3.3. Организационные и административные методы защиты информации

Блок организационно - технического и технологического обеспечения включает средства защиты от несанкционированного доступа в каналах, сетях и системах, в физическую и логическую среду, а также механизмы контроля за целостностью ресурсов и информации. В [135] рассматриваются основные компоненты и требования к организационно-административному контуру обеспечения защиты. Среди основных проблем организационно-административного характера рассматриваются проблема организации контроля доступа, применимость мер защиты, проблемы восстановления АИС, кадровую политику и проблемы обучения пользователей, распределение работ, ответственность и др.

Блок мер связан с реализацией следующих групп мероприятий, осуществляемых по отношению к основным компонентам АИС (рис. 20) [111]:

1. *Входной контроль* состоит в осуществлении комплекса мероприятий, призванных предотвратить проникновение в АИС недобросовестных пользователей и работников, использование недоброкачественной вычислительной техники и периферии, программного обеспечения, а также информации.

Входной контроль по отношению к персоналу и пользователей осуществляется посредством следующих специальных мероприятий:

- *специальная кадровая политика* - выдвижение специальных требований к персоналу, ведение дел только с хорошо зарекомендовавшими себя клиентами (пользователями);
- *тестирование кандидатов на рабочие места* - многостороннее тестирование кондидатов на рабочие места, с тем, чтобы выявить самых подходящих для конкретных рабочих мест. Проблема защиты информации будет значительно облегчена, если безответственный или

нечестный работник будет выявлен до того, как его возьмут на работу, или по крайней мере до того, как он проявит свои отрициательные качества [125,5,90,118 и др.];

- *подписка о неразглашении тайны* - подписание пакета договоров, призваных обеспечить защиту коммерческой тайны конкретной организации, а также защитить организацию от принятия на работу людей, которые обладают коммерческой тайной другой организации.

По мнению экспертов [81] информационная безопасность АИС на 80% зависит от правильного подбора, расстановки и воспитания его персонала. При этом, идеальным рассматривается работник, обладающим следуюшим набором качеств: честность, принципиальность, исполнительность, пунктуальность, дисциплинированность, эмоциональная устойчивость, стремление к успеху и порядку в работе, самоконтроль в поступках и действиях, правильная оценка собственных возможностей и способностей, умеренная склонность к риску, осторожность, умение хранить секреты, тренированное внимание, хорошая память.

По отношению к средствам вычислительной техники входной контроль осуществляется с помощью следующих мероприятий:

- *приобретение вычислительной техники и средств защиты информации, соответствующих стандартам и удостоверенных сертификатом качества* по уровням защищенности, исключая таким образом использование вычислительной техники сомнительного происхожденеия и неопределенного качества [94,126,116]. В этой связи стандарты имеют особое значение в решении рассматриваемых вопросов. Наряду с рядом других, должны быть разработаны и утверждены стандарты, соответствующие уровням защищенности. В [158] предлагается рассматривать два основных стандарта - для государтсвенных и для коммерческих АИС;

- *организация местного тестирования* для выявления возможных несоответствий, описанных в сертификате и/или заказанной спецификации.

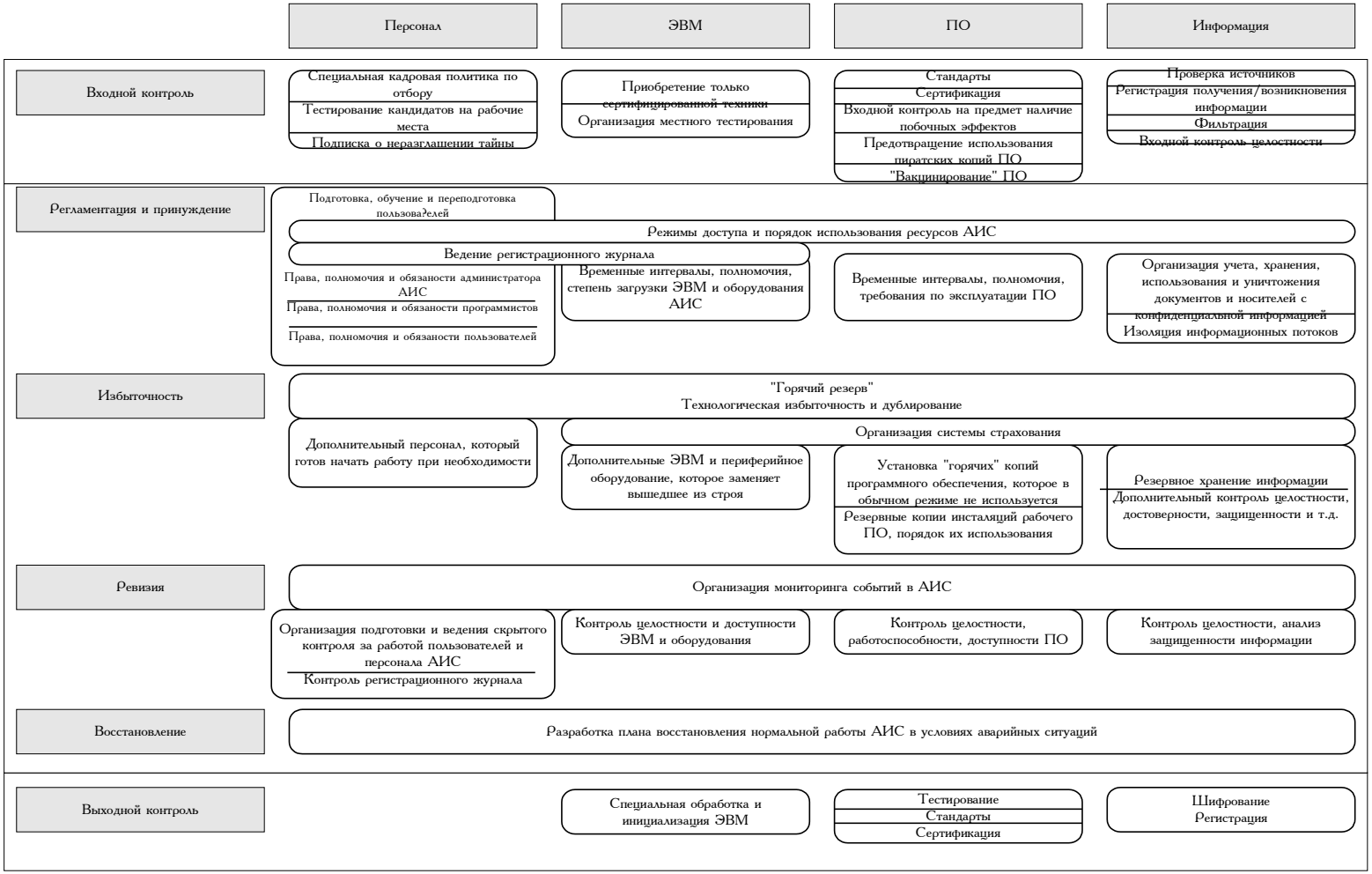

Рис. 20 Состав организационно-технологических методов и средств обеспечения информационной безопасности АИС по объектам и операционным этапам.

Для осуществления входного контроля программного обеспечения реализуется следующий комплекс работ, призванный исключить использование некачественного программного обеспечения:

- *приобретение только сертифицированного ПО*, тем самым предотвращая использование заведомо некачественного ПО;
- *реализация местного тестирования ПО* на предмет выявления побочных эффектов, в том числе, таких как “люки”, программные закладки и др.;
- *предотвращение использования “пиратских” копий ПО*. Это касается компьютерных игр, которые имеют самый высокий “оборот” нелегальных копий и являются идеальной средой для программных злоупотреблений;
- *организация “вакцинирования” ПО*. Данное мероприятие осуществялется в целях предотвращения “заражения” определенными компьютерным вирусами.

Входной контроль для информации и данных является ресурсоемким процессом, который призван обеспечить соблюдение таких показателей качества и безопасности данных, как конфиденциальность, достоверность и целостность. Реализуется за счет проведения следующих организационных мероприятий:

- *организация проверки источников информации* - является основным мероприятием, призванным предотвратить подлог информации;
- *организация мероприятий по регистрации получения/ возникновения информации* - призванные обеспечить учет возникновения информационных потоков в предметной области;

- *организация фильтрации информации* - обеспечивающая выявление и удаление так называемого “информационного мусора”, который затрудняет обработку информации, занимает ресурсы и т.д.
- *контроль целостности информации*, позволяющий выявить случаи неправомерного изменения информации;
- другие.

2. *Регламентация и принуждение*. В эту группу входит комплекс мероприятий, регламентирующих взаимодействие основных компонентов АИС: персонала, средств вычислительной техники и периферии, программного обеспечения и данных, а также взаимодействия с другими АИС .

Основные мероприятия, которые должны быть реализованы - разработка режимов доступа и порядка использования ресурсов АИС. Кроме того, должно быть организовано ведение регистрационного журнала доступа пользователей к ресурсам.

В ходе данных работ должны быть осуществлены мероприятия по подготовке и переподготовке пользователей в рамках которых им должно быть объяснено с какой информацией они работают, почему для организации важно, чтобы она была соответственно защищена, какие методы и средства применяются и т.д. Только корректное использование средств защиты может привести к желаемому результату.

Разрабатываются специальные регламентирующие документы, определяющие права, полномочия и обязаности администраторов, программистов и пользователей АИС.

В отношении средств вычислительной техники должны быть определены временные интервалы, полномочия, режимы работы, степень загрузки ЭВМ, их устройств и др.

Также должны быть описаны и доведены до сведения пользователей временные интервалы, полномочия и требования по эксплуатации программного обеспечения.

В процессе организации работ по защите информации необходимо организовать систему учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией.

Также должна быть реализована изоляция информационных потоков разных уровней.

3. *Избыточность.* Этап представляется как совокупность дополнительных мероприятий, в обычных условиях не обязательных, обеспечивающих повышение надежности обработки данных в АИС. Данные мероприятия влияют на все компоненты АИС, но и главным образом на технологический процесс обработки данных.

Обеспечивая надежность обработки данных, в том числе и за счет использования их избыточности данную проблему необходимо рассматривать комплексно. При этом важно располагать так называемым “горячий” резервом для возможных “узких” мест, имея ввиду полное дублирование и приведение в готовность тех технологических участков, от работы которых зависит успешная жизнедеятельность АИС.

Другим аспектом является технологическая избыточность и дублирование, применимых по отношению ко всем критическим компонентам АИС. Технологическая избыточность предусматривает дублирование некоторых технологических операций в целях исключения ошибок (например, ввод информации, ее передача, многократная проверка источников, некоторые виды расчетов и т.д.).

Дублирование связано с созданием некоторой совокупности дополнительных компонентов АИС, которые в обычном режиме не используются, в том числе и следующих:

- *избыточность персонала* - наличие на рабочем месте дополнительного персонала, занимающегося в обычном режиме другой деятельностью, и приступающего к работе на “критическом” участке в случае необходимости;
- *избыточность ЭВМ и периферийного оборудования*. Связано с созданием резерва ЭВМ и периферии, в обычном режиме не используемого, но которым заменяются вышедшие из строя средства и устройства;
- *избыточность ПО*. Под ней имеется в виду установка на одном компьютере “горячих” копий ПО, в обычном режиме неиспользуемых, но заменяющих вышедших из строя рабочих копий ПО. Другим важным моментом является организация хранения пакетов инсталяций программного обеспечения и порядок учета их использования;
- *избыточность информации и данных*. Состоит в реализации комплекса мероприятий, обеспечивающих надежность хранения и использования информации. В рамках данного комплекса реализуется резервное копирование и хранение данных, а также организация дополнительного контроля целостности, достоверности и защищенности данных. При реализации комплекса работ по обеспечения избыточности данных следует придерживаться следующих правил, отраженных в [59]:

♦ определить для каких типов программ и данных нет необходимости предусматривать резерв, либо надо предусмотреть только внутренний резерв, либо и внутренний и внешний резервы;

- использовать в качестве резерва для жестких магнитных дисков накопитель на магнитной ленте;
- осуществить копирование в конце рабочего дня содержимого жестких дисков и уничтожение исходных данных на них;
- осуществить периодическое копирование информации в процессе работы. Частота копирования выбирается из соображений минимизации среднего времени на копирование и времени восстановления информации после последнего копирования в случае порчи модифицированной версии;
- осуществить обучение пользователей навыкам организации резервирования программ и данных;
- при использовании накопителей на магнитных лентах или гибких магнитных дисках целесообразно создание нескольких копий данных, помещенных в специальные хранилища.

4. *Ревизия*. Представляется в виде совокупности мероприятий, ориентированных на выявление фактов неправильного и неправомерного взаимодействия компонентов АИС.

В рамках данных мероприятий следует организовать разносторонний и многофункциональный мониторинг АИС с целью выявить отклонения в работе АИС, причины возникновения, а также пути их преодоления.

Под *мониторингом системы* понимается получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля [30].

По отношению к персоналу должен быть организован и проведен скрытый контроль работы. Данное мероприятие необходимо для выявления нарушений регламента и режимов эксплуатации АИС. Возможные нарушения могут быть выявлены во время проверки

регистрационного журнала. Анализ содержимого системного журнала должен помочь выявить средства и априорную информацию, использованные злоумышленником для осуществления нарушения.

Периодически необходима проверка целостности, работоспособности и доступности ЭВМ и оборудования. Проверка осуществляется с использованием разных режимов доступа и работы, с целью выявления возможных нарушений или нештатных ситуаций.

Проверка целостности программного обеспечения должна осуществляться в двух режимах в ручном и автоматическом. В автоматическом режиме она должна осуществляться как системным программным обеспечением, так и специальными программными модулями, предотвращающими и/или регистрирующими все попытки нарушенать целостность названного обеспечения. Последующий анализ регистрационного журнала позволяет выявить как попытки, так и нарушения целостности.

Проверка работоспособности и доступности программного обеспечения состоит в проведении комплекса постоянных мероприятий, призванных выявить возможные нарушения доступности данного вида обеспечения.

На основе мониторинга системы, призванный вовремя выявить нарушения или условия, приводящие к нарушению целостности, доступности и защищенности информации, в АИС проводится анализ соблюдения этих характеристик ее данных.

5. *Восстановление.* Сводится к выполнению комплекса мероприятий по восстановлению нормальной работы АИС.

Черезвычайные ситуации обычно трудно предсказуемы и плоды человеческого труда, активы компании могут быть уничтожены за

считанные минуты. Причиной могут быть стихйные бедствия или преднамеренные преступные действия злоумышленников.

Поэтому очень важно, чтобы после подобного рода ситуаций восстановление деловой активности была четко спланирована. Централизованное управление процессом восстановления в черезвычайных ситуациях важно для поддержания деятельности компании в критических ситуациях, ее способности предоставлять клиентам хотя бы минимум услуг. Ввиду того, что способность предоставлять услуги, определяет их конкурентоспособность, центральные отделения информационных систем такого рода компаний должны вести разработку мер по восстановлению всей их деятельности. В случае, когда информационная система компании основывается на технологии на базе мэйнфрэймов, вопросы разработки и планирования процесса восстановления гораздо проще, чем для компаний, информационные системы, которых основаны на использовании технологий клиент/сервер. Кроме того, использование в распределенных вычислительных средах технологии от нескольких поставщиков создает многочисленные предпосылки для нарушений в работе, что еще больше усложняет восстановление нормального функиционирования информационной системы в черезвычайных ситуациях.

Среди самых распространенных методов обеспечения надежности и восстановления нормальной работы системы можно выделитьтаких, как создание “горячего” или “холодного” центра восстановления.

Восстановление - это сложная задача, так как центральные информационные службы слабо контролируют распределенные информационные ресурсы компании или осуществляют контроль совместно с администрацией локальной сети. Центральная служба не в состоянии контролировать всю систему в целом, в связи с чем

необходимо разработать комплекс документов, определяющих основные шаги и мероприятия по восстановлению нормальной работы. Такого рода документы называют также планом восстановления нормальной работы АИС и он должен быть разработан для каждой конкретной такой системы.

В рассматриваемом плане восстановлени должны найти отражение следующие основные моменты[30]:

- *возможные нарушения* нормальной работы АИС;
- *немедленная реакция на нарушения*, реализуемая на основе действий пользователей, персонала и администрации в момент обнаружения нарушения;
- *оценка ущерба от нарушения* на характеристики потерь и их стоимости (включая и восстановление);
- *возобновление обработки информации.* После устранения нарушения и первичного восстановления необходимо как можно быстрее возобновить работу;
- *полное восстановление функционирования системы.* Состоит в удалении и замене поврежденных компонентов системы и возобновлении обработки информации в полном объеме.

6. *Выходной контроль.* Этап сводится к реализации совокупности работ по предотвращению утечки конфиденциальной информации с внещних компонентов АИС.

Уволившимся работникам напоминается о подписанном договоре о неразглашении коммерческой тайны. Кроме того, если уволившийся работник поступил на работу к конкуренту, необходимо послать письмо конкуренту и сообщить о том, что конкретный работник, который устроится у него на работу обладает коммерческой тайной и если она будет разглашена, то на него будет подано в суд.

В случае морального устаревания или выхода из строя ЭВМ либо периферийного оборудования продаются или безвоздмездно передаются другому пользователю. Перед тем как осуществить это важно выполнить комплекс работ по инициализации ЭВМ и оборудования.

В отношении разработанного в АИС программного обеспечения, следует иметь в виду, что оно должно соответствовать существующим стандартам и требованиям, определяющим конкретный класс ПО; перед его выпуском необходимо провести полное многофункциональное тестирование; последним этапом является получение сертификата соответствия конкретному классу защищенности.

Передача данных из АИС должна регистрироваться в специальном журнале, который может быть как автоматизированным, так и ручным. Кроме того, должно быть организовано шифрование исходящей информации с помощью электронной подписи, что решит многие проблемы по аутентификации источника данных.

Считаем необходимым отметить необходимость стандартов при разработке, внедрении и эксплуатации АИС и системы информационной безопасности. На сегодняшний день разработано несколько основных стандартов, призваных помочь в унификации используемых подходов и методов при проектировании СИБ.

Первые шаги при разработке стандартов в области информационной безопасности были сделаны в США, где разработан пакет документов (так называемая “Радужная серия") [178-182 и др.], регламентирующих проектирование с определенным уровнем безопасности военных АИС. Если для АИС военного назначения разработанные требования являются обязательными, то для коммерческих автоматизированных информационных систем они являются рекомендательными. На сегодняшний день документация

“радужной серии” закладывается в основу проектирования систем информационной безопасности многих коммерческих (особенно банковских) АИС и используется в других странах.

В России разработан пакет документов аналогичного назначения [46-51]. На их основе производится сертификация средств защиты информации. Для коммерческих АИС они также являются рекомендательными.

Таким образом, можно отметить, что организационно - административные методы и средства обеспечения информационной безопасности составляют базис, на котором основываются и совершенствуются другие методы и средства защиты информации.