *мониторинг АИС.* Предназначен для регистрации деятельности пользователя как в ходе сеанса, так и в течение более длительного времени;

- *постобработка.* Это последующая обработка и анализ собранной с помощью мониторинга информации;

- *ревизия и аудит.* Имеют своей целью контроль ресурсов и реализацию операций по оптимизации их использования;

- *контроль целостности и доступности.* Обеспечивают проверку целостности и доступности ресурсов и процессов в АИС.

Иногда пассивную часть аппаратно-програмнных методов и средств называют ядром безопасности [31].

Для выполнения своих функций ядро безопасности должно обладать следующими основными свойствами:

- *изолированность.* Состоит в том, что ядро безопасности должно быть защищено от мониторинга своей работы;

- *полнота.* Ядро безопасности должно регистрировать все события в АИС. При этом не допустимо наличие способов обхода регистрации;

- *верифицирцемость*. Состоит в том, что для выявления возможных нарушений собранную информацию необходимо анализировать и проверять.

С точки зрения содержания существует достаточно широкий состав программно-технических средств и формализуемых методов, позволяющих реализовать основную программно-техническую защиту информационной системы от несанкционированных действий.

Рассмотрим более подробно перечисленные выше методы обеспечения информационной безопасности АИС.

3.4.1. Активные программно-технические методы и средства обеспечения информационной безопасности.

Системы разграничения доступа. Основная функция системы разграничения доступом - это управление взаимодействием между объектами и субъектами АИС. Она предусматривает выполнение следующих операций защиты:

- идентификацию и аутентификацию пользователей, персонала и ресурсов системы. При этом, идентификация связана с присвоением каждому объекту и/или субъекту персонального идентификатора;
- проверку полномочий, заключающуюся в проверке соответствия временных интервалов разрешения доступа и прав на осуществление тех или иных действий;
- разрешение и создание условий работы в пределах установленноо регламента;
- реагирование - задержка работ, отказ, отключение, сигнализация и т.д. при попытках несанкционированных действий.

В компьютерных системах выделяют следующие виды аутентификации [221,168]:

- *аутентификация пользователей сети.* Имеется ввиду опознание пользователей, которым необходим доступ к защищаемой информации или требуется подключение к АИС;

- *аутентификация процессов.* Состоит в опознании процессов и определении правомерности их операций;

- *аутентификация хранящихся файлов данных.* Направлена на установление того факта, что данные не подверглись модификации;

- *аутентификация сообщений.* Сводятся к установлению подлинности полученного по каналам связи сообщения, в том числе решения вопроса об авторстве этого сообщения и установления факта приема сообщения.

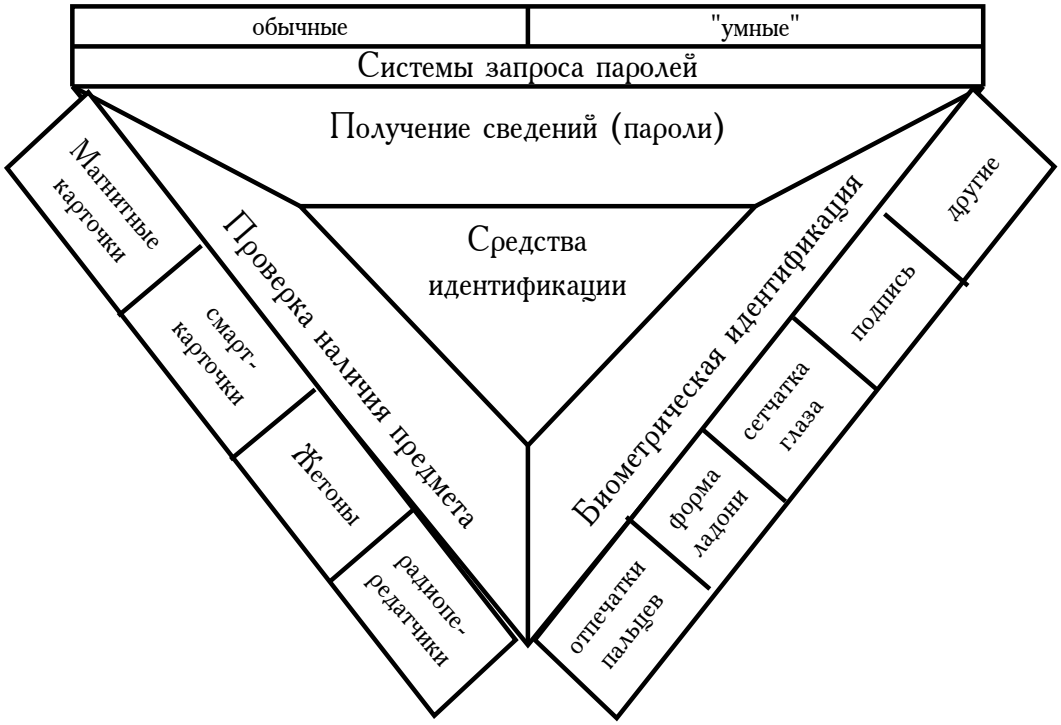

Рис. 22. *Классификация принципов и средств идентификации пользователей*

В настоящее время известны три основные группы методов аутентификации пользователей: *запрос сведений, проверка наличия предмета* и *биометрическая идентификация* (рис. 22).

Одним из распространенных методов аутентификации является *установление личности по тем специфическим сведениям, которыми он располагает, т.е. по паролю*. Считается, что эти сведения хранятся исключительно в памяти пользователя и не могут быть известны посторонним.

На сегодняшний день в большинстве случаев аутентификация пользователей осуществляется с помощью паролей. Но обычные пароли - слабая защита. Как видно из состава рассмотренных злоупотреблений, создана большая группа программных злоупотреблений, которые позволяют открыть или получить идентификаторы и пароли. Кроме того, обычные пароли могут подсматриваться. В связи с этим, разрабатываются технические средства, позволяющие заменить обычные пароли техническими эквивалентами, которые позволили бы идентифицировать пользователей при входе в систему.

Другой метод аутентификации пользователя состоит *в проверке наличия у пользователя некоего предмета - физического объекта, представляющего собой электронный аналог обычного ключа*. В качестве таких предметов могут быть использованы магнитные пластиковые карточки, карточки со встроенным микропроцессором, жетоны, радиопередатчики небольшого радиуса действия и др. [27,39,91 и др.].

Магнитная пластиковая карта - это карта с магнитной полосой, на которой записана последовательность символов, являющейся уникальной и по содержанию определяющей права доступа и полномочия держателя.

Пластиковая карта со встроенным микропроцессором - представляет собой пластиковую карту со встроенным микропроцессором, используемую не только для хранения информации, но и как средство шифрования информации.

В настоящее время магнитные карты и карты со встроенным микропроцессором нашли широкое распространение в банковских технологиях для идентификации и аутентификации клиентов [103, 8].

Жетон - это устройство, вырабатывающее псевдослучайную буквенно-цифровую последовательность (слово). Это слово меняется синхронно через определенное время одновременно со сменой такого же слова в центральной базе данных. В результате вырабатывается одноразовый пароль, который используется в определенный промежуток времени и только для однократного входа в систему.

Прибор *Touch Memory* - это специальный электронный прибор, содержащий уникальный индентификатор и используемый для идентификации и аутентификации путем кратковременного касания к специальному считывателю, связанному с компьютером [144]. На сегоняшний день существуют несколько модификаций Touch Memory, отличных по возможностям и стоимости. Хотя в литературе зачастую подвергается сомнению уровень его надежности [67,91], на практике из-за низкой стоимости и легкости в эксплуатации активно внедряется разработчиками в системы разграничения доступа [144,75].

Определенную перспективу имеют так называемые активные средства опознания, каким является *миниатюрный радиопередатчик* слабого радиосигнала, который пользователель носит с собой. Как только передатчик оказывается вблизи от специального приемника (обычно на расстоянии нескольких десятков сентиметров), последний принимает радиосигнал и проанализировав его, выдает разрешение на доступ. Достоинство данного подхода в том, что аутентификация осуществляется автоматически, без вмешательства проверяемого лица и без физического контакта с устройством считывания.

Наиболее надежными считаются *биометрические методы идентификации*, в которых личность идентифицируется по отпечаткам пальцев, форме ладони, сетчатке глаза, подписи, голосу и др. характеристикам [36, 39].

Системы разграничения доступа можно условно разделить также на системы физического разграничения доступа и системы разграничения доступа к ресурсам АИС.

Наиболее полно системы физического разграничения доступа рассмотрены в работах [36,39,135,38,114,144 и др.].

Среди существующих систем физического разграничения доступа можно выделить следующие основные группы [39]:

- СВЧ- и ультразвуковые системы. Предназначены для обнаружения объектов, определения их размеров, скорости и направления перемещения;
- Лазерные и оптические системы. Реагируют на пересечение нарушителем светового луча. Применяются для охраны внутренних помещений зданий, так как при внешнем применении из-за большого числа возможных воздействий они являются источником постоянных ложных тревог;
- Телевизионные системы. Широко применяются для наблюдения за территорией охраняемого объекта или за обстановкой внутри помещения;
- Кабельные системы. Используются для охраны небольших, временно находящихся на территории объектов, а также оборудования внутри помещений.

Для управления доступом реализуется политика безопасности, призванная обеспечить разграничение доступа с заданным уровнем надежности. Под политикой безопасности понимают совокупность правил и мероприятий, призванные регулировать доступ к ресурсам АИС.

Известны и разработаны два типа политики безопасности - избирательная и полномочная [112,30,136].

Криптографические методы и средства обеспечения информационной безопасности. Криптографическое закрытие

информации считается достаточно эффективным как с точки зрения защиты, так и наглядности для пользователей. На сегодняшний день этот вид защиты широко применяется как при обработке, так и хранении информации [99,22,41,63,38,74,106 и др.]. При передаче информации по линиям связи криптографическое закрытие является основным методом ее надежной защиты.

Шифрование подразумевает реализацию двух процедур [135,162, 169]:

- процедура шифрования исходного открытого текста документа (сообщения) с целью получения зашифрованного текста;

- процедура расшифрования зашифрованного текста с целью получения открытого текста.

С помощью криптографии возможно обеспечение:

- шифрования информации для защиты как от несанкционированного доступа со стороны пользователя злоумышленника, так и от компьютерных вирусов;

- контроля целостности хранящихся данных и программ с целью обнаружения случайных и преднамеренных искажений;

- аутентификации передаваемых сообщений с целью проверки целостности их содержания и подтверждения подлинности авторства;

- аутентификации документов с целью решения спорных вопросов относительно авторства документов на основе цифровой подписи;

- защиты программ от несанкционированного копирования и распространения;

- генерации паролей и организации парольных систем.

Правильный выбор системы шифрования позволяет достичь следующие цели:

- скрыть содержание документа от посторонних лиц (обеспечение конфиденциальности документа) путем шифрования его содержимого;

- обеспечить совместное использование документа группой пользователей системы путем криптографического разделения

информации и соответствующего протокола распределения ключей. При этом для лиц, не входящих в группу, содержание документа является недоступным;

- своевременно обнаружить искажение, подделку документа (обеспечение целостности документа) путем введения криптографического контрольного признака;

- удостовериться в том, что абонент, с которым происходит взаимодействие в сети является именно тем, за кого он себя выдает (аутентификация абонента/источника данных)

Криптографические алгоритмы разделяются на два класса:

- симметричные;

- асимметричные.

В симметрических алгоритмах шифрования секретный ключ шифрования совпадает с секретным ключом расшифрования.

В асимметричных схемах шифрования (криптоалгоритмы с открытым ключом) открытый ключ шифрования не совпадает с секретным ключом расшифрования.

В криптографии принято правило Керкхоффа, в соответствии с которым стойкость шифра должна определяться только секретностью ключа. Злоумышленнику - криптоаналитику в системе защиты может быть известно все, кроме секретного ключа.

Под криптостойкостью понимают сложность алгоритма раскрытия. Считается, что криптосистема раскрыта, если злоумышленник способен с вероятностью, превышающей заданную, провести следующие операции:

- вычислить секретный ключ;
- выполнить эффективный алгоритм преобразования, функционально эквивалентный исходному криптоалгоритму.

Для того, чтобы заявить о раскрытии криптосхемы, нужно не только указать сам алгоритм раскрытия, гарантирующий

злоумышленнику успех, но и то, что данный алгоритм выполним за реальное время.

Для решения задачи аутентификации информации в широком смысле, т.е. для защиты от всех способов обмана, Диффи и Хелманом в 1976 г. предложена концепция аутентификации на основе "цифровой подписи" [27]. Она заключается в том, что каждый пользователь сети имеет свой секретный ключ, необходимый для формирования подписи, соответствующий этому секретному ключу открытый ключ, предназначенный для проверки подписи, известен всем другим пользователям сети. В предложенной схеме цифровая подпись вычисляется на основе защищаемого сообщения и секретного ключа конкретного пользователя, являющегося отправителем этого сообщения. Каждый пользователь, имеющий соответствующий открытый ключ, может аутентифицировать сообщение по подписи. Кроме того, знание открытого ключа не позволяет подделать подпись. Такие схемы аутентификации называются асимметричными.

Основная область применения цифровой подписи - это коммерческие компьютерные системы, в которых отсутствует взаимное доверие сторон (финансовые системы, системы контроля за соблюдением договоров и т.д.). Возможно применение схем цифровой подписи для создания "электронного нотариуса" с целью обеспечения, например, авторских прав на программные изделия.

Во многих отношениях цифровая подпись похожа на обычную (таблица 3).

Таблица 3.

Сравнительные характеристики обычной и цифровой подписей.

Обычная подпись	Цифровая подпись
У каждого человека свой,только ему присущий почерк, который характеризуется определенным написанием букв, давлением на	Каждый человек использует для подписи документов свой уникальный секретный ключ

ручку и т.д.	
Попытка подделки подписи обнаруживается с помощью графологического анализа	Любая попытка подписать документ без знания соответствующего секретного ключа практически не имеет успеха
Подпись и подписываемый документ передаются только вместе на одном листе бумаги. Ситуаций, когда подпись передается отдельно от документа не существует. При этом подпись не зависит от содержания документа на котором она поставлена	Цифровая подпись документа есть функция содержания этого документа и секретного ключа. Цифровая подпись может передаваться отдельно от документа
Копии подписанного документа недействительны, если они не имеют своей настоящей (а не скопированной) подписи	Копия подписанного цифровым способом документа не отличается от его оригинала (нет проблемы подписи каждой копии

Восстановление. При активном взаимодействии со всеми подсистемами защиты, подсистема восстановления призвана обеспечить непрерывную работу всех компонентов АИС. В ее рамках реализуется комплекс мероприятий восстановления, приведенный на рис. 25.

3.4.2. Пассивные программно-технические методы и средства обеспечения информационной безопасности

Пассивные методы и средства защиты призваны активно взаимодействовать как между собой, так и с группой активных средств защиты АИС.

На рис. 23 представлена схема взаимодействия пассивных средств обеспечения информационной безопасности между собой при выработке необходимой информации для других подсистем защиты АИС.

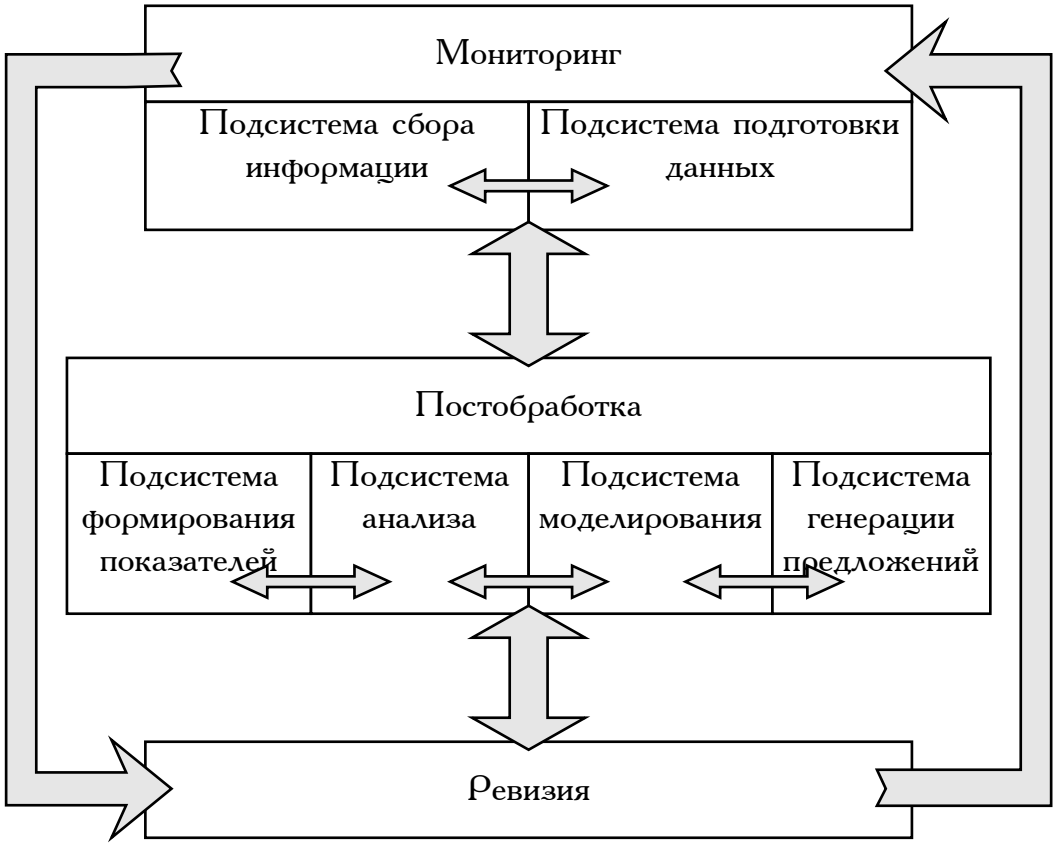

Рис. 23. Состав и взаимодействие пассивных средств обеспечения информациионной безопасности АИС.

Средства мониторинга. Система мониторига АИС включает две основные подсистемы - подсистемы сбора информации, (непосредственно мониторинг АИС) и подсистему подготовки данных для других подсистем защиты информации.

По нашему мнению, в АИС должен осуществляться многоуровневый мониторинг (на уровне операционной системы, СУБД, приложений). Наряду с этим средства мониторинга должны быть составной частью АИС и жругие ее части должны работать независимо от состояния АИС: эксплуатация, обслуживание, ремонт и т.п.

Система мониторинга осуществляет анализ сторон конфликта; структуры конфликтного поведения (конфликтная ситуация, конфликтные установки сторон, конфликтные действия); динамики

конфликта; решения конфликта (тактика и стратегия); среды конфликта.

Осуществление мониторинга для выявления ПЗ предполагает синтезированный анализ следующих вопросов (рис. 24):

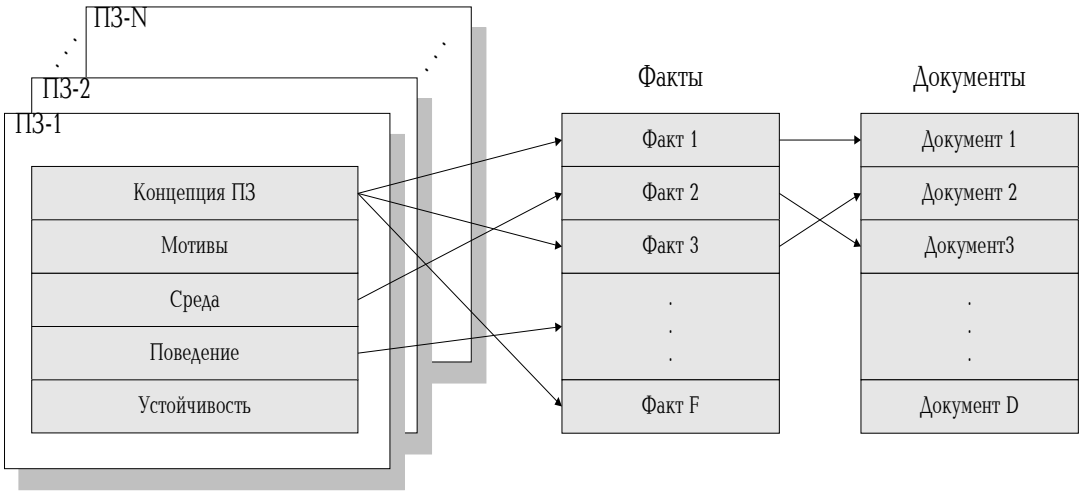

Рис. 24. Концепция мониторинга, ориентированная на выявление программных злоупотреблений

- представление о ПЗ или ее концепция;
- мотивы, влияющие на процессы разработки и внедрения ПЗ;
- компьютерная среда;
- “поведение” ПЗ и методы обнаружения;
- устойчивость ПЗ (методы маскировки, внедрения и т.д.).

Подсистема подготовки данных призвана учитывать необходимость и требования к входным данным для всех компонентов системы информационной безопасности АИС. Имеется ввиду, что данные, регистрируемые подсистемой сбора информации должны быть подготовлены, специальным образом форматированы и записаны в специальных файлах для того, чтобы их использовали другие подсистемы. На рис. 25 системе мониторинга соответствует этому “избыточность”.

Постобработка. Хотя во многих источниках отмечается необходимость и важность последующей обработки собранной системой мониторинга информации, до сих пор в литературе (кроме [134,52]) данная проблема не нашла должного отражения.

По нашему мнению в функции подсистемы постобработки АИС, должна входить и последующая обработка и анализ собранной с помощью мониторинга информации, результатом которой должно быть предоставление справок, отчетов и рекомендаций ответственному за состояние безопасности лицу.

В качестве основных данных, содержащихся в основных отчетах и справках можно признать такие показатели как частота сменяемости задач; число ошибок при идентификации; число нарушений полномочий; время использования процессора для одного процесса; число технических сбоев и другие, характеризующие работу и состояние системы защиты.

Ревизия и аудит. Подсистема ревизии призвана осуществить проверку наличия, целостности и доступности ресурсов и процессов в АИС.

Аудит связан с действиями и событиями, затрагивающими безопасность системы. К ним отнсят: вход в систему (успешный или нет); выход из системы; обращение к удаленной системе; операции с файлами; смена привилегий или иных атрибутов безопасности. Следует отметить, что полный перечень событий, потенциально подлежащих регистрации зависит от избранной политики безопасности и от специфики АИС.

В заключении отметим настоятельную необходимость обеспечения логической целостности комплекса программно-технических средств.

Ввиду того, что рассматриваемые методы и средства ориентированы на отдельные компоненты АИС, важно более детально остановиться на рассмотрении их взаимодействия с программно-техническими средствами обеспечения информационной безопасности

данной системы. При этом в качестве основных признаются такие компоненты АИС, как персонал, ЭВМ, периферийное оборудование, коммуникации, операционные системы, системное и прикладное программное, данные.

Состав методов и средств осуществления ревизии и аудита по конкретным объектам АИС, приведен на рис. 25.

Приведенный состав программно-технических методов и средств обеспечения информационной безопасности были определены для процесса функционирования АИС (рис. 17, 25).

Рассмотрим основные методы и средства обеспечения информационной безопасности при взаимодействии АИС с внешней средой, т.е. на этапах входного и выходного контроля).

Входному контролю должны подвергаться все компоненты АИС (персонал, ЭВМ, периферийное оборудование, коммуникации, операционные системы, системное и прикладное программное обеспечение, информация).

Персонал должен быть идентифицирован и аутентифицирован. Каждый вход в систему должен регистрироваться в системном журнале. Каждый пользователь после аутентификации должен пройти проверку полномочий, после чего ему должны быть выделены определенные ресурсы, соответствующие его классу. Подсистема реализации входного контроля должна управлять паролями, метками безопасности, полномочиями и др.

При входе в систему каждый компьютер должен быть идентифицирован и аутентифицирован. В условиях любой АИС в каждый момент времени необходима информация о том с какой удаленной системой работает функционирцющая АИС, перечень услуг, которые предоставляются удаленной системе или АИС получает от нее.

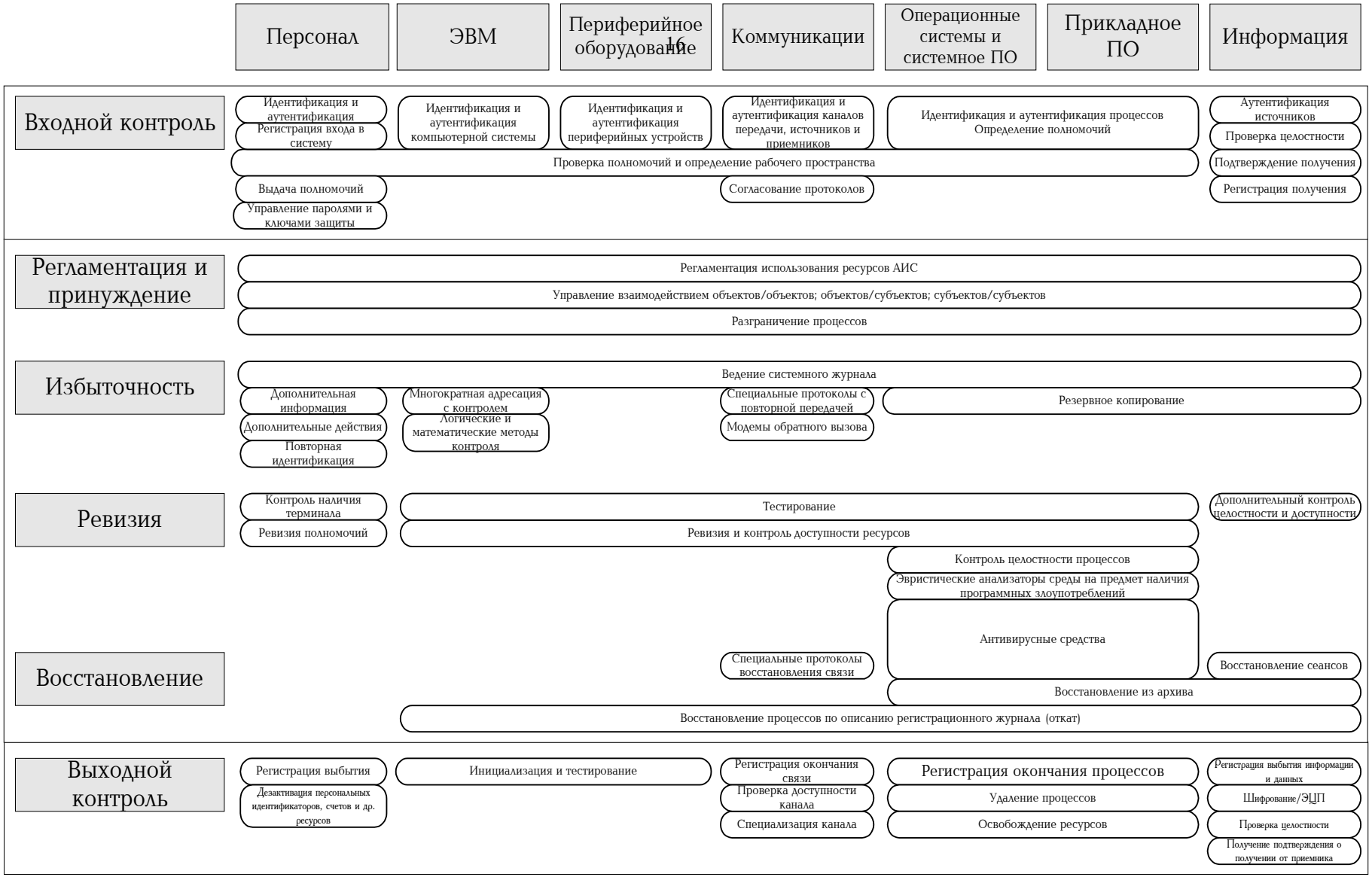

Рис. 25 Состав программно-технического обеспечения системы информационной безопасности.

Аналогиченые требования входного контроля предъявляются и к периферийному оборудованию.

В отношении коммуникаций представляется возможным более подробно рассмотреть систему защиты, базирующуюся на 7-ми уровневой модели.

Коммерческие структуры выделяют значительные ресурсы для защиты информации, поскольку возможность раскрытия профессиональных секретов и корпоративных планов или финансовых сделок является катализатором для проведения соответствующих исследований и разработок. В качестве базисной (эталонной) признана 7-ми уровневая модель Международной организации по стандартизации (МОС) и Международного консультативного комитета по телеграфии и телефонии (МККТТ).

В рамках эталонной модели для каждого уровня определяются соответствующие стандарты (форматы, семантика элементов данных, элементы взаимодействия смежных уровней). В свою очередь, уровни эталонной модели включают классы уровней специфичных для конечных систем; маршрутизации и специфичных для смежных систем.

Для коммерческих систем большое значение имеют первые два класса из-за возможностей проведения контроля в рамках существующего трафика: прикладного, представления данных, сеансового и транспортного уровней, а также сетевого. Размещение средств защиты на мультиуровнях обеспечивает требуемую степень безопасности за счет совместимости программно-аппаратных средств и поддержки средств связи (рис. 26).

При сравнении существующих стандартов следует выделить различия, в основе которых лежат признаки функциональности и необходимости.

Если размещение элементов защиты на всех уровнях эталонной модели является обязательным для государственных компьютерных

систем, то коммерческим целесообразно использовать прикладной уровень.

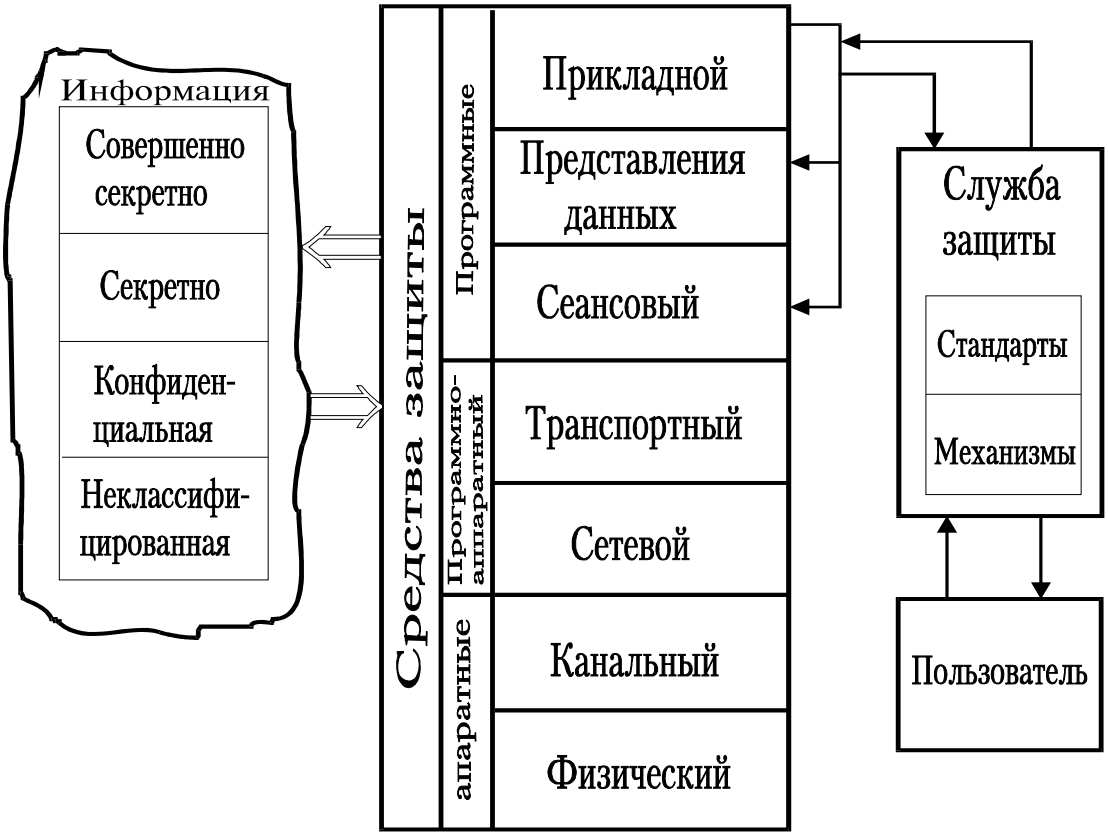

Рис. 26. Схема организации защиты информации в системе, базирующейся на эталонной модели

На уровне операционной системы, системного и прикладного программного обеспечения должны должны осуществляться идентификация и аутентификация процессов, определение полномочий для каждого процесса.

Входной контроль по отношению к информации осуществляется в слудующих направлениях:

- идентификация и аутентификация источников;
- проверка целостности данных;
- подтверждение получения данных;
- регистрация получения данных.

В рамках выходного контроля реализуется комплекс мер по предотвращению использования ресурсов неавторизированными субъектами.

При выбытии персонала из системы должна быть реализована обязательная регистрация выбытия, дезактивация персональных идентификаторов, паролей, счетов и других ресурсов.

В отношении ЭВМ и периферийного оборудования реализуются специальные процедуры инициализации, призванные предотвратить использованеи так называемого “информационного мусора”, регистрация окончания сеанса работы с удаленной системой и др.

При окончании сеанса связи должна производится регистрация об окончании, а также причину окончания. Проверка доступности канала призвана обнаружить возможные проблемы связи, с тем, чтобы предотвратить дополнительные затраты времени на ее восстановление.

Другой мерой является специализация канала, т.е. использование определенных каналов для осуществления только однотипных сеансов с тем, чтобы уменьшить доступ потенциальных нарушителей.

При окончании программных процессов должна быть сделана соответствующая запись в системном журнале с указанием причины окончания (нормальное или принужденное). В случае, если процесс закончился аварийно необходимо освобождение захваченных им ресурсов.

Весьма важным моментом является предоставление информации. Современные АИС характеризуются постоянным обменом информацией между ними. Поэтому при каждом выбытии информации обязательно должна производится шифрование и/или подпись с помощью средств реализации электронно-цифровой подписи (ЭЦП), а также ее регистрация и получение подтверждения от удаленной системы о принятой информации.