С.А. Прохоров, А.А. Федосеев,
В.Ф. Денисов, А.В. Иващенко

Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения

Самара 2009

УДК 006.88, 007.51

Рецензенты:

декан механико-математического факультета Самарского государственного университета, заведующий кафедрой безопасности информационных систем д.ф.-м.н., профессор В.И. Астафьев;

президент консорциума «Интегра-С», академик всемирной академии наук комплексной безопасности В.А. Куделькин.

Прохоров С.А., Федосеев А.А., Денисов В.Ф., Иващенко А.В.
Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения // Самара: Самарский научный центр РАН, 2009 – 199 с., ил.

ISBN 978-5-93424-409-6

Рассматриваются новые направления проектирования функционально-полных профилей прикладных автоматизированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения. Издание предназначено для специалистов служб безопасности, информационных служб и служб автоматизации предприятий наукоемкого машиностроения, предприятий инфраструктуры инновационного развития регионов. Отдельные материалы могут быть полезными для разработчиков средств безопасности, а также для студентов специальностей «Автоматизированные системы обработки информации и управления», «Комплексное обеспечение информационной безопасности автоматизированных систем».

ISBN 978-5-93424-409-6

Печатается по решению издательского совета Самарского научного центра Российской академии наук

Содержание

Список сокращений

АИС – Автоматизированная информационная система;
АС – Автоматизированная система;
АСНИ – Автоматизированная система научных исследований;
АСУТП – Автоматизированная система управления техпроцессами;
БД – База данных;
БИР – Безопасность информационных ресурсов;
БТО – Безопасность технологического оборудования;
ЕИП – Единое информационное пространство;
БП – Безопасность продукции;
ДПД – Диаграмма потоков данных;
ИСОКБП – Интегрированная система обеспечения комплексной безопасности предприятия;
ИТ – Информационные технологии;
ИКТ – Информационно-коммунникационные технологии;
ЛПР – Лицо, принимающее решение;
НСД – Несанкционированный доступ на объекты предприятия;
ОТС – Организационно-техническая система;
ПЗ – Профиль защиты;
ПМК – Программно-методический комплекс;
ПО – Программное обеспечение;
ПТК – Программно-технический комплекс;
САПР – Система автоматизированного проектирования;
СУБД – Система управления базами данных;
СЭВП – Системы электронного взаимодействия предприятий;
ТЗ – Техническое задание;
ТЭО – Технико-экономическое обоснование;
ЧС – Чрезвычайная ситуация;
ЭБ – Экономическая безопасность;
ЭВМ – Электронная вычислительная машина;
CALS – Continuous Acquisition and Life cycle Support, Непрерывное развитие и поддержка жизненного цикла (продукта, изделия);
SOA – Сервис ориентированная архитектура;
UML – Унифицированный язык моделирования.

Предисловие

Данная работа посвящена решению актуальной задачи обеспечения комплексного, согласованного и централизованного характера управления безопасностью предприятия, как сложной организационно-технической системой. В ней содержатся рекомендации и обобщения, которые будут полезны специалистам, занимающимся созданием и развитием системы обеспечения безопасности предприятий, особенно в том случае, если им приходится решать эту задачу впервые.

В основу работы положены современные подходы к построению архитектуры предприятий, методология открытых систем, международные и Российские стандарты описания продукции, процессов и ресурсов предприятий. Предложена системная классификация рисков, методы анализа процессов и рекомендации по проектированию и выбору средств мониторинга угроз безопасности и обеспечения устойчивости, надежности, качества и безопасности целевых и обеспечивающих автоматизированных систем предприятия.

Авторами предлагается систему обеспечения комплексной безопасности предприятия структурно представить в виде спецификации программно-технических и программно-методических комплексов, которые вместе образуют профиль интегрированной системы, то есть согласованный набор базовых стандартов, необходимых для решения определенного класса задач. Данный профиль может стать основой для построения концепций управления комплексной безопасностью на различных предприятиях наукоемкого машиностроения.

Авторы выражают благодарность за поддержку ректору Самарского государственного аэрокосмического университета, члену-корреспонденту РАН, профессору В.А. Сойферу, генеральному директору ГНПРКЦ «ЦСКБ Прогресс» д.т.н., профессору А.Н. Кирилину, первому заместителю генерального директора – генеральному конструктору ГНПРКЦ «ЦСКБ Прогресс» к.т.н. Р.Н. Ахметову.

Также авторы выражают благодарность за ценные замечания рецензентам: декану механико-математического факультета Самарского государственного университета, заведующему кафедрой безопасности информационных систем д.ф.-м.н., профессору В.И. Астафьеву и президенту консорциума «Интегра-С», академику всемирной академии наук комплексной безопасности В.А. Куделькину.

Введение

С самых ранних времен возникновения социально-производственных отношений в обществе вопросы обеспечения безопасности жизни человека, его продуктивной деятельности и общества в целом являются главными для сохранения целостности и устойчивости к различного рода внешним воздействиям окружающей среды обитания человека, начиная с защиты жилья, личной безопасности человека от зверей и чужих людей, негативных природных явлений, обеспечения безопасности промыслов и производства изделий для потребления, и кончая недружелюбными действиями других лиц и их группировок.

С развитием промышленных технологий производства продукции наблюдается усиление конкуренции между производителями, и вопросы обеспечения целостности, устойчивости деятельности и обеспечения безопасности предприятий выходят на передний план, становятся основной «головной болью» владельцев, управляющих и персонала предприятия.

Исторически сложилось так, что вопросами безопасности предприятий занимаются различные организационные структуры предприятия (охрана, разработчики изделий и технологий, охрана труда, энергетики, информационные службы и др.) в рамках своих компетенций, прав и обязанностей. Каждая из этих служб применяет в своей деятельности определенные модели процессов и средства обеспечения безопасности.

В связи с развитием продукции, технологий производства и усложнением основных процессов предприятий, развитием кооперационных связей предприятий и их интеграции в процессы инновационного развития общества существенно изменяются условия функционирования предприятий. Борьба за рынки сбыта, ограниченные ресурсы и сохранение сфер своего влияния приводит с одной стороны к применению все более изощренных способов нанесения вреда действующим предприятиям, а с другой к формированию эффективных высокотехнологичных средств защиты от различного рода посягательств на целостность предприятия и его безопасность.

Можно утверждать, что к настоящему времени в развитых странах сформировалась «индустрия безопасности», в которой работают большие коллективы и малые группы различных

специалистов, разрабатывающих средства нападения и защиты предприятий, включая такие направления, как законодательство и способы уклонения от его выполнения, средства экономической разведки, промышленного шпионажа, электронной разведки и защиты информации, физического воздействия и физической зашиты человека, зданий и сооружений, идентификации продукции, пожарной и охранной сигнализации, видеонаблюдения и др.

Деятельность таких коллективов, как правило, регламентируется государством и относительно крупными промышленными корпорациями, но не исключено, что результатами этих работ и продуктами рынка индустрии безопасности могут воспользоваться и различного рода нарушители: отдельные физические лица (по причине простого незнания и «разгильдяйства»), конкуренты, организованные преступные группировки (в сферах экономики, производства контрафактной продукции, воровства и бандитизма, национального и международного терроризма), а также спецслужбы иностранных государств.

Существенно изменяются возможные источники угроз безопасности предприятия, методы и средства их инициализации и реализации: от несанкционированного доступа на предприятие, попыток ликвидации отдельных объектов, до получения конфиденциальных данных и попыток захвата предприятия и, часто имеющих место быть в новой российской практике, недружественных поглощений. Все это и заставляет искать новые адекватные средства обнаружения и контроля угроз безопасности, оценки рисков и разработки мер по их устранению, нейтрализации и снижению ущерба в деятельности предприятия.

Можно утверждать, что к настоящему времени индустрия безопасности обеспечивает технические возможности практически полного «тотального» контроля всех объектов и субъектов безопасности на разных уровнях государства и предприятий, однако необходимо учитывать правовые, психологические и морально-этические аспекты создания и функционирования таких систем. Помимо технических, организационных и финансовых аспектов, необходимо решение общезначимых проблем законности, обеспечения достоверности и своевременной актуализации данных, целесообразного уровня информированности персонала и контрагентов о возможностях системы, способов доступа к информационным ресурсам, прикладным аналитическим программам

и моделям обеспечения безопасности. Поэтому на передний план выступают задачи мотивации заинтересованных лиц и формирования целевого назначения таких систем с учетом различных позиций различных групп пользователей и коллектива предприятия и обеспечения корректной постановки задачи обеспечения безопасности предприятия как сложной организационно-технической системы.

В этих условиях применение отдельных локальных систем обеспечения безопасности является недостаточно эффективным. Решения по обеспечению безопасности с позиций отдельных структур предприятия и лиц, принимающих решения на разных уровнях управления могут находиться в противоречии. В последние годы на ряде предприятий начинают развиваться специализированные службы обеспечения комплексной безопасности.

Основные задачи таких служб: координация работ всех подразделений предприятия по вопросам обеспечения безопасности на всех уровнях управления (предприятие в целом, подразделения и процессы предприятия, рабочие места персонала), планирование общих и частных мероприятий по обеспечению безопасности предприятия, поддержание в рабочем состоянии общих и специализированных средств обеспечения безопасности, организация взаимодействия со службами безопасности государства, регионов и муниципальных образований и контрагентов.

Деятельность распределенных служб безопасности предприятия должна обеспечиваться соответствующими регламентами, процессами, моделями оценки сложности объектов и процессов контроля безопасности, средствами мониторинга событий угроз безопасности и оценки рисков, распределения ресурсов и планирования мероприятий.

К настоящему времени в среде специалистов сложилось и понятие комплексной безопасности предприятия [7, 42, 45], суть которого состоит в интеграции всех необходимых и достаточных средств организационно-правового, методического, информационного, технического и программного обеспечения всех основных целевых и обеспечивающих процессов предприятия, физической защиты зданий и сооружений, безопасности использования различного рода материальных и информационных ресурсов.

Однако до настоящего времени интеграция различных средств обеспечения безопасности в практической деятельности предприятий не находит должного применения в силу ряда обстоятельств, главные из которых – это отсутствие мотивации ключевых лиц и персонала предприятий, реальная сложность описания объектов, процессов и внешних связей предприятия и, соответственно, оценки угроз их безопасности, проблемы применения «наследуемых» информационных систем и технологий и их интеграции со средствами обеспечения безопасности. Не менее важную роль при этом играют и такие факторы, как нестабильность законодательства, неустойчивость рынка продукции и услуг, общая культура предприятия, наличие необходимых знаний, навыков и умений и, конечно, наличие условно «свободных» ресурсов, необходимых для реализации проектов безопасности и их эксплуатации.

Цель данного издания – обобщение имеющегося опыта разработок систем безопасности, анализ современных тенденций их развития и формирование на этой основе основных концептуальных положений, методик, технологий и инструментов анализа процессов предприятий наукоемкого машиностроения с позиций обеспечения их безопасности, разработки рекомендаций по проектированию и выбору необходимых и достаточных средств сбора и обработки данных для принятия согласованных решений по нейтрализации возможных угроз безопасности и минимизации рисков в деятельности на всех стадиях жизненного цикла изделий на разных уровнях управления.

В настоящей работе вопросы выбора функционально-полного комплекса методов и средств обеспечения безопасности предприятий наукоемкого машиностроения рассматриваются с точки зрения развивающейся методологии открытых информационных систем [8, 12] и архитектурного подхода [1] к построению профилей прикладных автоматизированных систем обеспечения деятельности предприятий [12, 21, 22], а также применения типовых проектных решений в сфере информационно-коммуникационных технологий (ИКТ).

Применение архитектурного подхода, системных матриц обеспечения деятельности предприятия и моделей жизненного цикла организационно-технических систем в соответствии с международным стандартом ИСО/МЭК 12207 «Процессы жизненного цикла систем» позволило определить системную классификацию объектов и субъектов безопасности предприятия, и связанных с ними угроз безопасности и рисков в деятельности как основы для разработки моделей про-

цессов обеспечения безопасности предприятия, постановки задач и определения требований к выбору методов и средств их реализации.

При постановке и решении задач обеспечения комплексной безопасности предприятий можно выделить три основных момента.

Во-первых, необходимо обеспечить комплексный характер управления безопасностью предприятия, то есть интегрировать все техническое, программное, информационное и организационное обеспечение системы безопасности предприятия и обеспечить согласованный и централизованный характер управления безопасностью.

Для этого необходимо обеспечить упорядочение и выделение основных ключевых процессов предприятия, внутренних и внешних рисков нарушения их целостности, определить общесистемные приоритеты и обеспечить действительно комплексный характер управления безопасностью предприятия, то есть интегрировать все организационные, информационные, технические и программные средства различных систем (подсистем) безопасности и обеспечить согласованный и гармонизированный характер управления безопасностью на разных уровнях управления в зависимости от уровня интенсивности внешних воздействий и возможных последствий угроз безопасности конкретного вида.

Во-вторых, при проектировании интегрированной системы обеспечения комплексной безопасности предприятия, требуется предусмотреть возможность ее эволюционного развития в соответствии с особенностями функционирования предприятия.

Для этого необходимо разработать функционально-полную распределенную систему так называемых «Услуг и профилей безопасности» для всех ключевых процессов предприятия в соответствии с особенностями функционирования предприятия на рынке, характеристиками продукции предприятия, ресурсов и услуг подразделений, потоками внутренних и внешних воздействий, состояния процессов и средств их автоматизации, предусмотреть «встраивание» средств мониторинга и идентификации угроз безопасности (желательно автоматических) и возможности их эволюционного развития.

Методы и алгоритмы управления безопасностью конкретных процессов должны быть достаточно универсальными, основанными на общих положениях теории управления (логическое управление по наличию дискретных сигналов, управление по отклонению

контролируемого параметра, программное управление комплексом действий и мероприятий по обеспечению безопасности и др. более сложные и адаптивные алгоритмы) и при появлении новых видов угроз, обеспечивать возможность применения средств обеспечения безопасности общего и специального назначения, аттестованных или сертифицированных, соответствующими государственными или отраслевыми организациями, и рекомендованных для применения в условиях конкретной отрасли и предприятия.

В третьих, для обеспечения эффективности, в основе своей индивидуальных, проектов обеспечения комплексной безопасности конкретных предприятий, необходимо учитывать возможности современных инструментальных средств построения распределенных баз данных информационных ресурсов предприятия, применения типовых проектных решений в сфере автоматизации процессов предприятия и информационно коммуникационных технологий, используемых как в основных процессах предприятия, так и при обеспечении его безопасности.

Особенно актуально решение этой задачи на предприятиях наукоемкого машиностроения, в связи с тем, что на таких предприятиях, как правило, реализуются достаточно сложные бизнес-процессы, включающие прикладные научные исследования, проектирование сложных изделий, подготовку производства, и собственно управление производством, высокие требования по обеспечению безопасности, и наличие большого объема информации, подлежащей защите.

Построение интегрированной системы обеспечения комплексной безопасности предприятия (ИСОКБП) наукоемкого машиностроения затруднено на наш взгляд в связи со следующими факторами:

- негибкость исторически сложившейся структуры предприятия, бизнес-процессов и наличие достаточно жестких правил документирования проектов;
- большой объем разрешительной и регламентирующей документации и сложное, часто неформальное, разделение зон ответственности исполнителей существенно усложняет задачу анализа состояния безопасности подразделений и предприятия в целом;
- недостаточная мотивация и информированность персонала предприятия по отношению к ограничениям их деятельности,

связанным с обеспечением безопасности может вызывать открытое или скрытое сопротивление при внедрении средств централизованного мониторинга безопасности;

- необработанность регламентов, организационно-экономических механизмов и инструментальных средств мониторинга состояния уровня безопасности в подразделениях для выработки общих и частных рекомендаций по устранению текущих и прогнозируемых возможных угроз безопасности затрудняет решение задач ведения базы данных о ресурсах безопасности, поддержания ее в актуальном состоянии в соответствии с текущими и планируемыми изменениями на предприятии;
- наличие на предприятиях наукоемкого машиностроения достаточно большого количества разнообразных, разработанных на разных концептуальных и программно-аппаратных платформах систем автоматизации основных процессов (АСНИ, САПР, управление производством, материальными и финансовыми ресурсами и др.) затрудняет решение задач унификации процессов сбора и обработки данных, протоколов и форматов обмена данными между заинтересованными и «нужными» для принятия оперативных решений.

Вместе с тем, актуальность решения задач обеспечения комплексной безопасности предприятий подтверждается фактическим состоянием нашей и мировой экономики. К настоящему времени сложились определенные предпосылки и накоплен определенный опыт их решения на разных уровнях управления. В рамках работ по стандартизации, проводимых государственными и общественными профессиональными организациями (международными и национальными комитетами и рабочими группами по стандартизации), разработчиками ИКТ, средств и систем безопасности сложился определенный понятийный аппарат в сфере обеспечения надежности организационно-технических систем, качества информационных систем и обеспечения комплексной безопасности.

В соответствии с этими подходами основным инструментом интеграции различных систем является упорядочение и гармонизация применяемых на предприятии различных стандартов и технических решений, их анализ на соответствие продукции, процессам и ресурсам предприятия и формирование проектным путем ограниченного функционально-полного набора необходимых и

достаточных средств обеспечения того или иного вида деятельности. В соответствии с рекомендациями [12] такой упорядоченный и ограниченный набор стандартов, спецификаций требований к компонентам и описания основных проектных решений в сфере обеспечения безопасности процессов предприятия будем называть **профилем** интегрированной системы обеспечения комплексной безопасности предприятия.

В данной работе сформулированы основные положения разработки профилей и концепции построения интегрированной системы обеспечения комплексной безопасности предприятия и предложена базовая архитектура комплекса средств информационных технологий служб обеспечения безопасности, ориентированная на разработку сервисов «услуг безопасности» для всех основных объектов, процессов и субъектов предприятия.

В состав такого профиля входит описание основных компонентов интегрированной системы обеспечения безопасности предприятия, включая определения объектов и субъектов безопасности, процессы мониторинга и идентификации инцидентов-угроз безопасности, общесистемные требования к формированию информационной среды и распределенных служб обеспечения безопасности, требования к процессам обработки и представления данных для принятия решений на разных уровнях управления. Профиль может стать основой для построения концепций, общих и частных проектов автоматизации управления комплексной безопасностью на различных предприятиях наукоемкого машиностроения.

1 Состояние и проблемы обеспечения комплексной безопасности предприятий наукоемкого машиностроения

Модель устойчивого развития любого, а особенно наукоемкого предприятия, является результатом эволюции, накопленного опыта, грамотной научно-технической политики, должного взаимодействия с органами государственной власти и местного самоуправления и другими различными инфраструктурами поддержки, инновационной деятельности, а также соответствия принятым концепциям безопасности общества и государства [19].

В случае эволюционного развития и в периоды кризисных ситуаций работают методы «проб и ошибок», основанные на «броуновском движении» различных институтов общества (организационных структур государства, владельцев предприятия, научных и производственных коллективов предприятия и др.) в направлении достижения «желаемых» результатов многогранной деятельности предприятия, определяемых, не всегда совпадающими, а часто и противоположными, частными и групповыми интересами, мотивами совместной продуктивной деятельности или осознанных и неосознанных негативных воздействий на предметы деятельности предприятия.

Обеспечение безопасности деятельности всегда являлось важнейшей задачей общества, а с развитием промышленных технологий расширяется не только спектр потенциальных угроз безопасности, но и усложняются применяемые методы их обнаружения, противодействия внешним факторам окружающей среды и нейтрализации негативных воздействий на объекты и субъекты деятельности предприятия.

Вопросами обеспечения безопасности занимаются практически все институты общества и, как правило, в рамках своих профессиональных интересов. Строители обеспечивают проектную техническую безопасность зданий, конструкторы борются за безопасность изделий, технологи следят за оборудованием и материалами, экологи – за состоянием среды обитания, охрана не пускает посторонних, спецслужбы следят за секретами, медики берегут наше здоровье, энергетики борются с отказами в системах энергообеспечения и т. д.

В своей непосредственной деятельности различные службы предприятия применяют соответствующие профессиональные модели и средства обеспечения безопасности, ведут более или менее объективный учет негативных событий, измеряют значения факторов безопасности и принимают более или менее приемлемые решения относительно средств обеспечения безопасности в своих предметных областях деятельности.

Однако такие локальные решения не всегда учитывают межпредметные связи в реальных производственных условиях, используют различный понятийный аппарат и часто вступают в противоречие с решениями других служб. Разрешение этих противоречий выполняется путем долгих согласований различных проектов обеспечения безопасности изделий, технологий, зданий и персонала, а в условиях дефицита времени при обнаружении угроз безопасности – на основе знаний и опыта лиц, принимающих решения (ЛПР), и административного ресурса на соответствующем уровне управления предприятием.

Не менее важную, а в критических ситуациях и определяющую, роль играет определение согласованных механизмов реализации мероприятий по обеспечению безопасности, их правового, нормативно-методического, технического и программного обеспечения и их исполнения специализированными службами безопасности и оперативным персоналом.

Отсутствие на предприятиях общих концепций и согласованных проектов безопасности приводит к неэффективному использованию имеющихся ограниченных ресурсов, «войнам в проектах» и повышенным рискам.

Для современных предприятий наукоемкого машиностроения, работающих в конкурентной среде, задачи определения различного рода рисков, их минимизации и нейтрализации с минимальными затратами является первостепенными и приоритетными для всех сфер деятельности и уровней управления. Вместе с тем, можно констатировать, что фактическое состояние ведущих предприятий объективно отражает факт отсутствия согласованного комплекса междисциплинарных моделей развития методов и средств обеспечения комплексной безопасности, учитывающего различные аспекты деятельности предприятий в обществе.

Следует признать бесперспективными попытки создания такой модели в рамках отдельных профессиональных школ и предметных

отраслях знаний. Вместе с тем известно, что большинство проблем управления современными предприятиями решается с применением интеллектуальных ресурсов, играющих роль производительной силы, способной преодолеть многие негативные явления в обществе. В этой связи интеллектуальные ресурсы предприятия, а также поддерживающие их средства автоматизации процессов и информационно-коммуникационных технологий (ИКТ), следует рассматривать наряду с другими природными, материально-техническими и демографическими ресурсами, как основной фактор, определяющий потенциал предприятия.

Результаты интеллектуальной деятельности предприятий наукоемкого машиностроения занимают особое место в обеспечении обороноспособности государства, а также развитии сфер его экономики. Специфика работ таких предприятий заключается в том, что практически все результаты научно-технической деятельности предприятия и его многочисленных контрагентов по своему смысловому и практическому применению являются объектами двойного назначения. В соответствии с законом РФ от 13 апреля 1998 г. № 60-ФЗ «О конверсии оборонной промышленности в Российской федерации» к продукции двойного назначения следует относить:

- техническую документацию (нормативно-методическую, конструкторскую, проектную, технологическую, эксплуатационную, программную), регламентирующую проектирование, строительство и эксплуатацию, модернизацию объектов (зданий, сооружений, изделий) оборонной инфраструктуры государства;
- результаты интеллектуальной деятельности (интеллектуальную собственность), в том числе исключительные права на них;
- технологии производства работ и создания новых материалов, изделий и конструкций;
- научно-техническую документацию, регламентирующую безопасность, в том числе экологическую, техногенную, сейсмическую, пожарную безопасность при производстве и эксплуатации объектов инфраструктуры;
- стандарты безопасности для человека и окружающей среды;
- научно-техническую информацию на материальных носителях, а также изобретения, полезные модели, промышленные образцы другие результаты интеллектуальной деятельности двойного назначения;

– специальное (прикладное) программно-математическое обеспечение.

Учитывая современные тенденции интеграции на мировых рынках продукции и услуг, расширение научных и производственных связей с отечественными и зарубежными контрагентами, а главное специфические особенности предприятий наукоемкого машиностроения, от которых напрямую зависит не только качество продукции предприятия, но и поддержание различных составляющих национальной безопасности (экологической, технологической, оборонно-промышленной, продовольственной, информационной, физической и др.), весьма актуальными являются вопросы правовой охраны, защиты интеллектуальной собственности, прав владения, идентификации недоброкачественной и контрафактной продукции, определения рисков научно-технической деятельности и путей снижения ущерба от ошибок в проектах, неправомочных действий установленных и неустановленных юридических и физических лиц относительно объектов, процессов, ресурсов и субъектов предприятия.

Особое внимание в условиях нестабильной экономики, конкуренции на рынке товаров и услуг, возможности террористических угроз, недостаточной компетентности персонала, а также наличия элементарных ошибок, вызванных халатностью или усталостью персонала, в проектах предприятий должно уделяться построению комплексных систем обеспечения безопасности на всех уровнях управления и для всех ключевых процессов его деятельности.

При разработке концепции, политики и тактики обеспечения безопасности особое внимание должно уделяться применению информационных систем и технологий с учетом развития кооперационных связей машиностроительного комплекса и кластерной политики агломерации и соответствия инновационных проектов предприятия научно-техническим Программам РФ и других стран.

В последнее время в России активизировались (стали возрождаться) процессы автоматизации предприятий машиностроительного комплекса. Растущая конкуренция на рынке информационных систем и технологий со стороны западных и отечественных поставщиков требует особого внимания к обоснованию решений в области автоматизации процессов в

соответствии со стратегией развития предприятий, создания новых производств и услуг для потребителей.

В этой связи весьма актуальной становится задача защиты интеллектуальной собственности предприятия и соответствующих мер по обеспечению безопасности при проведении маркетинговых исследований рынка, подготовке и представлении инновационных проектов Предприятия на различных тендерах, конкурсах, выставках и др. мероприятиях, на которых может происходить «несанкционированная» утечка информации и инициированы угрозы безопасности предприятия.

В настоящее время наблюдается существенное увеличение роли и участия государства и инфраструктур инновационного развития в деятельности предприятий наукоемкого машиностроения, как основы поднятия экономики государства, технического обеспечения национальных проектов и улучшения социальных показателей жизненного уровня населения. Различными специалистами рекомендуется ряд достаточно строгих методов упорядочения показателей деятельности и оценки потенциала предприятий, логистических схем согласования национальных, корпоративных и местных интересов различных субъектов хозяйствования, интеграции предприятий в крупные межгосударственные, национальные и региональные проекты.

Подготовка и принятие решений по таким проектам также требует обязательного рассмотрения возможных рисков на всех стадиях жизненного цикла действующих производств и новых проектов. Это предполагает рассмотрение инновационных предложений и инвестиционных проектов предприятий с позиций обеспечения комплексной безопасности предприятия (экологической, технической, технологической, экономической, политической) на разных уровнях управления. На сегодня ясно, что проекты обеспечения безопасности и применяемые в них технологии должны быть открытыми для развития, но содержать в себе средства обеспечения конфиденциальности данных, защиты от несанкционированного доступа к информации, технической защиты помещений и оборудования и др.).

Опыт разработок и реализации ряда комплексных и целевых программ социально-экономического развития Предприятий и автоматизированных систем обеспечения их деятельности позволяет

сформулировать следующие положения концепции разработки проекта ИСОКБП:

- интеллектуальная поддержка традиционных схем управления объектами и ключевых процессов предприятия, осуществляемых действующими подразделениями и специализированными функциональными службами предприятия (служба безопасности, ИТ-служба, служба защиты интеллектуальной собственности, и др.), а также с привлечением внешних организаций вневедомственной охраны, энергоснабжения, эксплуатации зданий и сооружений, закупок материалов и комплектующих, ремонта непрофильного оборудования, профилактики здоровья и других контрагентов, работающих по договорам услуг и аутсорсинга;
- ориентация не на отдельные частные академические, производственные, технологические, экономические, правовые и прочие тиражируемые модели, а на создание функционально-полного комплекса, сегментированных для отдельных подразделений и производств, адекватных и верифицируемых моделей обеспечения безопасности деятельности с встроенными процедурами их согласования и легитимации;
- создание ситуаций актуализации процессов обеспечения безопасности деятельности, закрепленных за отдельными структурными подразделениями Предприятия с выявлением основных внутренних и внешних источников угроз безопасности, оценки рисков и их влияния на ключевые показатели деятельности подразделений и предприятия в целом;
- декомпозиция общей модели процессов обеспечения безопасности в рамках логистической схемы согласования различных экономических, производственных, бюджетных, коммерческих, ресурсных, социально-культурных и иных интересов;
- разработка общей единой открытой стратегии обеспечения безопасности предприятия и политик обеспечения безопасности ключевых процессов предприятия в сферах разработки научно-технической продукции и услуг Предприятия, производственной, технологической, экологической, физической, экономической, информационной и политической безопасности;
- разработка паспортов безопасности объектов и процессов предприятия и рекомендаций реестров функционально-полного комплекса средств организационно- методического, технического

и программного обеспечения безопасности, рекомендуемых и/или разрешенных для применения в подразделениях предприятия;

- создание реальной системы взаимодействия подразделений и лиц, принимающих решения по обеспечению безопасности на соответствующем уровне управления процессами предприятия в условиях перенасыщенной управлением и контролем внутренней и внешней среды предприятия, на основе унифицированной модели оценки рисков, разработки сценариев и программ действий по обеспечению безопасности, использования общих и специализированных баз данных с разграничением уровня доступа к ним различных категорий пользователей, а также исключения несанкционированного доступа к объектам, процессам и ресурсам системы обеспечения безопасности;
- организация независимого мониторинга состояния безопасности ключевых процессов предприятия и отдельных обеспечивающих процессов с целью выявления источников угроз безопасности, «скрытых» нематериальных активов, и упущенной выгоды, основанной на ресурсной сбалансированности процессов предприятия и новых инновационных проектов, согласования различных интересов субъектов деятельности предприятия с выявлением «общего пространства» и стимулированием конкретных мероприятий для получения синергетического и кумулятивного эффектов при использовании средств обеспечения безопасности.

Таким образом, анализ состояния, опыта разработок проблем обеспечения безопасности показывает, что в основу концепции проекта интегрированной системы обеспечения комплексной безопасности предприятий наукоемкого машиностроения могут быть положены, апробированные на различных объектах и находящиеся в развитии методологии, использующие:

- базовые функционально-полные модели деятельности предприятий, учитывающие основные системообразующие характеристики объектов предприятия и внешней среды;
- модели взаимодействия предприятий с организациями и предприятиями инфраструктуры инновационного развития общества, территориальных образований и муниципальных служб обеспечения общественной безопасности;
- современные подходы и модели оценки потенциальных опасных воздействий и рисков предприятий в научно-технической сфере;

- вычислительные и экспертно-статистические методы оценки сложности, потенциала и рисков объектов и субъектов деятельности предприятия и их ранжирования по различным критериям оценки и приоритетам;
- модели привлекательности инвестиций в инновационные проекты предприятий и их встраивания в государственные (федеральные и региональные) целевые программы, проекты социально-экономического развития территорий, межгосударственные программы научно-технического сотрудничества;
- модели и современные средства обеспечения безопасности информационных технологий (базы данных, геоинформационные системы, сети ЭВМ и др.);
- методы согласования интересов, координации действий и узаконивания решений, основанные на принятых регламентах, стандартах других и установленных обществом «правилах» соблюдения культурных и этических норм совместной деятельности корпоративных предприятий;
- технологии проблемно-ситуационного моделирования деятельности в сложных организационно-технических системах;
- автоматизированные системы проектирования технических объектов и систем управления проектами текущей деятельностью предприятий.

В последующих разделах рассматриваются дополнительные вопросы, раскрывающие и уточняющие отдельные положения рассматриваемых концепций, методологий и технологий проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения.

Отдельные положения предлагаемых методов и средств проектирования в силу своей общности и ориентации на апробированные международные и национальные стандарты могут быть также использованы для разработки профилей прикладных автоматизированных систем предприятий инфраструктуры инновационного развития регионов, органов власти и местного самоуправления, а также могут быть полезными для предприятий разработчиков аппаратных и программных средств обеспечения безопасности, которые тоже являются предприятиями наукоемкого машиностроения.

2 Архитектура предприятий и информационных технологий, объекты и субъекты обеспечения комплексной безопасности

2.1 Архитектурные модели предприятий и безопасность

За последние годы в области использования информационно-коммуникационных технологий (ИКТ) в проектах автоматизации и информатизации предприятий произошел переход к широкому практическому использованию дисциплины «Архитектура предприятия» [2]. В соответствии с современными концепциями развития архитектурного подхода в проектах автоматизированных информационных систем под Предприятием понимается любая организация, осуществляющая тот или иной вид полезной для общества и результативной деятельности и осуществляющей производство востребованной потребителями продукции и услуг, активно взаимодействующая с поставщиками разного рода ресурсов и другими контрагентами.

Уже много лет в недрах ИТ-сообщества идут дискуссии о моде на ИТ-архитектуры, умы по-прежнему будоражит идея: найти нечто, позволяющее упростить решение проблем применения ИКТ в процессах обеспечения многогранной деятельности современных предприятий. Попытаемся разобраться, необходима ли разработка модели ИТ-архитектуры для предприятий машиностроения и можно ли использовать здесь аналогии и практические рекомендации специалистов в сфере традиционной строительной архитектуры и архитектурного системного проектирования сложных организационно-технических систем (ОТС), к которым безусловно относятся и современные предприятия? У управленцев-практиков разного уровня часто возникает вопрос: «а зачем мне это надо?», ведь предприятие работает, оснащено средствами автоматизации и информационными технологиями, а при необходимости можно купить или самим разработать необходимые программные средства.

Специалисты в области ИТ им отвечают: «Архитектура, как универсальная полноценная модель предприятия, необходима для современных ИТ, как инструмент, направленный на решение проблем, связанных с обеспечением качества, надежности, эффективности и безопасности функционирования различных автоматизированных информационных систем предприятия (несвязанность приложений, отставание разработки и внедрения

программного обеспечения от темпов развития предприятия, недостаточно развитие функций программных систем и др.)»

Но понятие архитектуры предприятия имеет и более глубокий смысл, она отражает естественные человеческие потребности в обустройстве и защиты среды обитания, формирования внешнего облика, внутреннего устройства и ландшафта, средств взаимопонимания людей при совместной деятельности на основе приемлемого выбора конструктивных методов и средств жизнеобеспечения и сохранения целостности при различного рода негативных воздействий. Как и в обыденной жизни, грамотно выбранные архитектурные решения для предприятия в целом и его составных частей, позволяют решать достаточно простыми и доступными для понимания, способами задачи защиты и обеспечения безопасности любой сложности по мере их возникновения и с возможностями достаточно четкой их привязки к объектам деятельности предприятия и компонентам автоматизированных систем.

И чем труднее задача (а в случае с обеспечением комплексной безопасности она действительно очень сложна), тем настойчивее наша вера и убежденность в «волшебные средства» современных ИТ. Тем не менее, проблемы остаются, возникают новые, и всегда перед думающим управленцем и собственниками предприятия, возникает проблема выбора – как сориентироваться в море практических безграничных возможностей современных ИТ, какое решение выбрать, как минимизировать затраты времени и других ресурсов, на кого можно положиться, кто сможет гарантировать устойчивую и безопасную работу сложных механизмов предприятия.

Как отмечается в [1] современные подходы к Архитектуре предприятий – это не мода и не волшебное средство, а плодотворный подход к организации ИТ и обеспечения устойчивой деятельности предприятий. О какой архитектуре идет речь? Множится количество определений архитектуры предприятия (Enterprise Architecture), но все они сводятся примерно к следующему:

- архитектура описывает компоненты предприятия как сложной организационно-технической системы (ОТС) и их взаимосвязи вне зависимости от природы их физической реализации;
- архитектура включает в себя принципы развития и поддержки сложных ОТС современных предприятий, в частности, средствами информационных и коммуникационных технологий.

При этом под «системой» понимается любой комплекс предметов деятельности предприятия, представляющий собой единство закономерно расположенных и взаимосвязанных частей. В роли системы может выступать предприятие, его подразделение, основные сферы деятельности, а также и весь комплекс технологического и компьютерного оборудования, сетей, системного и прикладного программного обеспечения, который используется на предприятии и довольно условно называется «информационными технологиями».

Изначально понятие «архитектура» относилось только к зданиям и сооружениям, но со временем в этом слове смогли разглядеть намного более широкий смысл. Показательна аналогия между строительством зданий и информационных систем. То и другое представляет собой сложный, трудоемкий и часто непредсказуемый процесс. Результат этого процесса необходимо поддерживать в работоспособном состоянии и грамотно эксплуатировать, обеспечивая при этом минимизацию возможных рисков в эксплуатации зданий и деятельности предприятия.

На наш взгляд, именно развитие архитектурного подхода особенно актуально для обоснования рациональной структуры средств обеспечения комплексной безопасности предприятия. Знание архитектуры предприятия, состава его подразделений, зданий и сооружений, продукции, технологий, а также его окружения позволяет обоснованно определять месторасположение объектов и субъектов возможные проявления угроз безопасности и обоснованно определять необходимые и достаточные средства обеспечения безопасности, как с позиций традиционной архитектуры зданий и предприятия, так и с позиций использования на предприятии различных информационных технологий.

Однако следует учитывать, что ИКТ развиваются намного быстрее, чем здания и более подвержены разного рода внутренним и внешним негативным воздействиям, приводящим к рискам в деятельности предприятия. В тоже время именно средства ИКТ технологий обеспечивают также и физическую безопасность собственно зданий, сооружений, оборудования предприятия, информационных ресурсов, персонала и других элементов ОТС.

Как описать архитектуру современного предприятия и достаточно полную модель системы обеспечения комплексной безопасности? Для описания неподвижных и неодушевленных

предметов достаточно трех проекций, так в проектах строительства здания используют отдельные архитектурные проекции и разрезы, поэтажные планы, изображения фасадов и панорамные виды.

Описывая систему ИТ (отдельный компонент, программную систему, базу данных и т.п.) только в каком-то одном ракурсе, мы строим соответствующую проекцию. Можно разработать проекции на основе различных точек зрения, присущих разным группам сотрудников внутри предприятия и ее партнерам. Это владелец предприятия, руководители подразделений, сотрудники служб безопасности и ИТ-специалисты, пользователи и администраторы программных систем, проектировщики баз данных и их администраторы, сотрудники отдела закупок, клиенты и т.п. Таких проекций может быть очень много. Даже если путем долгих усилий опишем их, то получим совершенно бесполезную модель, воспринять которую нормальный человек не сумеет. Что же делать?

Можно предположить, что набор архитектурных планов полностью описывает здание. Три проекции в совокупности являются полной архитектурной моделью неподвижного объекта. Но их уже недостаточно для описания процессов деятельности предприятия с присущими им временными и динамическими характеристиками (длительность процессов, скорость и интенсивность возмущений и др.). Получается, что для любой ОТС можно построить множество архитектурных моделей, каждая из которых будет с той или иной степенью полноты и достоверности отображать объект управления.

Будем называть проекцией отображение взгляда на систему с некоторой точки зрения, а полной проекцией – исчерпывающее описание определенного взгляда на систему. Описание архитектуры является совокупностью отдельных проекций, которая образует архитектурную модель, с той или иной степенью полноты описывающую систему. Любую ОТС можно полностью описать с помощью некоего конечного числа полных проекций. Совокупность проекций, полностью и исчерпывающе описывающих систему, назовем полной архитектурной моделью. Полнота в данном случае означает, что любую другую проекцию удастся построить на основе данной архитектурной модели.

К настоящему времени одной из классических архитектурных моделей, претендующей на функциональную полноту, является матричная модель Захмана, представляемая совокупностью таблиц, описывающих различные проекции и срезы предприятия. По крайней

мере, все известные на сегодняшний день архитектурные модели предприятий, при вдумчивом рассмотрении, легко укладываются в эту модель [34]. В свете введенных Захманом определений строки и столбцы модели Захмана являются проекциями: строки с точки зрения групп, заинтересованных лиц или основных функций деятельности, столбцы – с точки зрения областей рассмотрения (что, кто, как, когда, где, зачем и сколько). Остановимся на полноте модели Захмана. Если со строками (с заинтересованными лицами и их функциями) все более-менее понятно, и полнота зависит от грамотного выделения таких групп, то со столбцами дело обстоит несколько сложнее. Всегда ли достаточно этих вопросов? Например, из рассмотрения выпал важный вопрос: «Какой допустимый уровень риска?».

Кроме того, модель Захмана предполагает статику, и без «оживления» ее дополнительной проекцией, характеризующей динамику, попросту не обойтись. А, поскольку динамика различных процессов предприятия различна, то надо знать динамические характеристики негативных воздействий на систему (в общем случае случайные процессы): что является объектом угроз (здесь подойдет статическая модель), кто является источником и инициатором угроз, когда наступают инциденты угроз, как развивается ситуация, какие возможные осознанные и неосознанные цели источника угроз и др.

Еще одно серьезное замечание связано с «начинкой» ячеек таблицы. Понятно, что полнота зависит от степени детализации их наполнения. Очевидно, что, заполнив ячейки текущими знаниями по тому ли иному вопросу с позиций той или иной группы заинтересованных лиц, мы полноты не достигнем. Поэтому в реальных производственных ситуациях у различного рода специалистов всегда возникает множество вопросов по практическому использованию модели Захмана в их непосредственной деятельности, ответы на которые возможно получить путем детализации клеток таблицы и развертыванием соответствующих им проекций.

Таким образом, можно утверждать, что модель Захмана является наиболее полной моделью корпоративной архитектуры предприятия. По крайней мере, другую модель практически всегда можно получить из модели Захмана. А зачем нам вообще строить модели и описывать процессы предприятия, технологии, средства безопасности и другие аспекты деятельности?

Понятно, что на каждом предприятии они есть. Но как удержать их достаточно большое многообразие в ограниченной памяти руководства и персонала предприятия? Какие действия надо принимать в тех или иных реальных ситуациях? Чем можно заменить отказавший элемент? Как развести информационные сети и множество других вопросов, главный из которых – как доводить необходимые знания до персонала предприятия и контрагентов?

Для ответа на эти вопросы можно провести аналогии со строительством. Видимо, если нужно построить конуру для собаки, то ее просто строят без предварительной разработки архитектурных планов в трех проекциях, а если строится здание, то без архитектурных проекций явно не обойтись. Если на предприятии используются один-два компьютера для подготовки отдельной документации, бухгалтерских проводок и отчетности для налоговых служб то, вполне возможно, строить ИТ-архитектуру не обязательно.

Для наукоемких предприятий ситуация может быть значительно сложнее. Как и любой объект, предприятие может развиваться стихийно или планомерно. Стихийное развитие позволяет подстраиваться под изменения окружающего мира, но грозит авралами и ошибками. Планомерное развитие, к сожалению, часто отрывается от реальности и при излишнем оптимизме (вере в моду, рекламу поставщиков средств ИКТ и др.) или прямолинейности, недостаточной грамотности заказчиков, проектировщиков и лиц, принимающих решения, может также привести к негативному результату.

Как всегда, истина находится посередине. А сформулировать ее можно так: необходимо планомерное развитие, позволяющее гибко реагировать на изменения окружающей обстановки. Однако даже стихийное развитие ИКТ вовсе не отрицает важности архитектурного подхода – как раз наоборот. Хотя бы потому, что при определенной сложности предприятия и его целевых и обеспечивающих автоматизированных систем (АС) вы просто не сможете определить, как реагировать на изменения, а архитектурный подход, при его последовательном применении и достаточно корректном документировании, позволяет установить определенную дисциплину оценки возникающих проблем при изменении каких-либо элементов в системах и обнаружении негативных воздействий среды, своевременно сформировать комплекс мероприятий по обеспечению

безопасности и устранению негативных факторов, зарезервировать необходимое количество ресурсов для их реализации.

Целесообразно рассмотреть соответствие между основными подходами традиционных классических архитектурных проектов зданий, архитектурой предприятия и архитектурой информационных систем. В таблице 2.1, заимствованной из работы [1], наглядно представлены общие моменты, присущие каждому из направлений, видна явно прослеживаемая преемственность и взаимообусловленность основных понятий архитектурного подхода.

Совместное рассмотрение и учет общих положений архитектурного подхода особенно важно при решении задач комплексной безопасности предприятий, так как все инциденты угроз безопасности необходимо привязывать к территории, помещениям (аспект строительной архитектуры). Угрозы обычно влияют на те или иные бизнес-процессы, продукцию и субъекты предприятия (аспект архитектуры предприятия), которые реализуются в зданиях предприятия и, при нарушениях целостности, также необходима привязка к строительным архитектурным планам предприятия.

Бизнес-процессы предприятия поддерживаются распределенными комплексами средств автоматизации и ИКТ, которые размещаются в зданиях предприятия. Они обеспечивают взаимодействие с внешней средой и информационную безопасность предприятия (аспект ИТ-архитектуры), т. е. всякого рода нарушения в работе автоматизированных систем предприятия также требуют привязки к территориальным аспектам, строительным чертежам и общей архитектуре предприятия.

Полнота сложившихся в мировой и отечественной практике стандартов архитектурного (общесистемного) проектирования автоматизированных систем предприятия доказана успешным опытом строительства множества зданий «Электронных предприятий». При этом можно утверждать, что модель Захмана полнее традиционной «строительной» архитектуры.

Еще одна архитектурная модель, претендующая на полноту, состоит из двух проекций: функциональной и технологической. Функциональная проекция охватывает бизнес-процессы предприятия. Она выросла из столбца «Как» модели Захмана при описании ИТ-архитектуры. Вторая представляет «основные средства» информационных технологий.

Таблица 2.1 – Сравнение архитектурных подходов

Архитектурно-строительный проект	**Корпоративная архитектура**	**ИТ архитектура**
Планы этажей, План конструкции кровли	Описание классических уровней архитектуры: бизнес-архитектура, прикладная архитектура, архитектура данных, инфраструктура, модель бизнес-процессов	Описание корпоративных ИТ стандартов, ИТ подразделений, программных систем, оборудования, сетевой инфраструктуры
Фасады	Товары и услуги, предоставляемые клиентам.	Сервисы, предоставляемые различным группам пользователей
Архитектурные разрезы	Организационный – организационная структура, финансовый – план счетов, финансовые отчеты и т.п.	Описание отдельных компонентов, в частности, программных систем: от ПО до установленного оборудования и используемых сетевых протоколов
Ситуационный план	Годовой план и бюджет	Краткосрочный план
Генеральный план	Стратегия	Основные средства, включая ИТ, интеллектуальный капитал
Пояснительная записка	Управление конфигурацией	Регламенты взаимодействия
План и разрезы фундамента	Интеграционные решения	Средства обеспечения коллективной работы (ИТ, связь, почта)
Проекты перекрытий	Способы взаимодействия отдельных компонентов	План внедрения корпоративных стандартов
Ведомость и чертежи перемычек	План развертывания корпоративной сети	План внедрения системы качества, Описание портальных решений
План инженерных коммуникаций	Система безопасности	Система ИТ безопасности
Проекты конструктивных элементов	Товары и услуги, предоставляемые клиентам.	Сервисы, предоставляемые различным группам пользователей

Рассмотрим ее в классической модели «слоеного пирога». Нижний слой технической ИТ-архитектуры – сетевой. Следующий – слой оборудования (серверы, дисковые массивы, сетевые устройства, рабочие места). Следом расположен слой базового программного обеспечения, устанавливаемого на оборудование предыдущего слоя (операционные системы и сетевые протоколы). Затем идет активно развивающийся слой, который представляет собой материал построения функционального программного обеспечения (СУБД, серверы приложений, технологические программы). Следующий слой – структура и форматы данных. За ним следуют слой приложений и, наконец, слой сервисов, предоставляемых пользователям. Если применить все эти проекции к каждому слою модели Захмана, получается, что в модели «слоеного пирога» технологической проекции содержание ячеек таблицы более единообразно. В совокупности функциональная и технологическая проекции обладают свойством полноты описания ИТ.

Как и во многих других случаях, при работе с архитектурой имеются два подхода, дедуктивный и индуктивный. В первом случае, построив полную архитектурную модель, мы сможем по мере необходимости получать из нее нужные проекции. Во втором строятся отдельные модели, которые на каждом этапе развития проекта все больше приближаются к полной архитектурной модели. Пожалуй, среди моделей последнего типа наиболее полезна в практическом смысле иерархическая модель, или модель постепенного уточнения и детализации требований к компонентам. Она состоит из нескольких уровней, и каждый последующий раскрывает и уточняет предыдущий.

Сделаем ряд замечаний относительно практического применения рассмотренных выше моделей архитектуры и информационных систем предприятий.

Первое замечание состоит в том, что при построении иерархической модели важно вовремя остановиться. Что значит вовремя? Когда описание системы станет достаточным для достижения конкретной цели, ради которой оно и было предпринято. Как связаны полная архитектурная и иерархическая модели? Решение этих и других смежных вопросов зависит от уровня методического обеспечения и достоверности данных предпроектного анализа стратегий развития предприятия и его бизнес-процессов,

применяемых на предприятии средств управления, декларируемых концепций и фактического состояния информационных систем.

Даже далекие от архитектуры люди знают, что существуют архитектурные стили и важно обеспечивать, по крайней мере, в рамках одного предприятия, единство стиля. В ИТ-строительстве ситуация значительно хуже, и о единстве стиля построения, стратегий развития информационных систем предприятия часто не задумываются, хотя крупные ИТ компании – производители компонент технического и программного обеспечения и пытаются формировать, а часто и диктовать, свои фирменные стили: «типовые решения» и другую атрибутику.

А это означает, что супермодные, дорогие системы часто соседствуют с теми, которые называют «наследуемыми», но которые нормально работают и от которых часто просто невозможно отказаться в силу ряда обстоятельств. В таких случаях ИТ представляют собой отдельные не связанные или слабо связанные технические и программные компоненты, что не позволяет добиваться согласованной и эффективной работы современных систем, обеспечивать их надежное функционирование и безопасность. Поэтому архитектура ИТ зависит не только от требований бизнеса, но и от конкретных пользователей и их представлений о роли ИТ в их деятельности, наличия различного вида ресурсов.

Архитектура ИТ существует не в безвоздушном пространстве она должна вписываться в «ландшафт» предприятия, соответствовать принятым правилам и нормам корпоративной культуры предприятия. Отсюда можно вывести весьма полезное следствие: при изменении окружающей среды архитектура предприятия и его информационных систем, средства обеспечения безопасности должны меняться, хотим мы этого или нет, ведь постоянно появляются новые задачи предприятия, требующие автоматизированного решения, постоянно уходят и приходят клиенты и партнеры и т.п. И в этой связи, в каждом конкретном случае важно обеспечивать анализ изменений в архитектуре предприятия и оценки их влияния на показатели безопасности его деятельности, помнить поговорку «лучшее-враг хорошего».

Для предприятий наукоемкого машиностроения, работающих в тесной интеграции и конкуренции с зарубежными странами, в своей деятельности необходимо также учитывать особенности страны и

общества в других регионах мира (совместные международные проекты, потребители продукции, поставщики и другие контрагенты). Архитектура предприятий разных стран имеет нечто общее, но обладает и отдельными национальными чертами. Опыт прямого использования западных ИКТ в основной продукции и управлении процессами отечественных предприятий показал, что в ИКТ также есть такие особенности и их надо учитывать как в технической политике, так и в стратегиях безопасности предприятия.

Учет этих особенностей заключается в анализе целесообразности использования и гармонизации стандартов предприятия с принятыми международными и национальными стандартами в сфере описания продукции, процессов и ресурсов предприятий. В связи с широким развитием локальных, корпоративных и глобальных сетей ЭВМ, мобильных средств связи особое место в этих стандартах отводится стандартам информационных технологий и информационной безопасности, унификации конструкций изделий ИКТ и интерфейсов представления различных данных.

Архитектура предприятия оказывает существенное влияние на формирование концепции безопасности и решения по выбору методов и средств обеспечения безопасности. Весьма важным является унификация системы соглашений о взаимодействии с другими предприятиями и, в частности, с предприятиями инфраструктуры поддержки инновационного развития. При этом производится разработка регламентов и протоколов обмена данными интерфейсов взаимодействия с внешним миром, формирование функционально полных структур прикладных информационных систем обеспечения их деятельности и соответствующий выбор типовых и индивидуальных решений в целевых и обеспечивающих АС предприятий.

К настоящему времени сложилась представление о 3-D архитектуре предприятий разного уровня. Так, например, обобщенную архитектуру любого предприятия можно представить в виде куба, в котором проекции соответствуют различным представлениям и срезам работы предприятия, например: первая проекция – вертикаль управления (органы управления предприятием и его подразделениями), вторая проекция – продукты и услуги, инновационные проекты, третья проекция – методы и инструменты управления. Такое представление предприятия является достаточно

понятным для отображения всех основных сторон его деятельности и организации его взаимодействия с другими институтами общества, в том числе с применением систем электронного взаимодействия предприятий (СЭВП) [4 – 6].

Укрупненная Архитектура предприятия, обеспечивающая различные аспекты безопасности его деятельности, является детализацией общей 3-D модели «электронного государства» и «электронных предприятий». При этом описание проекций рассмотренного выше куба может выполняться с применением отдельных таблиц модели Захмана, а также доступных методов описания продукции, процессов и ресурсов предприятий, основанных на международных, национальных и корпоративных стандартах, гармонизированных между собой, по крайней мере, в рамках отраслевой направленности текущих и инновационных проектов предприятия.

Подробное описание отношений и взаимосвязей между сущностями- объектами предметной области деятельности предприятия, потоки данных, процессов и логики принятия решений может выполняться с применением соответствующих языков и инструментальных средств проектирования АС, например, на основе методологий IDEF, UML, и др. [2].

Таким образом, явно прослеживается связи, необходимые для грамотного формирования стратегий и программ развития предприятий, концепций автоматизации и информатизации процессов предприятия. Обеспечение функциональной полноты, целостности, устойчивости, надежности и безопасности предприятия может быть достигнуто при соблюдении системных принципов проектирования сложных систем в следующей, в общем случае итеративной, последовательности системного проектирования профилей безопасности предприятия: «Системная архитектура предприятия – анализ рисков и угроз безопасности – функциональное описание информационных систем (ИТ-архитектура) – архитектура технических и программных средств реализации – решения по комплектации, эксплуатации и техническому обслуживанию систем».

Нарушение этой последовательности, часто встречающееся на российских предприятиях, как правило, ведет к дополнительным рискам в их деятельности, неадекватному выбору организационно-технических решений, снижению качества процессов, увеличению сроков реализации проектов и, в конечном итоге, увеличению затрат

различных ресурсов, снижению конкурентоспособности на внутренних и внешних рынках продукции и услуг.

2.2 Объекты и субъекты безопасности предприятия

Применение основных положений современного подхода к архитектуре предприятий позволяет обосновать выбор объектов и субъектов обеспечения безопасности и, в соответствии с миссией и концепцией развития предприятия, целями, мотивами и действиями ЛПР и ведущего персонала, знаний рынка продукции, возможностей и намерений конкурентов и контрагентов, упорядочить возможные угрозы и риски в деятельности предприятия в целом, так и отдельных подразделений, служб, процессов и ресурсов. Так, например, исходя из представления Предприятия в виде 3-D модели и анализа типологии внешней инфраструктуры предприятий наукоемкого машиностроения основными субъектами, определяющими часто противоречивые и нуждающиеся в должной координации и согласовании, требования к средствам обеспечения безопасности различных процессов предприятия являются:

- владельцы предприятия, стратегические партнеры и контрагенты;
- разработчики проектов, основной продукции и услуг предприятия;
- координаторы целевых Программ развития предприятий, управляющие проектами;
- владельцы общих и специализированных информационных ресурсов предприятия;
- владельцы специализированных технологий (научные подразделения, службы САПР изделий и технологических процессов, САПР по сферам деятельности);
- инвесторы-заказчики и владельцы финансовых ресурсов по привлекательным для них инновационным и инвестиционным проектам предприятия;
- организации и предприятия инфраструктуры инновационного развития региона, государства и мира;
- поставщики материалов и комплектующих, и в частности средств обеспечения безопасности, информационно-коммуникационных технологий;
- потребители продукции и услуг предприятия;
- владельцы коммуникационных ресурсов (провайдеры сетей ЭВМ).

Здесь следует также отметить, что указанные выше субъекты в силу ряда обстоятельств, мотивов и осознанных или неосознанных

действий могут также быть и источниками угроз обеспечения безопасности деятельности предприятия.

В схемы взаимодействия подразделений обеспечения безопасности предприятия с элементами внутренней и внешней инфраструктуры включается следующий, не являющийся исчерпывающим список архитектурных «осей»:

- Ось «архитектурных аспектов» предприятия (Организационные структуры предприятия);
- Ось «представлений» продукции и услуг предприятия (Функции структурных подразделений элементов);
- Ось времени развития системы (стадии жизненного цикла систем предприятия);
- Ось обобщения/конкретизации архитектурных блоков и элементов;
- Ось агрегации/детализации архитектурных блоков и элементов;
- Ось прикладного сегментирования схемы (выделение типовых функциональных модулей многократного применения в различных целевых и обеспечивающих АС предприятия).

В совокупности этот набор архитектурных осей определяет состав необходимых и достаточных интерфейсов взаимодействия подразделений и служб обеспечения комплексной безопасности предприятия.

Для обеспечения работы с этим набором «осей» принципиальным является четкое различение таких понятий как «объекты угроз безопасности» и «объекты проектирования средств обеспечения безопасности».

На основе анализа общесистемных и специфических характеристик предприятий различных типов в работе [6] предложена базовая модель деятельности предприятия, которая определяет общие процессы, основные системообразующие элементы и сферы взаимодействия предприятия с внешним окружением, требования к методам описания продукции, процессов и ресурсов предприятия, процессам проектирования деятельности, методам соорганизации специалистов – участников проектов.

Опыт показывает, что состав процессов проектирования любых ОТС предприятий, в том числе и интегрированных систем обеспечения комплексной безопасности является достаточно стабильным, может быть типизирован и использован в системах стандартов и профилей взаимодействия открытых информационных систем разного уровня.

Современные подходы системного проектирования сложных ОТС предусматривают применение сервисной идеологии с самых первых шагов анализа и проектирования предприятия и его АС. Так, например, стандарт ISO/IEC 15288 «Стадии жизненного цикла систем» рекомендует анализ и проектирование любой системы начинать с выяснения потребностей заинтересованных лиц, выраженных в «необходимых им сервисах» – услугах для себя и, соответственно, услугах для других.

Однако в современной практике наблюдается большое многообразие трактовок понятия услуги, в частности, услуга может рассматриваться как только коммерческая деятельность, как государственная услуга правительственных служб для населения, как техническая служба в смысле терминологии «открытых систем», как программный сервис прикладной ИС, как Веб-сервис, как сервис СУБД или ОС и т.п.

Применительно к предмету настоящей книги речь идет о разработке «сервисов безопасности» как о продуктах особого рода. Это особенно важно, поскольку побуждает рассматривать системы обеспечения безопасности не в узком смысле, как средства защиты от различного рода посягательств на целостность и устойчивость работы предприятия, а как объективно необходимый комплекс обеспечения деятельности автоматизированного «электронного предприятия».

При использовании в архитектуре безопасности предприятия сервис-ориентированного подхода большое внимание уделяется доставке сервиса клиенту (внутреннему или внешнему заказчику или потребителю) и разграничению доступа к услугам, причем действия по доставке результата обслуживания и организации доступа к нему также могут рассматриваться как сервис. При этом особая роль с позиций обеспечения безопасности отводится информационным и коммуникационным службам предприятия и внешних провайдеров корпоративных и глобальных сетей ЭВМ.

Отметим, что в настоящее время отсутствуют достаточно обоснованные критерии и однозначные правила выделения базового набора процессов предприятия и сервисов, представляемых внешним потребителям. Базовые процессы «верхнего уровня детализации» подвергаются декомпозиции на более простые бизнес-процессы с достаточной степенью изолированности и модульности. Практика показывает, что для решения задачи определения взаимосвязей между основными процессами предприятия и прикладными

сервисами приходится использовать специальные методы анализа и синтеза «сквозной» сервис ориентированной архитектуры (SOA).

При этом для формирования рациональной сервис-ориентированной архитектуры целесообразно опираться в большей степени не на компьютеризацию как таковую и реализацию технических коммуникаций, а на организацию и оптимизацию информационных потоков, их природу, и на определение рационального состава узлов принятия решений в той или иной ситуации, механизмов взаимодействия между ними и основными процессами предприятия. Результаты такого анализа позволят выбрать обоснованные, необходимые и достаточные характеристики «сервисов безопасности» в рамках предприятия. При этом надо учитывать, что прикладной сервис в сфере обеспечения комплексной безопасности современных предприятий:

- инициируется или выполняется по любому каналу, не обязательно связанному с ИКТ,
- может состоять полностью или частично из неавтоматизированных операций и интерфейсов,
- при своем выполнении оперирует как информационными, так и любыми иными ресурсами (людскими, материальными средствами, финансовыми, энергетическими),
- взаимодействует с внутренними и внешними потребителями самыми разнообразными способами и в самые разные моменты (например, непосредственный результат сервиса может заключаться в получении клиентом устной консультации в приватной беседе с поставщиком услуги при личной встрече или по телефону).

При выборе «сервисов безопасности» необходим системный анализ фактической и перспективной архитектуры предприятия, учет особенностей процессов и взаимосвязей между ними.

Архитектура современных предприятий определятся системообразующими объектами деятельности (товары и услуги, конструкции и технологии изделий, оборудование, материальные и информационные ресурсы, инфраструктура, производство, персонал, процессы, документация), активными элементами и множеством связей между ними и внешней средой. Состояние объектов, процессов и документации предприятия в силу естественных причин является различным, но может быть оценено по общим показателям оценки и тесноте связей с другими объектами.

В то же время можно считать, что на каждом предприятии, в той или иной мере, реализуются общесистемные процессы: оценка потребностей и показателей деятельности, определение потенциала и возможностей, правовое обеспечение деятельности, совершенствование техники и технологии, использование ресурсов и их восстановление, обеспечение экологической, технологической и экономической безопасности, подготовка и обучение персонала и др.

Применение рассмотренного выше подхода к архитектуре предприятий и модели Захмана, построение многомерных системных матриц «Потребности-Цели – Объекты – Процессы деятельности – Инструменты – Связи между элементами и средой», а также унификация видов обеспечения, состава и содержания работ и мероприятий по конкретным проектам, опыт управления программами развития, обеспечивает достаточные концептуальные основы системного проектирования архитектуры предприятий и соответствующих программ его развития.

В таблице 2.2 приведен пример описания системной матрицы обобщенного машиностроительного предприятия. В клетках матрицы могут указываться целевые показатели и характеристики проектов, требуемые ресурсы и другие системные параметры. Состав системных объектов может уточняться и детализироваться для каждой клетки этой матрицы.

Системная матрица предприятия может рассматриваться как верхний уровень описания всего множества объектов (предметов и сфер деятельности предприятия) и функций, выполняемых структурными элементами (собственно процессов и функциональных преобразований над предметами) и, при соответствующей конкретизации и детализации предметов деятельности, определяет функционально полный набор задач управления организационно-техническими системами (ОТС), обеспечивающих работу предприятия, служит основой для разработки модели функционирования предприятия, определении и упорядочения рациональных структур организационного, информационного, технического и программного обеспечения деятельности предприятия.

Таблица 2.2 – Системная матрица задач обеспечения деятельности предприятия

<table>
<tr><th rowspan="2">Основные процессы обеспечения деятельности предприятия</th><th colspan="5">Системные объекты деятельности предприятия</th></tr>
<tr><th>Продукция и услуги</th><th>Материальные и информационные ресурсы</th><th>Инфраструктура (здания, сооружения)</th><th>Процессы и технологии</th><th>Организационные структуры</th></tr>
<tr><td>Оценка качества системных объектов и потребностей в их развитии</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Организационные структуры и механизмы обеспечения деятельности</td><td></td><td colspan="3" rowspan="6">В клетках системных матриц указываются оценки состояния соответствующих объектов, и в частности, показателей состояния безопасности, сложности инцидентов угроз безопасности, рисков и ресурсов, необходимых для обеспечения устойчивого функционирования предприятия.
В простейшем случае это могут быть экспертные оценки целесообразности реализации мероприятий по обеспечению безопасности соответствующих объектов и процессов</td><td></td></tr>
<tr><td>Оценка потенциала и «точки роста» экономики предприятия</td><td></td><td></td></tr>
<tr><td>Методы и инструментальные средства управления</td><td></td><td></td></tr>
<tr><td>Правовое обеспечение деятельности</td><td></td><td></td></tr>
<tr><td>Надежность, экология, технологическая и общественная и экономическая безопасность</td><td></td><td></td></tr>
<tr><td>Программы взаимодействия и делового сотрудничества</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Для практического использования системных матриц разработан достаточно строгий математический аппарат теории графов, матричной алгебры, функционального анализа и др., а также ряд инструментальных средств структурного анализа, моделирования и проектирования сложных систем [13].

Основная сложность в их использовании заключается в необходимости корректного определения терминов описания системных объектов, функций структурных элементов, общих и частных процессов предприятия, методов и техники управления, т. е. для обеспечения согласованной и устойчивой работы предприятия необходимо наличие общедоступного для понимания различными субъектами понятийного аппарата.

На сегодняшний день основным инструментом согласования понятий являются классификация, стандартизация и унификация методологических и конструктивных элементов сложных человеко-включающих систем и самое главное – упорядочение и гармонизация большого разнообразия, применяемых стандартов. Применительно к предметам архитектуры предприятий ключевыми стандартами являются стандарты описания организационных структур, продукции, процессов, ресурсов, интерфейсов взаимодействия и протоколов обмена данными.

Все это, безусловно, важно и для решения задач обеспечения безопасности системных объектов, процессов и субъектов предприятия и одной из основных задач построения профиля систем безопасности предприятия является рассмотрение с единых системных позиций существующих и перспективных подходов к выбору ограниченного множества таких стандартов. А только списки стандартов, так или иначе затрагивающих вопросы безопасности составляют десятки страниц. И в этой связи проведение работ по их упорядочению, гармонизации и адресной привязке к процессам и стадиям жизненного цикла изделий и соответствующих ОТС является безусловно необходимым.

2.3 Процессы и стадии жизненного цикла организационно-технических систем предприятия

Обычно при проектировании, или спонтанном развитии предприятия, органы управления предприятием разделяют сферы ответственности, функции и предметные направления деятельности основных подразделений и служб используя различные

неформальные подходы и достаточно строгие модели деятельности предприятия и модели оптимизации организационных структур на основе анализа процессов предприятия, функций структурных элементов и потоков данных.

Наиболее перспективным подходом к рациональному распределению функций подразделений является упорядочение основных процессов жизненного цикла предприятия на основе стандарта ISO/IEC 15288 «Стадии жизненного цикла систем», в соответствии с которым, все процессы жизнедеятельности предприятия подразделяются на:

- Процессы предприятия:
    - Управление внешней средой предприятия;
    - Управление инвестициями;
    - Подготовка соглашений с контрагентами;
    - Управление жизненным циклом;
    - Управление ресурсами;
    - Управление качеством;
    - Управление информацией;
- Процессы проектирования:
    - Планирование проекта;
    - Оценка стоимости проекта;
    - Управление проектом;
    - Принятие проектных решений;
    - Управление рисками;
    - Управление конфигурацией;
    - Аттестация;
- Технические процессы
    - Формулировка требований заказчика;
    - Анализ требований;
    - Решения по архитектуре;
    - Реализация;
    - Интеграция;
    - Верификация;
    - Переработка;
    - Обслуживание;
    - Ликвидация;
- Соглашения
    - По поставкам различного рода продукции и услуг внутренним и внешним контрагентам;

- По закупкам различного рода ресурсов для обеспечения деятельности предприятия и его подразделений.

Эти процессы являются взаимосвязанными и в совокупности определяют достаточно полный набор деятельности всех субъектов предприятия в отношении его продукции, применяемых технологий и необходимости приобретения и эффективного использования разного рода ресурсов. Следует также отметить, что **обеспечение безопасности** является необходимым атрибутом любого из процессов предприятия и для каждого из них могут быть определены внутренние и внешние источники угроз безопасности, риски и меры по обеспечению безопасности.

Упорядочение и привязка этих процессов к конкретным подразделениям и исполнителям осуществляется путем построения модели предприятия в виде упорядоченной совокупности организационной структуры, материальных и информационных потоков (документов, сообщений, сигналов) и процедур деятельности (алгоритмов, расчетных формул для идентификации, измерения и оценки показателей состояния предприятия в текущей или прогнозной ситуации. Модель предприятия – основной инструмент подготовки и принятия решений в различных ситуациях и, при условиях обеспечения ее корректности, позволяет отвечать на вопросы, что будет, если изменится какой-либо элемент структуры или характеристики внешних воздействий.

Грамотно и обоснованно спроектированные процессы жизненного цикла ОТС базируются на принципах модульности (максимальная взаимосвязь функций, реализуемых процессом, при минимуме связей между процессами) и самостоятельности («владельцы» процессов предприятия должны нести ответственность за результаты своих действий), а также обеспечить их целостность, надежность и безопасность.

Функции, реализуемые процессами, определяются в терминах частных целей, входных и выходных потоков данных, выходных результатов, показателей их качества, процедур реализации процесса и необходимых ресурсов. Это справедливо для любых ОТС и в, частности для систем обеспечения их безопасности. Общие процессы обеспечения безопасности предприятия вовсе не отрицают возможности использования дополнительных процессов, учитывающих специфику предприятия.

Унификация и повторное использование процессов на каждом уровне детализации архитектуры предприятия является ключевым моментом. Результаты процессов на любом уровне, будь то информация, предметы или услуги, являются входными для тех же процессов уровнем выше или ниже. Это влечет некоторый отклик, повторную информацию, продукцию и услуги, которые модифицируют первоначальные результаты. Таким образом, выходы процессов на всех уровнях системной архитектуры могут быть использованы с целью достижения согласованного результата, например, описаний элементов системы, формирующих устойчиво работающую архитектуру предприятия.

Постоянно меняющиеся факторы, влияющие на ОТС предприятия, изменения в продукции и услугах, операционной среде, новые возможности при реализации элементов системы, изменения структуры и перераспределение ответственности в организациях требуют постоянного пересмотра решений о возможности запуска того или иного процесса. Таким образом, применение процесса становится динамическим, зависящим от многих внешних факторов, влияющих на систему.

Описание стадий жизненного цикла помогает в планировании, реализации и управлении процессами предприятия в сложных условиях, обеспечивая достижение понятной и достаточно общей цели верхнего уровня и построения эффективной архитектуры предприятия. Предшествующий положительный опыт предприятия, особенно в традиционной сфере деятельности может помочь в выборе стадий и применении процессов жизненного цикла для построения подходящей и эффективной модели жизненного цикла любой системы.

Конкретные предприятия реализуют стадии по-разному, пытаясь сочетать противоречивые стратегии успешной реализации основных процессов и одновременного уменьшения степени риска. Выполнение стадий параллельно во времени и в различной последовательности может привести к вариантам жизненного цикла с весьма различающимися характеристиками.

Выбор формы жизненного цикла систем обеспечения комплексной безопасности обусловлен такими факторами, как: особенности предприятия, целевое назначение и сложность продукции и услуг, стабильность требований, возможности

технологии, необходимость изменения характеристик системы с течением времени, возможности бюджета и наличие ресурсов.

Естественное встраивание средств безопасности в целевые и другие обеспечивающие АС предприятия необходимо для успешного выполнения основной деятельности предприятия. Укрепление связи с командами проектирования, технического обслуживания и соответствующими внутренними структурами и внешними организациями, ответственными за реализацию различных функций и стадий жизненного цикла продукции и услуг предприятия ведет к повышению устойчивости процессов предприятия в целом.

Система обеспечения безопасности предприятия, как и любая другая ОТС также имеет свой собственный жизненный цикл. Этот цикл увязывается и синхронизируется с жизненным циклом целевых систем предприятия, например на стадии «Концепция целевой системы предприятия» определяются требования к системе обеспечения ее безопасности и инфраструктуре служб предприятия, ответственных за функционирование целевых систем.

В то же время обеспечивающие системы могут накладывать дополнительные ограничения на целевые системы предприятия. В связи с этим ИСОКБП сама может рассматриваться как целевая, имеющая свои обеспечивающие системы. На рис. 2.1 приведен пример схемы взаимодействия целевых и обеспечивающих систем.

Обеспечивающая система может предшествовать целевой, т.е. уже существовать в инфраструктуре организации, ответственной за целевую систему (классический пример – многие проекты военных ведомств с высокой степенью секретности), или входить в состав организации-поставщика услуг. Предварительно существующие обеспечивающие системы могут накладывать дополнительные ограничения на целевую систему.

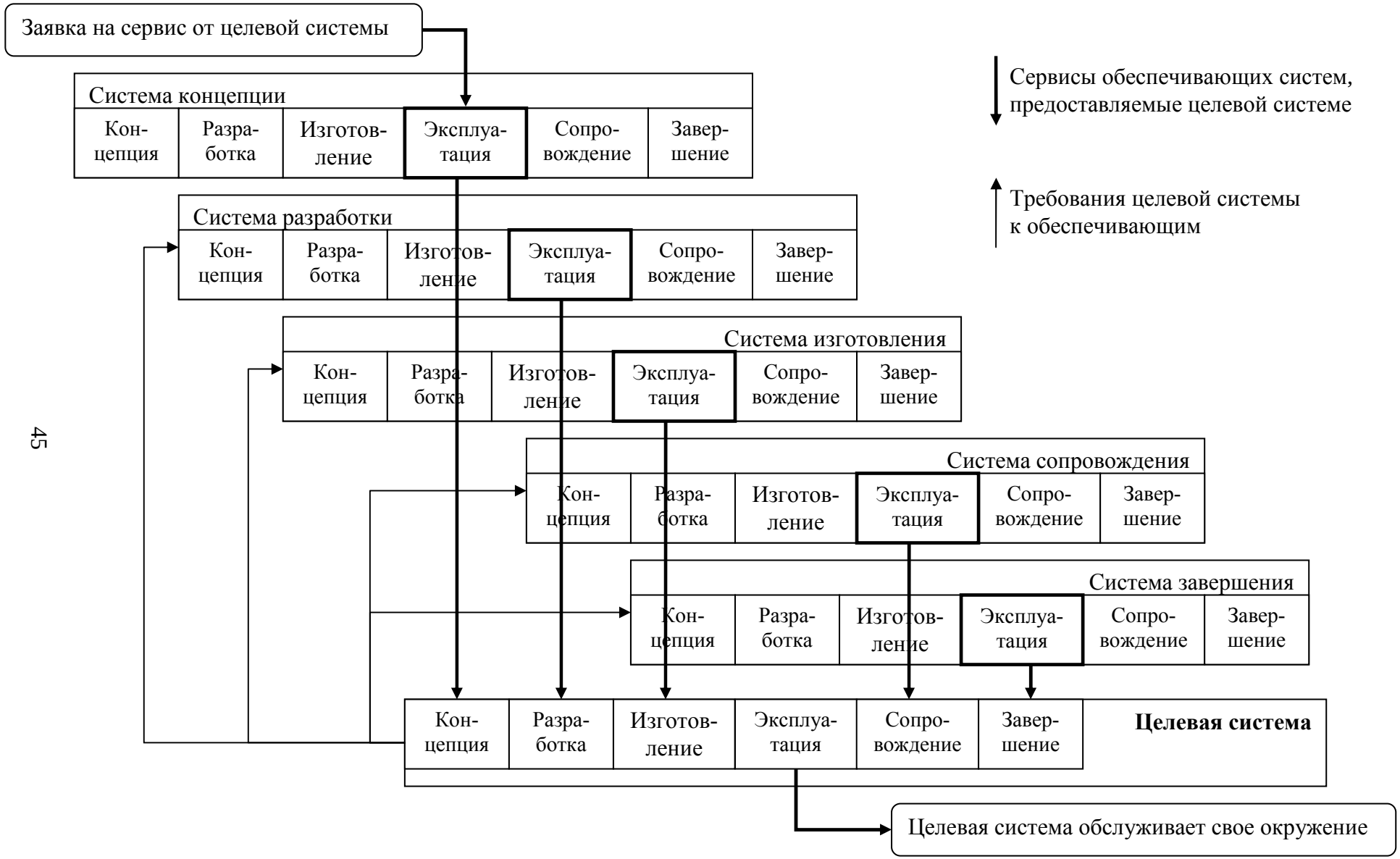

Рис. 2.1 Взаимодействие целевой системы с обеспечивающими системами

Таким образом, можно определить следующие стадии жизненного цикла систем обеспечения безопасности:

1. Разработка концепции общесистемного проекта обеспечения безопасности и спецификаций требований к организационному, методическому, техническому и программному обеспечению;
2. Разработка системы внутренних и внешних соглашений и выбор базовых стандартов представления данных об объектах, процессах и ресурсах предприятия, объектах угроз безопасности;
3. Разработка системного проекта и отдельных проектов комплектации подразделений безопасности средствами и системами безопасности, (приобретение компонент);
4. Системные и эксплуатационные испытания компонент и передача их в эксплуатацию;
5. Комплексирование, интеграция и встраивание испытанных компонент средств безопасности в процессы и эксплуатируемые АС предприятия (в том числе подготовка персонала);
6. Завершение, в том числе ликвидация старых, отработавших свое, систем и отдельных компонент, и разработка рекомендаций по их модификации для новых условий и тиражированию проектных решений в подразделениях предприятия.

Здесь следует отметить, что такое описание жизненного цикла систем предусматривает на каждой стадии итеративное выполнение вложенных циклов «Концепция – разработка – изготовление – эксплуатация – завершение». К большому сожалению, работы последней стадии во многих Российских предприятиях, программах и проектах часто не планируются и не обеспечиваются необходимыми ресурсами. Это может приводить к сопротивлению персонала, несвоевременной корректировке регламентов, замене оборудования, программного обеспечения и др. негативным последствиям, увеличивающим риски предприятия, вплоть до отказа от внедрения новых, в т.ч. работоспособных, систем и в итоге неоправданного списания затрат в убытки (закапывания денег в песок).

Необходимо также учитывать, что по результатам концептуального системного проектирования систем безопасности предприятия или инициатив отдельных подразделений на практике порождается различное конечное множество организационных и технических предложений по комплектации конкретными средствами безопасности как изделий основного производства, так и процессов их проектирования и технологий изготовления.

В этой связи весьма актуальными для предприятий являются работы по координации работ и ресурсообеспечению совокупности текущих и инновационных проектов. Обычно принятие решений по выделению или перераспределению ресурсов между альтернативным проектами принимается по результатам первых двух стадий жизненного цикла каждого проекта и корректируются с учетом интегрального состояния экономики предприятия, показателей зрелости его процессов, уровня безопасности.

При этом для совокупности инновационных проектов предприятия составляется матрица корреляционных связей между проектами и необходимыми для проектов ресурсами всех видов, на основе которой выполняются:

- оценка привлекательности и потенциальной результативности проекта для потребителей;
- оценка влияния проекта на показатели основной деятельности предприятия (в том числе крупных проектов) и совместных проектов с другими предприятиями;
- оценка потребностей в ресурсах;
- оценка рисков реализации проекта и решения по распределению ресурсов проекта по исполнителям;
- мероприятия по защите интеллектуальной собственности предприятия, авторов и прав владения на использование результатов работ;
- оценки полной стоимости владения проектом (системой) на всех стадиях его жизненного цикла, в том числе стадии завершения и ликвидации;
- подготовка бизнес планов для привлечения внутренних и внешних инвестиций на разных уровнях и по разным Программам (с учетом фактического или прогнозируемого состояния ресурсов).

2.4 Комплекс средств информационных технологий управления и безопасность процессов предприятия

Для иллюстрации основных концептуальных положений архитектурного подхода к разработке АС и обеспечению комплексной безопасности предприятий приведем функциональную структуру комплекса средств информационных технологий управления современным предприятием наукоемкого машиностроения (см. рис. 2.2).

Рис. 2.2 (1) Структура комплекса средств информационных технологий управления процессами предприятия (продолжение на стр. 50)

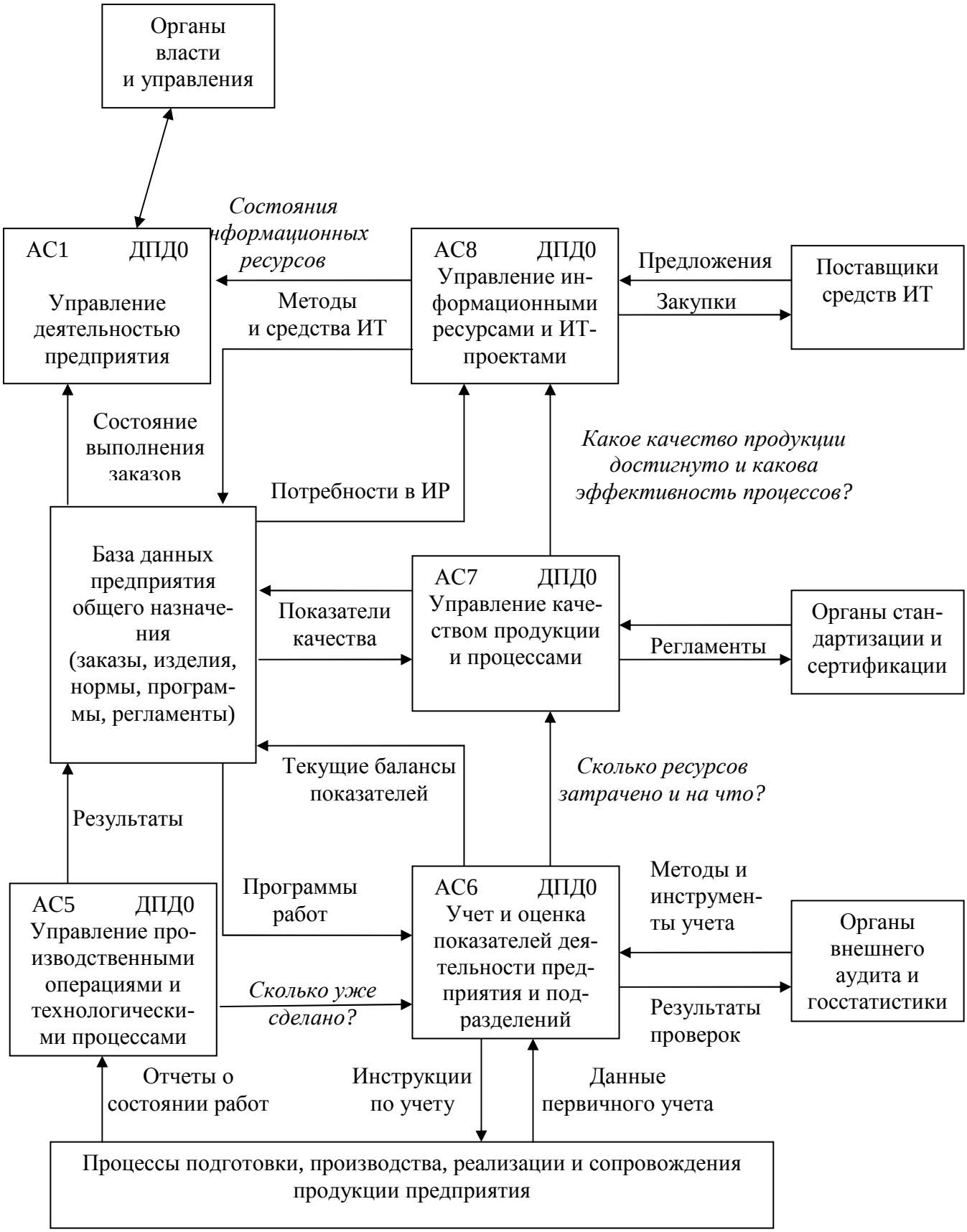

Рис. 2.2 (2) Структура комплекса средств информационных технологий управления процессами предприятия (продолжение)

Этот комплекс разработан на основе опыта предприятия по производству изделий авиационной, транспортной и грузоподъемной техники [18] и обобщает результаты этого и ряда других предприятий в сфере системного анализа продукции, процессов и ресурсов предприятия, а также опыт проектирования и эксплуатации отдельных подсистем традиционных автоматизированных систем управления процессами предприятия и их интеграции.

В состав типового комплекса средств ИТ управления предприятия с полным жизненным цикла изделий наукоемкого машиностроения, включаются ряд взаимосвязанных программно-методических и программно-технических комплексов, которые обслуживают целевые и обеспечивающие АС предприятия. Каждый из комплексов привязан к одному или нескольким связанным процессам предприятия, а в каждой из АС реализуются полные замкнутые циклы или контуры управления соответствующими объектами и процессами - от измерения и оценки состояния, анализа внешних воздействий, принятия решений и до выдачи управляющих воздействий и сообщений смежным системам. Таким образом в системе реализуются общие принципы программно-целевого и адаптивного управления с обратной связью, принципы функциональной целостности каждого из структурных элементов, а также основные подходы сервис ориентированной архитектуры прикладных АС.

В состав комплекса включаются следующие целевые АС предприятия:

- управление деятельностью предприятия;
- техническая подготовка производства;
- управление инфраструктурой предприятия;
- управление материальными ресурсами;
- управление производственными и технологическими операциями;
- учет и оценка показателей деятельности предприятия и подразделений;
- управление качеством продукции и процессов;
- управление информационными ресурсами.

Состав обеспечивающих систем здесь не рассматривается. К ним можно отнести системы автоматизации служб напрямую не связанных с производством основной продукции предприятия, таких как энергообеспечение, эксплуатация зданий и сооружений, управление персоналом, охрана, обеспечение здоровья в коллективе,

обучение персонала, ремонт оборудования и др. Следует только отметить, что принципы разработки обеспечивающих целевых и обеспечивающих систем одинаковы и при разработке интегрированных систем обеспечения комплексной безопасности необходимо учитывать влияние каждого из процессов на общее состояние безопасности предприятия и устойчивость и безопасность смежных процессов.

На рисунке 2.2 для каждой целевой АС представлены только диаграммы потоков данных (ДПД) верхнего уровня. Детализация этих диаграмм, а также техническая архитектура среды реализации рассматривается в общесистемном проекте КСИТ предприятия, а также в проектах целевых и обеспечивающих АС предприятия. Интеграция и координация целевых АС осуществляется посредством использования базы данных общего назначения, причем в качестве координаторов могут выступать основные «владельцы» базовых процессов – прикладных АС предприятия.

Приоритеты в распределении задач по координации и согласованию решений принадлежат лицам, принимающим решения на соответствующем уровне управления предприятием. При этом особое внимание уделяется процессам функционирования АС управления деятельностью предприятия, АС управления технической подготовкой производства (включая выполнение НИР, САПР-изделий, САПР-технологий, АС управления информационными ресурсами предприятия (включая защиту интеллектуальной собственности и анализ контрафактной продукции и ресурсов, а также рассмотрение всех процессов с точки зрения оценки последствий возможных нарушений и угроз безопасности предприятия и снижение рисков основной деятельности. Следует отметить, что в составе АС1 «Управление предприятием» предусмотрена подсистема обеспечения безопасности предприятия. Однако при боле детальном рассмотрении архитектуры предприятия и анализе угроз безопасности для основных процессов следует признать целесообразным разработку специализированных услуг безопасности и т.н. «модулей жизнеобеспечения» в каждой из целевых АС предприятия.

Анализ функциональной структуры типового комплекса средств АС предприятия позволяет явным образом выделять общие и специфические задачи обеспечения безопасности предприятия, определить основные объекты и субъекты угроз безопасности,

внутренние и внешние потоки данных, определить каналы их передачи, которые и надо контролировать на предмет всякого рода нарушений безопасности как со стороны персонала, внутренних и внешних контрагентов, так и со стороны возможных противоправных действий других фирм, техногенных катастроф природных явлений, экономических, политических и террористических угроз.

В частности вокруг каждой целевой АС предприятия можно выделить 8 основных контуров – «периметров» безопасности, а также один внешний контур – безопасность взаимоотношений с клиентами и один внутренний контур – информационная безопасность базы данных общего назначения. Аналогичный подход к определению периметров безопасности применяется также и при обеспечении физической безопасности зданий и сооружений предприятия, а также и персонала предприятия.

Рассмотренный выше архитектурный подход и типовая функциональная структура комплекса АС управления предприятием дает достаточные основания для включения в состав целевых АС специализированных средств обеспечения безопасности своей деятельности, т.н. «услуг обеспечения безопасности». Одной из важных проблем обеспечения безопасности предприятий является определение реальной сложности объектов контроля, процессов деятельности в условиях конкурентной среды и противодействующих воздействий внешних сил.

В этих условиях важно обеспечить согласование процедур принятия решений на разных уровнях управления на основе отбора достоверных данных об объектах в реальных условиях. В этой связи в составе средств обеспечения комплексной безопасности предприятия необходимо иметь средства, обеспечивающие:

- измерение и оценку показателей результативности деятельности, качества продукции и услуг и эффективности использования ресурсов в подразделениях;
- идентификацию и регистрацию событий – инцидентов угроз безопасности предприятию и целостности его ключевых процессов,
- ранжирование (упорядочение внутренних и внешних возмущений) по степени их влияния на целевой показатель развития предприятия;
- сегментацию (разделение области значений фактора на сегменты для проведения дальнейшего, более детального анализа);

- профилирование «наилучших» достижений (в смысле обнаружения и ликвидации угроз безопасности) для перспективного планирования деятельности предприятия и разработки текущих мероприятий по обеспечению безопасности в той или иной сфере деятельности;
- выявление ассоциаций (поиск факторов появляющихся вместе) различных инцидентов угроз безопасности предприятия;
- выявление исключений (поиск отклонений и элементов, выпадающих из общей картины, необычных ситуаций, несогласованных мнений и т.п.);
- оценку сложности объектов и процессов с позиций обеспечения их безопасности, уровня зрелости процессов по интегральным показателям для принятия решений по распределению ограниченных ресурсов на реализацию мероприятий с учетом технико-экономического потенциала предприятия и оценок их влияния на общие показатели деятельности (прибыль, рост активов, фондов и др.).

2.5 Основные положения концепции построения интегрированной системы обеспечения комплексной безопасности предприятия

Рассмотренные выше архитектурные подходы и анализ типового комплекса средств информационных технологий управления предприятием наукоемкого машиностроения с позиций обеспечения комплексной безопасности позволяют определить основные концептуальные положения для определения целей и разработки конкретных стратегий жизненного цикла интегрированных систем обеспечения комплексной безопасности предприятий (ИСОКБП).

Опыт разработок и реализации ряда комплексных и целевых программ развития предприятий и автоматизированных систем обеспечения их деятельности [14, 19] позволяет сформулировать следующие положения концепции разработки компонентов средств информационных технологий обеспечения деятельности предприятия, в том числе и в сфере обеспечения его безопасности:

- интеллектуальная поддержка традиционных схем управления объектами и ключевых процессов предприятия, осуществляемых действующими подразделениями и специализированными функциональными службами предприятия (служба безопасности, ИТ-служба, служба защиты интеллектуальной собственности, и др.) а

также с привлечением внешних организаций вневедомственной охраны, энергоснабжения, эксплуатации зданий и сооружений, закупок материалов и комплектующих, ремонта непрофильного оборудования, профилактики здоровья и др. контрагентам работающим по договорам услуг и аутсорсинга;

- ориентация не на отдельные частные академические, производственные, технологические, экономические, правовые и прочие тиражируемые модели, а на создание функционально-полного комплекса, сегментированных для отдельных подразделений и производств, адекватных и верифицируемых моделей обеспечения безопасности деятельности с встроенными процедурами их согласования и легитимации;
- создание ситуаций актуализации процессов обеспечения безопасности деятельности закрепленных за отдельными структурными подразделениями предприятия с выявлением основных внутренних и внешних источников угроз безопасности, оценки рисков и их влияния на ключевые показатели деятельности подразделений и предприятия в целом;
- декомпозиция общей модели процессов обеспечения безопасности в рамках логистической схемы согласования различных экономических, производственных, бюджетных, коммерческих, ресурсных, социально-культурных и иных интересов;
- разработка общей единой открытой стратегии обеспечения безопасности предприятия и политик обеспечения безопасности ключевых процессов предприятия в сферах создания научно-технической продукции и услуг предприятия, производственной, технологической, экологической, физической, экономической, информационной и политической безопасности;
- разработка паспортов безопасности объектов и процессов предприятия и реестров функционально-полного комплекса средств организационно- методического, технического и программного обеспечения безопасности, рекомендуемых и/ или разрешенных для применения в подразделениях предприятия;
- создание реальной системы взаимодействия подразделений и лиц, принимающих решения по обеспечению безопасности на соответствующем уровне управления процессами предприятия в условиях перенасыщенной управлением и контролем внутренней и внешней среды предприятия;

- применение унифицированной модели оценки рисков, сценариев и программ действий по обеспечению безопасности;
- использование общих и специализированных баз данных с разграничением уровня доступа к ним различных категорий пользователей, а также исключения несанкционированного доступа к объектам, процессам и ресурсам системы обеспечения безопасности;
- организация независимого мониторинга состояния безопасности ключевых процессов и отдельных обеспечивающих процессов предприятия с целью выявления источников угроз безопасности, «скрытых» нематериальных активов и упущенной выгоды, основанной на ресурсной сбалансированности процессов предприятия, новых инновационных проектов, согласования различных интересов субъектов деятельности с выявлением «общего пространства» и стимулированием конкретных мероприятий для получения синергетического и кумулятивного эффектов при использовании средств обеспечения безопасности.

В Концепции целесообразно особо выделить акценты, связанные с обеспечением безопасности непосредственно в подразделениях – «владельцах» ключевых процессов предприятия, оставляя за службой безопасности и службой информационных систем координирующую роль в методическом и техническом сопровождении средств обеспечения безопасности в основных подразделениях, а также эксплуатации общих средств мониторинга состояния безопасности и разработке соответствующих мероприятий общего характера.

Цели создания системы комплексной безопасности, включая и информационную безопасность должны быть увязаны с основными целевыми показателями и рисками в деятельности предприятия.

Основной целью создания (а для отдельных предприятий модификации и технического переоснащения) интегрированной системы обеспечения комплексной безопасности предприятия является упорядочение, гармонизация и интеграция различных средств организационного, методического, технического и программного обеспечения комплексов средств мониторинга и обеспечения безопасности основных процессов предприятия при воздействии на них внутренних и внешних угроз, планирования общих и частных мероприятий по идентификации угроз безопасности и минимизации ущерба в деятельности предприятия.

Концепция интегрированной системы обеспечения комплексной безопасности предприятия описывает основные положения, которые определяют направления развития методов и средств безопасности предприятия путем автоматизации процессов сбора и обработки данных о состоянии событий-угроз безопасности. Проектирование средств обеспечения безопасности ведется индивидуально для предприятия исходя из целей и задач стратегического развития. При этом учитывается необходимость обеспечения требуемого уровня безопасности в условиях постоянного совершенствования ИКТ при функционировании предприятия в конкурентной среде.

Основные стадии и этапы жизненного цикла ИСОКБП и отдельных частных проектов ключевых процессов предприятия выбираются в соответствии с рекомендациями стандарта ИСО/МЭК 12207.

В таблице 2.3 указаны основные цели каждой стадии и перечень возможных решений, рекомендуемых для дальнейших исследований и принятия решений по проектированию профиля систем обеспечения комплексной безопасности предприятия.

Таблица 2.3 – Пример стадий, целей и основных решений интегрированной системы обеспечения комплексной безопасности предприятий (на основе основных положений стандарта ISO/IEC 15288)

Стадии жизненного цикла ИСОКБП	**Целевые установки стадии**	**Диапазон решений**
Концепция	Определить состав объектов и угроз безопасности предприятия Определить состав показателей устойчивости и целостности и ключевых процессов предприятия Сформулировать концепцию обеспечения безопасности Определить функциональную архитектуру Предложить приемлемые проектные решения Определить состав пользователей и групп реализации проектов обеспечения безопасности, распределение их компетенции, функций, прав и ответственности Разработать спецификации требований к подсистемам и базовым программно-техническим и программно-методическим комплексам средств обеспечения безопасности предприятия. Определить принципы координации деятельности рабочих групп и ресурсообеспечения общесистемного и частных проектов обеспечения безопасности предприятия.	Локальные системы обеспечения безопасности ключевых объектов и процессов предприятия; Решения по безопасности на основе стратегических Программ обеспечения безопасности общества, промышленных корпораций и государства; Интегрированные интеллектуальные системы обеспечения комплексной безопасности предприятия
Разработка соглашений, регламентов и стандартов деятельности по обеспечению безопасности	Уточнить системные требования к средствам обеспечения безопасности в подразделениях, Определить общие регламенты взаимодействия служб обеспечения безопасности предприятия, основных подразделений- владельцев потенциально опасных объектов и процессов предприятия, их внутренних и внешних контрагентов Разработка документооборота служб обеспечения безопасности	Соглашения на основе законодательства РФ Корпоративные соглашения Регламенты, процедуры и форматы обмена данными Протоколы передачи данных

Стадии жизненного цикла ИСОКБП	Целевые установки стадии	Диапазон решений
Проектирование (приобретение) средств обеспечения безопасности	Выполнить анализ процессов и средств обеспечения безопасности ключевых процессов предприятия; Разработать функциональные и математические модели процессов обеспечения безопасности Создать описание проектного решения по выбору средств организационного, методического, технического и программного обеспечения общих и специализированных средств обеспечения безопасности Выполнить анализ рынка средств обеспечения безопасности и провести их тестирование на совместимость с эксплуатируемыми (наследуемыми) целевыми автоматизированными информационными и управляющими системами предприятия Сформировать перечень (реестр) средств обеспечения безопасности, рекомендуемых для применения в системах обеспечения безопасности предприятия Организовать проектирование (закупку) средств обеспечения безопасности Выполнить работы по комплексированию и инсталляции средств ИСОКБП на рабочих местах служб обеспечения безопасности	Разработка систем собственными силами Применение стандартов и типовых проектных решений ведущих разработчиков средств безопасности Применение отраслевых (корпоративных) решений
Эксплуатация	Разработать модели технического обслуживания средств обеспечения безопасности предприятия; Определить требования к знаниям, навыкам и умениям персонала служб безопасности и эксплуатации технического и программного обеспечения; Провести обучение и аттестацию персонала;	Модели технического обслуживания локальных (автономных) систем обеспечения безопасности ключевых процессов и объектов предприятия;

Стадии жизненного цикла ИСОКБП	Целевые установки стадии	Диапазон решений
	Обеспечить выделение необходимых ресурсов для эксплуатации системы; Эксплуатировать систему с целью удовлетворения потребностей пользователей целевых и обеспечивающих АС предприятия в сервисах безопасности.	Централизованный мониторинг состояния объектов службой безопасности Централизованный мониторинг состояния безопасности информационных ресурсов предприятия
Сопровождение	Организовать службу мониторинга и сопровождения средств безопасности предприятия; Разработать регламенты взаимодействия и типовые сценарии анализа инцидентов-угроз безопасности; Анализировать изменения в архитектуре предприятия, продукции, процессах и технологиях и их влияние на состояние безопасности для модификации систем и эксплуатации Обеспечить выделение необходимых ресурсов для длительного функционирование системы с учетом возможной модификации или замены отдельных компонент по мере их морального или физического износа.	Сопровождение средств безопасности силами специализированных служб предприятия; Сопровождение компонент силами разработчиков и поставщиков оборудования и программного обеспечения; Сопровождение силами специализированных организаций.
Завершение (ликвидация)	Анализировать работу систем, вести учет и прогноз технического и морального старения компонент, планировать своевременную замену, выделение ресурсов для ликвидации отдельных компонент и завершения проекта. Перевести в запас, сдать в архив или ликвидировать систему	Замена морально устаревших компонент, уничтожение объектов Реализация компонент на рынке

3 Классификация рисков и модели обеспечения безопасности предприятия

3.1. Архитектура предприятий и системная классификация рисков

Понятие «безопасность предприятия» подразумевает эффективное использование ресурсов, обеспечивающее стабильное функционирование предприятия в настоящем и устойчивое развитие в будущем.

Приведем несколько основополагающих определений. Угроза – это изменения во внешней или внутренней среде субъекта, которые приводят к нежелательным изменениям предмета безопасности. Риск – вероятность наступления вышеназванных нежелательных изменений. Ущерб – это нежелательное качественное изменение предмета безопасности, снижение его ценности для субъекта или его полная утрата.

Риски в деятельности предприятий наукоемкого машиностроения определяются относительно всех системных объектов и процессов деятельности предприятия, рассмотренных в главе 2 данной работы. Риски могут проявляться в силу недостаточного нашего знания о реальных характеристиках процессов предприятия и состоянии системных объектов, оборудования и технологий, в результате негативных воздействий среды, специально спланированных акций контрагентов, конкурентов, нестабильной социально-политической и экономической обстановки в государстве, природно-климатических явлений, техногенных катастроф, а также «неумелыми» или несвоевременными действиями персонала, отказами в работе оборудования и программного обеспечения и другими факторами. В общем виде риски в деятельности предприятий могут классифицированы по следующим группам:

- социально-политические: недостаточно полный учет стратегий, тенденций развития и научно-технической политики государства, а также других регионов присутствия (зарубежных государств);
- законодательные: возможные нарушения в деятельности предприятия в сфере законодательства России и других государств, приводящие к различного рода санкциям органов государственного управления относительно правомочности деятельности предприятия;

- природные (экологические): нарушения в сфере природопользования и охраны окружающей среды, возможные техногенные катастрофы, влияющие на деятельность предприятия;
- технические: отказы в работе технологического оборудования, систем энергообеспечения и жизнеобеспечения зданий и сооружений;
- экономические: снижение ниже допустимого уровня экономических показателей, таких как выпуск продукции, потребность в инвестициях и др., а также увеличение затрат ресурсов на ликвидацию последствий нарушений безопасности (восстановление зданий, технических объектов, информации, замена персонала и др.);
- человеческий фактор: влияние психофизиологических характеристик персонала на процессы предприятия и состояние корпоративной культуры совместной деятельности.

Вместе с тем следует отметить, что эта классификация является достаточно условной, сугубо эмпирической. Основной недостаток такой классификации – сложность определения внутренних и внешних факторов, приводящих к рискам, а главное – сложность определения корреляций между факторами, так как реальные риски практически всегда взаимосвязаны и обусловлены. Например, изменения в экологическом законодательстве могут потребовать принятия решений, не только по изменению технических характеристик изделий, внедрения экологически чистых технологий, но и решений по изменению организационной структуры предприятия, введения дополнительного контроля материалов и комплектующих, изменения системы охраны и доступа к объектам и процессам контроля безопасности предприятия.

Как правило, известные модели оценки рисков разрабатывались специалистами в отдельных сферах деятельности предприятия (модели оценки финансовых рисков, экологического состояния и рисков в природоохранной деятельности, безопасности труда, рисков утраты здоровья персонала и др.) часто без должной координации работ со смежными предметами деятельности. Часто применение таких моделей было инициировано из благих намерений улучшения жизни нашего общества, имело и, иногда имеет до настоящего времени, декларируемые и фактические, латентные цели. Например, целью разработки систем безопасности для ряда государственных и аккредитованных ими «надзорных» организаций является нахождение легитимных способов и инструментов получения, каких

либо ограничений на деятельность предприятий и «привилегий» для организаций занимающихся «тотальным» контролем в сферах деятельности предприятий - введения «обоснованной» платы за ресурсы для такого контроля и др.

Прямое применение таких моделей, даже в силу необходимости исполнения законодательных актов, непосредственно для обеспечения безопасности процессов предприятий мало, что дает для разработки конструктивных моделей обеспечения комплексной безопасности предприятия, оценки возможных и допустимых рисков и принятия мер по их снижению. Во всяком случае, более целесообразным является разработка индивидуальной для каждого конкретного предприятия модели процессов обеспечения безопасности, которая в общем случае может использовать и отдельные модели классических «отраслевых» подходов к обеспечению безопасности, интегрировать действительно работоспособные модели обеспечения безопасности на реально работающих предприятиях, обеспечить их встраивание в целевые и обеспечивающие АС предприятия.

Весьма важными являются вопросы координации деятельности владельцев предприятия, служб определения экономической и технической политики, проектирования продукции и услуг как задающих вектор развития предприятия и собственно служб обеспечения безопасности. Основы безопасности предприятия должны закладываться на самых начальных стадиях проектирования его архитектуры, в проектах реструктуризации предприятия.

В современных условиях с учетом развития информационных технологий практически во всех сферах деятельности предприятий на передний план выступает задача интеграции различных подходов, методов и инструментов с позиций осознанного и объективно необходимого комплекса мероприятий и средств обеспечения безопасности во всех основных процессах предприятия для снижения рисков в деятельности. При этом информационные технологии являются инструментом такой интеграции, так как при грамотном их применении, обеспечивают с единых системных позиций идентификацию угроз, регистрацию событий-инцидентов угроз безопасности, оценку интенсивности и значений внешних негативных воздействий, измерение факторов, аналитическую обработку данных и подготовку рекомендаций по выбору необходимых решений и других мероприятий, вплоть до формирования команд на выполнение

цепочек необходимых действий операторам и другим исполнительным механизмам.

В соответствии с описанным выше подходом к архитектуре предприятия основным инструментом интеграции является «прописывание» процессов обеспечения безопасности для системных объектов предприятия (продукция, технология, инфраструктура, ресурсы), определение для них источников угроз, рисков и сценариев возможных действий по минимизации возможных ущербов. При этом риски, во многом определяются состоянием безопасности информационных технологий на предприятии. Так по данным исследования, проведенного в 2007-2008гг. аналитическим агентством Economist IntelligenceUnit главными источниками ИТ-рисков признаны большой объем изменений, возрастающая сложность систем, а также недостатки в системах безопасности.

В 25% компаний более половины вынужденных простоев обусловлено изменениями в ИТ. При этом за последние три года постоянные изменения и возрастающая сложность ИТ стали основными источниками повышения ИТ-рисков. Это привело к тому, что все больше компаний начинают связывать корпоративные риски с ИТ: 75% респондентов сказали, что управление корпоративными рисками в их организациях тесно связано с управлением ИТ-рисками. Для многих компаний жизненно необходима предсказуемость их деятельности. Принимая во внимание тот факт, что ИТ- и бизнес-риски тесно связаны друг с другом, недостаточная предсказуемость ИТ равносильна недостаточной предсказуемости бизнеса, заключают аналитики. В связи с этим, компании, которым удастся успешно справиться с этими проблемами, будут иметь явное преимущество перед конкурентами.

Для обоснования интегрированной модели обеспечения комплексной безопасности предприятия в основу исходной классификации рисков в обеспечении деятельности предприятия могут быть положены современные подходы к архитектуре предприятия [1], базовые модели деятельности [17], развитие сервис-ориентированной архитектуры к организации информационных систем, а также вполне интуитивно-понятные схемы взаимодействия предприятия с его внешним окружением. В общем случае, именно связи с внешней средой, а также реакции подразделений на негативные внутренние и внешние воздействия и случайные факторы, надежность технологического оборудования и «зрелость»

процессов и определяют возможные направления классификации рисков в деятельности предприятия.

В данной работе предлагается системная классификация рисков по основным сферам деятельности предприятия на основе модификации матричной модели Захмана применительно к задачам обеспечения комплексной безопасности, приведенная в таблице Таблице 3.1.

Для каждой сферы деятельности предприятия, приведенной в первом столбце таблицы, определяются объекты угроз (предмет или процесс, на который направлено негативное воздействие), субъект угроз (указание того, кто является инициатором или носителем угроз), способ выявление и оценки риска, место обнаружения (возникновения) угрозы, время реагирования (когда определена угроза и когда требуется применять необходимые действия по нейтрализации угрозы), какие решения и в какой последовательности должны быть выполнены для устранения или снижения ущерба от угрозы, и тип риска.

По результатам анализа потоков данных и наиболее значимых документов предприятия можно также оценить и возможные типы инцидентов-угроз безопасности.

При построении реальной интегрированной системы обеспечения комплексной безопасности для конкретного предприятия желательно организовать заполнение этой таблицы экспертами – владельцами ключевых процессов, а также специалистами по отдельным техническим направлениям обеспечения безопасности, чтобы увязать содержание таблицы с внешними потоками данных и информационными ресурсами предприятия.

Таблица 3.1 – Системная матрица определения рисков по сферам деятельности (процессам) предприятия

Сферы деятельности (процессы) предприятия	**Объект угроз (что)**	**Субъект угроз (кто)**	**Способ оценки рисков (как)**	**Место возникновения (где)**	**Время реагирования (когда)**	**Действия (решения)**	**Основные риски (Последствия)**
Стратегия и планирование деятельности предприятия	Миссия и стратегия; Программы работ; Продукция; Соглашения с контрагентами	Руководство; Ведущий персонал; Контрагенты	Контроль документов; Экспертиза решений; Моделирование и оценка показателей	Переговорные площадки; Публикации в СМИ	Месяц, неделя, заданный срок по фактам обнаружения угроз безопасности	Программа нейтрализации угроз; Разбор полетов; Координация планов	Социально-политический риск; Законодательный риск (в том числе на территории других государств); Экономический риск.
Проектирование изделий и технологий	Ошибки проектирования; Несоответствие отраслевым и международным стандартам безопасности	Проектировщики Техники-оформители документации Смежные подразделения и контрагенты	Контроль документации; Экспертные системы	Подразделения служб проектирования; Смежники	В течении заданного срока по факту обнаружения	Оценить последствия; Подготовить решения по устранению ошибки	Технический риск; Экономический риск
Соглашения о взаимодействии с заказчиками, потребителями и контрагентами	Тексты соглашений и договоров	Службы технического развития. маркетинга, снабжения и сбыта	Контроль документации; Аудит партнера (контрагента)	Переговорные площадки	По мере выявления угроз безопасности	Сообщения о несоответствии, Остановка текущих операций	Технический риск; Экономический риск (упущенная выгода)
Стандарты, методики	Тексты стандартов предприятия Документация проектов	Службы стандартизации, качества и управления персоналом	Контроль документации; Поиск несоответствий, Гармонизация	Рабочие места исполнителей; Хранилища данных	По факту обнаружения несоответствий	Своевременное обновление	Технический риск снижения качества продукции, работ и услуг

Сферы деятельности (процессы) предприятия	Объект угроз (что)	Субъект угроз (кто)	Способ оценки рисков (как)	Место возникновения (где)	Время реагирования (когда)	Действия (решения)	Основные риски (Последствия)
			терминов				
Эксплуатация зданий и сооружений	Техническое состояние объектов; Эксплуатационные ведомости	Службы эксплуатации; Нарушители пропускного режима	Регламенты доступа, видеонаблюдение; Измерение параметров; Сигнализация и средства пожарной безопасности	Периметр и границы объектов контроля; Конструкция зданий и сооружений	Регламент обслуживания; Заданное время по факту наступления события - инцидента угроз безопасности	Оперативные сообщения службам для принятия мер в зависимости от уровня угроз; Блокировка доступа; Включение систем жизнеобеспечения	Технический риск разрушения зданий и сооружений; Экологический риск; Экономический риск
Снабжение и сбыт продукции	Отклонения показателей качества изделий и материалов	Службы снабжения; Поставщики	Контроль и выявление несоответствий	Склады предприятия и подразделений	График поставок и отгрузки продукции	Запрет использования; Блокировка	Технический риск; Экологический риск; Экономический риск; Утрата доверия клиентов
Энергоснабжение	Сбои в энергоснабжении; Отказы силового оборудования и сетей	Служба главного энергетика; Поставщики энергоресурсов; Потребители	АС контроля энергоресурсов предприятия	Электросети предприятия; Энергооборудование	Регламент обслуживания	Отключение блокировка; Включение резерва	Технический риск; Экологический риск; Законодательный риск; Экономический риск

Сферы деятельности (процессы) предприятия	Объект угроз (что)	Субъект угроз (кто)	Способ оценки рисков (как)	Место возникновения (где)	Время реагирования (когда)	Действия (решения)	Основные риски (Последствия)
Технологическое оборудование	Дефекты оборудования; Отклонения в режимах работы	Поставщики; Операторы; Служба ремонтов	АС контроля состояния оборудования	Рабочие места	Регламент технического обслуживания	Восстановление работоспособности; Замена; Ликвидация	Технический риск; Экологический риск; Законодательный риск; Экономический риск
Взаимоотношения с персоналом и посетителями	Пропускной режим; Уровень доступа к работам и документам	Служба управления персоналом; Служба безопасности; Охрана	Мотивация деятельности; Регламент доступа на предприятие; Правила поведения; Идентификация личности; Видонаблюдение и связь	Бюро пропусков; Переговорные площадки	Постоянно; План мероприятий работ с персоналом	Разъяснение; Мотивация; Обучение; Блокирование; Нейтрализация; Задержание; Воспитание; Наказание; Эвакуация	Человеческий фактор; Технический риск, Социально-экономический риск; Законодательный риск
Информационные ресурсы предприятия	Конфиденциальные данные предприятия	Информационная служба; Служба безопасности; Потребители - пользователи АС	Мониторинг состояния данных; Распределение прав доступа; Политика и настройки безопасности; Контроль СМИ и аудиоинформации	Базы данных целевых АС; Хранилища данных общего и специального назначения	Регламент обслуживания; Заданный период актуализации данных	Блокирование доступа; Шифрование; Восстановление данных; Архивирование	Экономический риск; Технический риск; Законодательный риск

Сферы деятельности (процессы) предприятия	Объект угроз (что)	Субъект угроз (кто)	Способ оценки рисков (как)	Место возникновения (где)	Время реагирования (когда)	Действия (решения)	Основные риски (Последствия)
Системное программное обеспечение целевых АС	Отказы в работе; Несанкционированное применение	Системные администраторы	Лицензирование; Политики безопасности; Тестирование; Мониторинг состояния	Серверы АС и хранилищ данных предприятия	Регламент обслуживания; Программа модернизации и замены компонент	Восстановление; Блокирование доступа; Замена	Технический риск; Экономический риск
Программно-аппаратные платформы АС	Отказы в работе; Несоответствие процессам предприятия; Несовместимость конфигурации	Информационная служба; Системные администраторы целевых АС	Экспертиза проектов; Тестирование; Испытания; Сертификация; Мониторинг состояния	Подразделения предприятия; Серверы и рабочие станции АС	Регламент обслуживания	Восстановление; Блокирование доступа; Замена	Технический риск; Экономический риск
Прикладное программное обеспечение	Несанкционированное применение; Сбои в работе	Конечные пользователи целевых АС	Идентификация и аутентификация доступа; Контроль целевого использования	Серверы и рабочие станции целевых АС	Регламент обслуживания	Блокирование доступа	Технический риск; Экономический риск
Сети ЭВМ и электронные коммуникации	Нарушение целостности, отказы; Несанкционированное подключение к каналу связи и съем информации	Администраторы сетей ЭВМ; Связисты; Провайдеры корпоративных и глобальных сетей ЭВМ; Операторы МТС и сотовой связи	Экспертиза проектов; Защита каналов передачи данных; Контроль каналов связи; Радиомониторинг; Виброакустическая защита	Территория и здания предприятия; Линии и аппаратура каналов связи	Регламент обслуживания	Восстановление работоспособности; Ремонт; Профилактическое обслуживание	Технический риск; Экономический риск

3.2 Анализ факторов обеспечения безопасности на уровнях управления

Проводя анализ рисков в деятельности предприятия, особо следует отметить необходимость четкого определения взаимосвязей между ними и возможности проектным путем разрабатывать процедуры мониторинга событий - инцидентов угроз безопасности и своевременно предусматривать меры по обеспечению безопасности, снижению ущерба от негативных воздействий. Достаточно условно эти мероприятия можно разделить в соответствии с рассмотренной выше классификацией процессов предприятия.

Сравнение формализованных описаний процессов обеспечения безопасности позволяет упорядочить и разделить все процедуры управления рисками предприятия на категории по уникальности:

1) общие – характерные для большинства основных процессов;
2) обособленные – для двух попарно связанных процессов;
3) уникальные – для отдельных специфических процессов и операций,
4) и по ориентированности на тип источников угроз:
5) внешние – для клиентов компании;
6) внутренние – для подразделений компании.

Для каждой группы основных и обеспечивающих процессов предприятия рекомендуется рассматривать вопросы внешней безопасности, внутренней безопасности и безопасности персонала. Приведем некоторые факторы, которые необходимо учитывать при разработке концепций, стратегий, тактики и средств обеспечения безопасности на этих уровнях.

При обеспечении **внешней безопасности** предприятий анализируются все внешние связи предприятия, в том числе на уровне отдельных подразделений, потоки данных, каналы их передачи с учетом возможностей случайного (по ошибке) или намеренного искажения данных внутренним или внешним источником сообщений, потери информации при ее передачи по каналам связи. Этот анализ выполняется при построении процессов обеспечения безопасности, «накладываемых» на основные организационные процессы предприятия (формирование миссии, программ технического развития, маркетинга и сбыта продукции, инновационной и инвестиционной политики, бизнес-планирования, управления проектами и другими процессами «верхнего уровня», а

также процессы подготовки соглашений о сотрудничестве с внешними организациями).

При анализе процессов предприятия можно использовать внешние диаграммы потоков данных предприятия, построенные в соответствии с рекомендациями стандарта IDEF0, UML и др. При этом необходимо учитывать:

- конкретное определение внешних контрагентов предприятия, содержание сущности взаимоотношений с внешним окружением и значения конкурентной борьбы в основных сферах деятельности предприятия, возможные формы и методы недобросовестной конкуренции;
- организационно-правовое обеспечение деятельности и состояние законодательства в сферах деятельности предприятия в регионах присутствия, возможные последствия его случайного или преднамеренного нарушения;
- определение направлений и содержания информационно-аналитической работы в подразделениях в интересах обеспечения экономической безопасности (а также влияния на экономическую безопасность возможных нарушений основных и обеспечивающих процессов предприятия);
- способы оценки состояния реальных конкурентных отношений, идентификации и определения потенциальных угроз со стороны основных конкурентов предприятия, партнеров, органов власти и других институтов общества;
- методы поиска и использования источников информации для маркетинговых исследований, деловой разведки в интересах разработки технической политики предприятия;
- приёмы оценки намерений конкурентов и степени их угрозы предприятию;
- методы проверки технической компетенции и благонадёжности партнёров (контрагентов) предприятия;
- порядок взаимодействия с контролирующими (проверяющими) органами, определение возможности наступления негативных последствий и их возможная, в рамках действующего законодательства, нейтрализация;
- методы экономической и технической контрразведки и их применение в целях обеспечения безопасности предприятия;
- методы оценки эффективности средств обеспечения комплексной безопасности предприятия;

При обеспечении **внутренней безопасности** процессов предприятия анализируются основные процессы научно-производственной деятельности предприятия, для которых определяются:

- потенциальные угрозы внутренней безопасности, объекты защиты и субъекты безопасности в конкретных подразделениях, целевых и обеспечивающих АС предприятия;
- организационная структура, формы и методы обеспечения деятельности подразделений службы безопасности и их взаимодействия с другими структурными подразделениями и службами предприятия;
- организация пропускного режима и требования к режимам доступа физических лиц на территорию предприятия;
- структура системы охраны объектов, формы, методы и режим охраны;
- организация доступа пользователей к информационным ресурсам общего и специального назначения и средствам автоматизированных рабочих мест;
- состав документооборота и системы оперативных сообщений служб безопасности;
- виды информации, составляющей коммерческую тайну, способы её получения и предоставления, а также сведения, которые не могут составлять коммерческую тайну в соответствии с Законом РФ №98-ФЗ от 29.07.2004 г. «О коммерческой тайне»;
- способы оценки сроков конфиденциальности информации и порядок организации защищённого документооборота, допуска лиц к работе со сведениями, составляющими коммерческую тайну;
- возможные каналы утечки интеллектуальных, материальных и финансовых ресурсов;
- определение мест накопления и хранения конфиденциальной информации предприятия;
- порядок проведения внутреннего и внешнего аудита безопасности процессов предприятия;
- состав имеющихся средств обеспечения безопасности процессов, в том числе в составе эксплуатируемых АС, специализированных средств охраны труда и техники безопасности.

На уровне обеспечения безопасности **работы с персоналом** – «владельцами» процессов предприятия на всех уровнях управления, потребителями и контрагентами определяются:

- кадровая политика предприятия с точки зрения обеспечения безопасности относительно отдельных групп и специализаций персонала;
- внутренние правила и ответственность за их нарушение;
- обучение персонала организации работы с клиентами, контрагентами и посетителями;
- участие ведущего персонала в работе других предприятий, каналы утечки интеллектуальных, материальных и финансовых ресурсов, материальная ответственность персонала;
- средства обеспечения личной безопасности персонала на рабочих местах, технологических линиях и установках;
- информационная работа с персоналом, методы получения значимой информации о путях;
- текущая работа с сотрудниками, владеющими конфиденциальной информацией предприятия;
- мотивация персонала;
- создание на предприятии системы противодействия внутрифирменному мошенничеству и разгильдяйству;
- предупреждение злоупотреблений персонала;
- работа с внутренними и внешними СМИ;
- защита информации в работе службы управления персоналом.

При описании процессов обеспечения безопасности на каждом уровне предприятия в качестве основы можно использовать рассмотренную выше классификацию угроз безопасности, а результаты оформлять и документировать в виде паспортов безопасности предприятия и ресурсов обеспечения безопасности.

3.3 Задачи обработки сведений об инцидентах угрозах безопасности предприятий

В реальных условиях основными механизмами идентификации и определения рисков в деятельности предприятий является анализ проектной и технологической документации, соглашений о сотрудничестве, коммерческих предложений контрагентов и заказных спецификаций, наблюдение реальных процессов. Выявление рисков осуществляется на основе анализа потоков внутренних и внешних данных о событиях-инцидентах угроз безопасности поступающих в систему от достаточно большого количества разнообразных источников. Тем не менее, любое событие может быть представлено как зафиксированное на определенный

момент времени состояние входящего, в общем случае случайного нестационарного потока данных.

Основными задачами обработки такого потока в интересах обнаружения и нейтрализации негативных событий и минимизации ущербов в деятельности предприятия и его ключевых процессов являются:

- определение регламента обслуживания соответствующего потока данных (сообщений, сигналов, документов);
- собственно регистрация события и определение источника сообщения о событии;
- выделение признаков угроз из потока (в основе информативных для деятельности) отдельных документов и сообщений;
- идентификация типа угроз и возможных последствий развития события и инициируемых им действий источников угроз с одной стороны и элементов принятия решений (в общем случае лиц принимающих решения или интеллектуальных устройств) в системах управления предприятия разного уровня;
- упорядочение потока событий и организация эффективного накопления потока событий (ведение архива истории событий);
- оперативная обработка в соответствии с заранее определенными правилами обработки и принятия решений;
- вторичная обработка массивов разнородных событий и корреляционных связей между ними (поиск взаимосвязанных событий, объектов и субъектов для принятия дополнительных мер, планирования мероприятий и других действий);
- принятие решений и информирование необходимых адресных сообщений для их исполнения.

Выбор методов и инструментальных средств решения этих задач напрямую связаны архитектурой предприятия, составом процессов, уровнем их автоматизации, состоянием баз данных информационных ресурсов и, конечно, принятой классификацией рисков, наличием средств обеспечения безопасности общего и специального применения. Для обоснованного выбора средств обработки (мониторинга) событий об угрозах безопасности рекомендуется для каждого конкретного предприятия формировать на основе паспортов безопасности объектов для каждого типа событий (или потока данных) комплекс сценариев обработки данных о событиях-инцидентах угроз безопасности.

В качестве примера в таблице 3.2 приведена исходная форма описания перечня событий- инцидентов угроз безопасности, которая может быть положена в основу разработки сценариев их обработки и соответствующего программного обеспечения в составе автоматизированных рабочих мест подразделений безопасности или встраиваемых программных модулей в целевые АС предприятия. В таблице принята следующая условная классификация кодов (типов) событий-инцидентов угроз безопасности:

- БТО – безопасность технологического оборудования;
- ЧСП – чрезвычайные ситуации, техногенные катастрофы, пожары, аварии систем жизнеобеспечения и др. события угрожающие безопасности персонала предприятия;
- НСД – несанкционированный доступ на объекты предприятия;
- ЭБП – экономическая безопасность предприятия;
- БИР – безопасность информационных ресурсов предприятия;
- БПП – безопасность продукции предприятия.

Этот пример носит иллюстративный характер. В реальных условиях представленная классификация может быть уточнена, дополнена и детализирована. Например, при кодировании событий к представленным выше кодам можно добавить такие атрибуты, как код подразделения, код регистратора событий, код процесса (продукции, ресурсов) объекта угроз безопасности.

По результатам обработки достаточно полного списка событий для отдельных объектов и процессов предприятия производится их автоматическое упорядочивание и классификация, запись в соответствующие разделы базы данных мониторинга состояния угроз безопасности, строятся корреляционные связи между текущими и «историческими», ранее зафиксированными событиями, определяются оценки значимости конкретного события для обеспечения безопасности и формируются адресные рекомендации по принятию мер в зависимости от типа события и угроз безопасности на соответствующем уровне принятия решений.

Таблица 3.2 – Перечень событий – инцидентов угроз безопасности предприятия и требования к их обработке (условный пример отдельных записей)

Код, дата, время	**Наименование события (факта)**	**Документ, вид сообщения, сигнал**	**Регламент обслуживания**	**Накопитель, таблица БД (условно)**	**Правила обработки**	**Решения и действия**
БТО 15.11.07 12.10	Отказ технологического оборудования (например, станка А в подразделении Б)	Телефонограмма, сигнал об отказе оборудования	По мере возникновения, частота опроса в соответствии с регламентом обслуживания	Отказы оборудования	Зарегистрировать, оценить ситуацию и возможные последствия	Определить меры, потребности в ресурсах, назначить исполнителей
ЧСП 20.02.08 9.00	Сообщение о штормовом предупреждении или других чрезвычайных ситуациях за период	Телефонограмма из МЧС	Ежедневная справка об отсутствии; Оперативное сообщение о факте	Метеопрогноз, чрезвычайные ситуации	Оценить уровень угрозы персоналу, зданиям и сооружениям	Подготовить помещения, принять меры по эвакуации персонала
НСД 03.04.08 02.45	Попытка (факт) нарушения пропускного режима неизвестными лицами в количестве 3-х человек	Сигнал с поста охраны, запись системы видеонаблюдения	В реальном масштабе времени	Нарушители режима доступа	Зарегистрировать факт, идентифицировать лиц и их намерения, оценить уровень угрозы, проверить историю	Задержать, допросить, ликвидировать угрозу
ЭБП 13.08	Сообщение о задержке поставок комплектующих изделий (по причине банкротства	Письмо, публикация в СМИ, телефонограмма, отчет о коман-	По факту	График поставок	Оценить достоверность сообщения и возможные последствия для предприятия, резерв време-	Игнорировать, заменить поставщика, изменить конструкцию изделия,

Код, дата, время	Наименование события (факта)	Документ, вид сообщения, сигнал	Регламент обслуживания	Накопитель, таблица БД (условно)	Правила обработки	Решения и действия
	поставщика, отсутствия транспорта и др.)	дировке специалистов			ни для принятия мер	предъявить иск
БИР 05.06.08 14.24	Попытка (факт) несанкционированного доступа в базу данных информационных ресурсов предприятия	Сообщение межсетевого экрана	В реальном масштабе времени	Журнал регистрации пользователей	Проверить источник сообщения, инициатора несанкционированного доступа	Блокировать доступ, проверить целостность БД, восстановить данные, обновить «черный» список, изменить параметры защиты
БПП 12.06.08	Рекламация на продукцию	Письмо, акт, протокол	По факту	Претензии	Зарегистрировать, проверить на актуальность и обоснованность претензии	Заменить, исправить, отказать

Вопросы обработки сложных событий в автоматизированных системах предприятий в последние годы выделяются в специализированное направление ряда крупных разработчиков типовых проектных решений в сфере ИКТ. По данным журнала Открытые системы IBM до конца года 2008 г. планирует выпустить на рынок новую линейку программных продуктов для обработки бизнес-событий (Business Event Process, BEP) - так Голубой гигант предпочитает называть обработку сложных событий (Complex Event Processing, CEP). BEP и CEP системы занимаются поиском и отслеживанием шаблонов, зависимостей и событий среди обилия деловой информации с тем, чтобы своевременно просигнализировать и предпринять соответствующие действия в случае успешного обнаружения связанных событий по заданным критериям и совпадением отдельных атрибутов, внешне несвязанных событий.

Например, если система финансового обслуживания регистрирует в течение одного дня такие события, как смена адреса клиента, смена пароля и последующую крупную денежную транзакцию, это с большой вероятностью свидетельствует о мошенничестве.

Решения по регистрации и мониторингу бизнес событий websphere Business Events 6.2 включает в себя инструменты для рядовых пользователей-аналитиков предприятий, участвующих в процессах обработки событий и подготовки данных для принятия решений. Например, программирование заменяется удобными методами определения нужных шаблонов, при обнаружении которых необходимо информировать лиц принимающих решения по закрепленным за ними предметам и сферам деятельности.

Продукт WebSphere Business Events eXtreme Scale 6.2 предназначен для обработки большого объема информации для предприятий с большим количеством виртуальных ЭВМ в распределенной сети и, которые требуют непрерывного мониторинга на случай возникновения определенных событий.

Для систем с большим количеством удаленных пользователей предлагаются решения по поддержке систем контроля транзакций Transaction Server Support Pac. Реализовнная на мэйнфрейме система CICS (Customer Information Control System) для онлайновой обработки транзакций и информации о клиентах сможет передавать события для последующей их обработки в WebSphere Business Events. По данным IBM, 3770 ее заказчиков используют рассмотренные

выше продукты BEP-линейки, включая 18 компаний, входящих в верхнюю двадцатку из списка крупных предприятий Fortune 500, и 20 крупнейших банков из списка Global 500.

Анализ современных подходов к обработке сложных событий в различных АС показывает актуальность и целесообразность их применения и в задачах обеспечения комплексной безопасности предприятий. Однако при принятии решений об их использовании следует отметить необходимость проведения достаточно детального анализа процессов предприятия, согласования интерфейсов целевых и обеспечивающих АС, унификации средств описания информационных ресурсов общего и специального назначения, а также наличия устойчиво работающих коммуникаций между различными ОТС предприятия. Особое внимание при проведении такого анализа должно уделяться оценке функциональной целостности предприятия в целом и его различных ОТС.

Представляется также целесообразным в рамках ИСОКБП использовать аппарат обработки событий-инцидентов угроз безопасности предприятия на предмет поиска в текстах сообщений и различного рода документов отдельных слов и их сочетаний, описывающих сведения, подлежащие защите. Работа такой автоматизированной системы мониторинга и поиска инцидентов-угроз безопасности может быть организована в фоновом режиме с минимальным участием подразделений безопасности. Выделенное из потока данных сообщение об источнике угрозы может передаться аналитику-эксперту, либо непосредственно ЛПР, для оперативного анализа и подготовке решения.

4 Оценка функциональной целостности организационно-технических систем предприятий

В общем случае основной целью функционирования ОТС предприятий и совокупности их обслуживающих целевых и обеспечивающих АС является удовлетворение потребностей в обеспечении надежного и своевременного представления полной, актуальной и достоверной информации о состоянии объектов, процессов и ресурсов предприятия, оценки внешних воздействий и возмущений для своевременного принятия решений. Степень выполнения данных потребностей в различных условиях эксплуатации системы, в том числе потенциально опасных, характеризуется понятием качества функционирования АС с точки зрения ее конечного пользователя.

Безопасность является одним из необходимых условий достижения требуемого качества функционирования АС. Она определяется состоянием защищенности ОТС от различных угроз, и в итоге – способностью АС обеспечить конкретному пользователю доступность, целостность и конфиденциальность информации в системе. Таким образом, формируемые требования к качеству функционирования АС должны быть направлены на достижение целей системы при ограничениях на допустимые затраты и уровень безопасности.

При этом должно учитываться, что системные требования к качеству функционирования ОТС и обеспечению безопасности являются взаимосвязанными. Основополагающим Российским стандартом в сфере оценки качества автоматизированных информационных систем наукоемких предприятий, обеспечения их надежности и функциональной целостности является ГОСТ РВ 51987 «Информационные технологии. Комплексы средств автоматизированных систем. Требования и показатели качества функционирования информационных систем. Общие положения».

Этим стандартом определяются основные термины и определения, процессы и модели оценки функциональной целостности АС различного назначения, и в частности:

- требования к надежности и своевременности представления информации (требования качества), которые характеризуют доступность информации (требование безопасности);

- требования к полноте и достоверности используемой информации (требования качества), которые характеризуют ее актуальность и целостность;
- требования к защищенности от несанкционированного доступа и сохранению конфиденциальности информации, а также к безошибочности действий должностных лиц, к защищенности ИС от опасных программно-технических воздействий также являются непосредственно требованиями безопасности.

Качество функционирования АС предприятий с учетом факторов, воздействующих на информацию, определяется уровнями целостности системы и ее составных компонентов. Уровни целостности должны устанавливаться в проекте предприятия, оцениваться и, при необходимости, уточняться при проектировании конкретных изделий и услуг, разработке технологий и контролироваться при производстве и эксплуатации системы.

В таблице 4.1 приведены основные характеристики качества функционирования АС с позиций обеспечения комплексной безопасности ОТС (предприятия). Эти характеристики должны оцениваться и контролироваться на предмет соответствия нормам и показателям безопасности, формируемых в зависимости от частоты угроз, объема и интенсивности негативных воздействий, сценариев развития событий и их последствий с учетом специфики конкретного предприятия.

Критерии выбора того или иного уровня качества функционирования ОТС, отвечающего задаваемому уровню целостности системы, определяются основе оценки достигаемой эффективности и/или потенциального ущерба от реализации возможных угроз системе. Обычно оценку проводят при допустимом или повышенном риске. Требования при допустимом риске заказчика являются наиболее жесткими. Полной проверке на соответствие этим требованиям подлежит вся ОТС в целом и составляющие ее подсистемы.

Выполнение этих требований является гарантией обеспечения безопасности информации и приемлемого уровня качества функционирования АС. Вместе с тем подготовка, проведение испытаний и доработка АС на соответствие данным требованиям характеризуются гораздо большими затратами по сравнению с требованиями при повышенном риске заказчика.

Таблица 4.1 – Соответствие угроз информации и основных характеристик качества функционирования АС

Потенциальные угрозы	**Характеристики качества функционирования АС**
Ухудшение качества представления требуемой информации: - при нарушении доступности информации вследствие ненадежности ПТК; - при нарушении сроков представления требуемой информации по запросу или при принудительной выдаче	**Характеристики качества процессов представления требуемой информации:** - надежность представления запрашиваемой или принудительно выдаваемой информации (выполнения технологических операций); - своевременность представления запрашиваемой или выдаваемой принудительно информации (выполнения технологических операций)
Ухудшение качества используемой информации: - при непредставлении части необходимой информации вследствие неполноты ее отражения в ОТС; - при потере актуальности информации на момент ее использования; - при наличии ошибок в информации, пропущенных или допущенных при контроле; - при некорректности функциональной обработки информации.	**Характеристики качества используемой информации:** - полнота используемой информации; - актуальность используемой информации; - безошибочность информации после контроля; - корректность обработки информации.
Нарушение безопасности функционирования: - при наличии ошибок должностных лиц; - при возможных опасных программно-технических воздействий (дефектов ПО, вирусов, целенаправленных атак на ресурсы АС); - при несанкционированном доступе к информационным ресурсам; - при нарушении конфиденциальности информации	**Характеристики безопасности функционирования АС:** - безошибочность действий должностных лиц; - защищенность от опасных программно-технических воздействий; - защищенность от несанкционированного доступа; - конфиденциальность информации

Требования заказчика при повышенном риске являются менее жесткими, а их реализация – менее дорогостоящей по сравнению с требованиями при допустимом риске. Использование данного варианта требований обусловлено тем, что на практике исчерпывающая проверка функционирования сложной системы при реальных ограничениях может оказаться нецелесообразной из-за быстрого морального старения, использования ранее хорошо зарекомендовавших себя подсистем или невозможной по другим соображениям.

Вследствие этого минимальной гарантией обеспечения качества функционирования АС является выполнение требований заказчика при повышенном риске. При формулировании этих требований учитываются положения технической политики, обосновывающей нецелесообразность или невозможность задания и выполнения требований заказчика, характерных для допустимого риска.

Общая модель процессов оценки функциональной целостности ОТС предприятия приведена на рисунке 4.1. Модель предусматривает оценку общесистемных решений с позиций определения рисков в деятельности, анализа возможных сценариев функционирования системы в обычных и критических ситуациях, оценку допустимых ущербов и определение требований к обеспечению целостности системы включая требования к общесистемным решениям и архитектуре предприятия, техническим средствам реализации проектов безопасности, организационному обеспечению и управлению персоналом и программному обеспечению целевых и обеспечивающих АС предприятия.

В состав типовых методик оценки качества функционирования ОТС включаются модели, представленные в таблице 4.2.

Рис. 4.1. Процессы оценки функциональной целостности организационно- технических систем

Таблица 4.2 – Состав типовых методик оценки качества функционирования ОТС

Наименование модели	**Краткое описание**
1. Анализ системотехнических требований к ОТС предприятия (оценка надежности представления информации)	Требуемая надежность представления информации в ОТС в течение заданного времени обеспечивается на основе использования механизмов дублирования и резервирования и достижения рационального соотношения между временем наработки компонентов АС на отказ и временем восстановления после отказа. Здесь под компонентами АС понимаются программно-технические комплексы и персонал эксплуатации, обслуживания и ЛПР.
2. Оценка своевременности и надежности выполнения технологических операций и представления выходной информации	Требуемая своевременность обработки запросов обеспечивается на основе выбора технологий обработки запросов с достаточной производительностью обработки, а также рациональной настройки параметров (например, распределения информационных потоков по приоритетам). Процессы обработки запросов моделируются как процессы массового обслуживания с заданным законом распределения входного потока запросов на представление данных
3. Оценка полноты оперативного отражения в информационных системах ОТС новых объектов учета	До момента, пока новые объекты учета, ранее не учтенные и появившиеся в динамике функционирования ОТС, не доведены до АС, формально отсутствует полнота оперативного отражения требуемых объектов учета (это особенно важно для систем безопасности). Требуемая полнота обеспечивается на основе реализации рациональных технологий обнаружения, сбора и обработки первоначальной информации. Процесс моделируется системой массового обслуживания с бесконечным числом обслуживающих приборов.
4. Оценка актуальности обновляемой информации	Требуемая актуальность обновляемой информации о реально существующих объектах учета обеспечивается выявлением значимых изменений и достаточно частого обновления информации в ОТС. Модель определяет вероятность сохранения актуальности информации при различных статистических распределениях входных потоков данных и различных способах (технологиях) их обработки.
5. Оценка безошибочности выходной информации после контроля	Требуемая безошибочность информации в документах на различных типах носителей обеспечивается на основе использования эффективных средств и способов выявления и исправления ошибок (в том числе по скорости, по недопущению ошибок контроля 1-го и 2-го рода) и рацио-

Наименование модели	Краткое описание
	нальной регламентации работы контролера – человека или специализированной экспертной системы. Модель оценивает вероятность обнаружения ошибок в зависимости от допустимого времени работы контроллера и объема проверяемых документов.
6. Оценка корректности обработки информации	Требуемая корректность обработки информации обеспечивается на основе использования эффективных способов анализа и переработки информации (как с использованием, так и без использования прикладного ПО), позволяющих учесть принципиальные моменты и не допустить алгоритмических ошибок в реальных условиях функционирования АС. Модель определяет приемлемые соотношения между объемом анализируемой информации, частью принципиальной информации, подлежащей учету, скоростью анализа информации, частотой ошибок аналитика, длительностью его непрерывной работы и ограничениями на допустимое время обработки информации в системе.
7. Оценка сохранения конфиденциальности информации	Требуемая конфиденциальность информации обеспечивается на основе реализации мероприятий, гарантирующих защищенность информационных ресурсов системы от несанкционированного доступа до истечения периода объективной конфиденциальности данной информации. Модель определяет приемлемые соотношения между временем смены значений параметров преград системы защиты и их расшифровки (вскрытия) и периодом объективной конфиденциальности информации для одной преграды.
8. Оценка безошибочности действий должностных лиц ОТС и персонала АС	Требуемая безошибочность действий должностных лиц ОТС в течение заданного периода времени обеспечивается на основе профотбора, специальной подготовки персонала, выполнения эргономических требований, реализации и использования эффективных средств программной поддержки их деятельности. Модель определяет для отдельного должностного лица, приемлемые соотношения между частотой возможных ошибок, временем их обнаружения и восстановления целостности системы.
9. Оценка защищенности ОТС от опасных программно-технических воздействий	ОТС считают защищенной от опасных программно-технических воздействий в течение заданного периода времени, если к началу периода целостность системы обеспечена, либо источники опасности не проникают в систему, либо не происходит активизации инициирующего события. Модель защиты основана на периодической

Наименование модели	Краткое описание
	профилактической диагностике целостности системы. Предполагается, что существуют не только средства диагностики, но и способы восстановления необходимой целостности системы при выявлении проникших источников опасности или следов их негативного воздействия. Требуемая защищенность ресурсов системы обеспечивается на основе реализации достаточного количества защитных преград, выбора относительно стойких к вскрытию средств и алгоритмов защиты и рациональной частоты смены параметров защиты. Процесс моделируется как последовательность преодоления преград нарушителем и оценки вероятности ее преодоления (с последующей оценкой ущерба).
10. Оценка защищенности информационных и программно-технических ресурсов ИС от несанкционированного доступа.	В модели оценивается вероятность несанкционированного доступа к информационным ресурсам (базам данных) предприятия в заданном интервале времени в зависимости от выбранного типа и характеристик настроек межсетевых экранов и возможных сценариев несанкционированного доступа к информационным ресурсам из внутренней и внешней среды предприятия.

Формальный аппарат этих методик и необходимые расчетные формулы для моделирования приведены в [28-30, 42]. Целесообразность применения этих методик и соответствующих программных средств обработки данных зависит от сложности ОТС, состава целевых АС и характеристик, основных прикладных задач. В таблице 4.3 приведены рекомендации по применению этих моделей для обеспечения безопасности функционирования целевых АС предприятий машиностроения. Звездочки в ячейках таблицы определяют необходимость и целесообразность применения этих или других аналогичных по функциям моделей для определенных типов АС, эксплуатируемых или проектируемых на предприятиях наукоемкого машиностроения.

Основными системными требованиями к обеспечению безопасности являются:

- требования к надёжности и своевременности предоставления данных;
- требования определения потенциальных внутренних и внешних источников угроз обеспечения безопасности продукции, ресурсов, технологий;
- обеспечение приемлемого уровня доступа пользователей к элементам системы;
- требования к полноте, достоверности и актуальности данных, поступающих и исходящих из системы;
- требования к безошибочной деятельности должностных лиц.

Степень реализации целей функционирования системы зависит от объективных и субъективных факторов (ГОСТ РФ 5127Т-2001г). Основные показатели надёжности работы системы (ГОСТ Р 51987 – 2002г). Этот стандарт устанавливает общие положения в части определения системных требований и показателей качества функционирования.

К настоящему времени, достаточно широко апробированные стандарты ITIL и COBIT предлагают проверенные временем архитектурные модели, процессы обследования оценки показателей качества и внешнего независимого аудита информационных систем, которые можно использовать для описания различных информационных систем предприятия и средств обеспечения их безопасности.

Таблица 4.3 – Применяемость типовых моделей оценки надежности и безопасности целевых автоматизированных систем предприятия

Тип АС предприятия	Рекомендуемые модели для оценки надежности и безопасности целевых АС предприятия (нумерация моделей в соответствии с табл. 4.2)									
	1	2	3	4	5	6	7	8	9	10
АС научных исследований	*	*		*		*	*			
САПР технических объектов и технологий и технологических процессов	*				*	*		*		
АС управления технологическими процессами и установками (жесткие системы реального времени)	*	*	*					*		
АС управления процессами предприятия	*	*		*		*		*		*
АС управления производственными и технологическими процессами реального времени	*	*								
АС испытаний объектов производства	*	*			*	*		*		
АС контроля и жизнеобеспечения зданий, сооружений и помещений предприятия	*	*	*	*				*	*	
Системы ведения баз данных общих и специализированных информационных ресурсов предприятия	*		*	*		*	*	*	*	
Системы представления данных на сайтах (порталах) предприятий	*			*						

5 Методология построения профиля прикладных автоматизированных систем предприятия

В основу методического обеспечения работ по совершенствованию архитектуры и мероприятий по программам устойчивого и безопасного развития предприятий могут быть положены апробированные на различных объектах и находящиеся в развитии методологии, использующие:

- базовые функционально полные модели деятельности предприятий, учитывающие их основные системообразующие характеристики;
- экспертно-статистические методы оценки сложности объектов, потенциала развития основных направлений деятельности предприятия и их ранжирования по различным критериям оценки и приоритетам;
- модели оценки привлекательности инвестиций в инновационные проекты и «точки роста» предприятия (стратегические продукты и услуги, востребованные заказчиками);
- модели открытого взаимодействия субъектов хозяйствования и современные средства информационных технологий (базы данных, моделирующие программные системы, сети ЭВМ и средства электронных коммуникаций);
- методы согласования интересов, координации действий и узаконивания решений, основанные на знаниях объективных законов развития организационно-технических систем и установленных обществом «правилах» соблюдения культурных и этических норм совместной деятельности;
- технологии проблемно-ситуационного моделирования совместной деятельности специалистов в сложных слабо-формализуемых ситуациях.

Опыт реализации ряда целевых программ развития предприятий позволяет сформулировать следующие положения, которые необходимо учитывать при разработке систем управления предприятиями и, соответственно, систем обеспечения их безопасности:

- интеллектуальная поддержка традиционных схем и процедур управления, осуществляемая квалифицированными специалистами и командами предприятия и специализированных консультационных фирм;

- ориентация не на отдельные частные макро и мини экономические, правовые финансовые, и прочие тиражируемые модели, а на создание комплекса моделей управления предприятием и обеспечения совместной деятельности специалистов с встроенными процедурами их согласования и принятия решений на разных уровнях управления;
- создание ситуаций актуализации и доступности моделей управления предприятием, интеграции интеллектуальных ресурсов, продукции и услуг предприятия в смежных областях деятельности и «точках роста» экономики региона;
- декомпозиция конструктивной модели предприятия в рамках логистической схемы согласования различных экономических, бюджетных, коммерческих, ресурсных, социально-культурных и иных интересов региона;
- создание реальной системы взаимодействия подразделений предприятия и внешних структур с закреплением прав, компетенций и ответственности каждого подразделения.
- организация мониторинга пересечения отдельных инновационных проектов предприятия с международными, федеральными и региональными Программами и проектами с выявлением “общего пространства” и стимулированием конкретных проектов для получения синергетического и кумулятивного эффектов.

Опыт разработки систем управления в организационно-технических системах (ОТС) показывает принципиальную необходимость применения методологии открытых систем для упорядочивания согласованной деятельности различных специалистов. В последние годы методология открытых систем находит все большее применение преимущественно при формировании общей среды функционирования открытых систем (выбор программно-аппаратных платформ, операционных систем, стандартизация протоколов, интерфейсов, унификация информационных служб и др. в соответствии с требованиями и рекомендациями руководства по проектированию профилей среды открытой системы [50]).

Требования стандартов и спецификаций закрепляются в виде набора функциональных стандартов, в которых отражаются особенности использования базовых стандартов при реализации прикладных систем, в том числе в сфере деятельности предприятия.

Профиль – это совокупность нескольких базовых стандартов и других нормативных документов, описаний организационных и технических решений, правил взаимодействия элементов с четко определенными и гармонизированными подмножествами обязательных и факультативных возможностей, предназначенных для реализации заданной функции или группы функций.

Функциональная характеристика (заданный набор функций) объектов ОТС является исходной информацией для формирования и применения профиля этого объекта или процесса. Профиль не может противоречить использованным в нем базовым стандартам и нормативным документам. На базе одной и той же совокупности стандартов могут формироваться и утверждаться различные профили для разных проектов и сфер применения.

В профилях сосредотачиваются наборы базовых стандартов из перечисленных выше групп, предназначенных для регламентации конкретных прикладных функций открытых систем. При этом могут использоваться требования и параметры отобранных для профиля базовых стандартов, а также могут дополнительно применяться некоторые стандарты де-факто и формализованные спецификации, не отраженные в международных стандартах. При сертификации приложений могут также использоваться базовые стандарты и технические документы в соответствии с назначением и функциями ОТС.

На стадиях жизненного цикла информационных систем выбираются и затем применяются основные функциональные профили: профиль прикладного программного обеспечения, профиль среды информационной системы, профиль защиты информации в системе, профиль инструментальных средств.

Особенно актуальным для предприятий – конечных потребителей ИКТ является разработка функциональных профилей прикладного уровня, направленных на решение задач управления инновационными проектами предприятий и текущими процессами в составе целевых АС. При этом одной из основных задач проектирования профиля следует считать обоснование функциональной полноты и целостности.

Особенно актуальным является разработка функциональных профилей прикладного уровня, направленных на решение задач управления предприятиями как сложными ОТС. В соответствии с современными концепциями федеральной архитектуры предприятий

под предприятием понимается любая организация, осуществляющая тот или иной вид полезной для общества и результативной деятельности и осуществляющей производство востребованной потребителями продукции и услуг, активно взаимодействующая с поставщиками разного рода ресурсов и другими контрагентами.

На основе анализа общесистемных и специфических характеристик предприятий машиностроения в работе [20] предложена базовая модель деятельности предприятия, которая определяет общие процессы, основные системообразуюшие элементы и сферы взаимодействия предприятия с внешним окружением, а также требования к методам описания продукции, процессов и ресурсов предприятия, процессам проектирования деятельности, методам соорганизации специалистов – участников проектов и инструментальным средствам.

Опыт показывает, что состав процессов проектирования системы управления ОТС является достаточно стабильным, может быть типизирован и использован в системах стандартов и профилей взаимодействия открытых информационных систем разного уровня.

Применение известных системных принципов декомпозиции сложных организационно-технических систем, позволяют выделить формально-логическое ядро методов и средств Программ управления и развития предприятий, обеспечивать управление общими и частными проектами и мероприятиями Программ, сравнивать отдельные проекты, находить общие точки и решать задачи согласования интересов на основе принятых правил и стандартов взаимодействия участников.

Для обоснования рациональной структуры профилей безопасности прикладных АС предприятия можно выделить следующие типовые задачи управления в открытых ОТС:

- диагностические задачи оценки состояния уровня безопасности предприятия, определение ключевых процессов, активных элементов и выделение частных объектов и субъектов безопасности (опасности) из среды;
- определение альтернатив взаимодействия активных элементов ОТС предприятия с внешней средой;
- описание моделей взаимодействия выделенного элемента с другими структурами предприятия и внешней средой;
- конструирование моделей принятия и согласования решений;

– поиск прототипов, приобретение или разработка модулей компонент ИСОКБП;
– конструирование организационных механизмов обеспечения взаимодействия подразделений, обеспечивающих безопасность предприятия, служб информационных систем и внешнего окружения.

Для решения этих задач сформировано формально-логическое ядро методов описания архитектуры, процессов функционирования, оценки качества и принятия решений по проектированию, модификации и реструктуризации АС.

Выделение функционально-алгоритмического ядра является основой систем автоматизированного проектирования функциональных профилей АС предприятий и предполагает использование формализованных алгоритмов и эвристических процедур анализа и синтеза системы управления ОТС при неточном задании исходных данных и неполноте информации о системе, возможность настройки ядра на заданные типы объектов проектирования, использование типовых решений, опыта и знаний экспертов по различным аспектам деятельности системы управления ОТС и ее элементов.

В качестве исходной модели проектирования АС, ориентированной на анализ и синтез функционально – полных структур АС положена модель вида

$$S = \{\psi_A, \psi_C, P_0(\psi_A, \psi_C)\},$$

где ψ_A - модель поведения ОТС,

ψ_C - модель средств реализации АС,

$P0(\psi_A, \psi_C)$ – многоместный предикат функциональной целостности преобразования $\psi_A, \mapsto \psi_C$.

Модель поведения задается направленным связным графом ψ_A(A,G), в котором А – множество задач управления объектом автоматизации, G – множество отношений и связей между задачами. Модель структуры задается частично-упорядоченным графом, описывающим структуру объекта проектирования $\psi c(C, R)$, в котором: С – множество структурных элементов средств реализации базиса системы (типовых средств организационного, методического, технического и программного обеспечения), R – множество отношений между ресурсами и интерфейсов между ними.

Для описания задач используется формализованное описание вида $Aij \Rightarrow \{X, F, Y, W, U, E, R, T, L)$, в котором X – входные объекты, F – вид функции управления, W – возмущения внешней среды, Y – выходные объекты (результаты деятельности), E – показатели качества результатов, R – показатели использования ресурсов, T – шкала времени жизненного цикла системы, L – алфавит признаков (тезаурус) описания объектов деятельности ОТС, i – номер функции управления, j – номер структурной подсистемы объекта автоматизации.

На множестве задач системы определяются отношения системности (S), информативности (I), координируемости (K) и технологичности (T) [14]. Аналогичные отношения существуют и между элементами структуры АС. Эти отношения положены в основу алгоритмов упорядочения задач и формирования требований к компонентам АС.

Такое представление задач управления хорошо согласуется с базовыми стандартами IDEF0, UML, а также рядом других международных и национальных стандартов описания продукции, процессов и ресурсов предприятия. В связи с этим оно может быть положено в основу разработки ядра автоматизированной системы анализа и синтеза (проектирования) профилей АС предприятий и отдельных компонент конкретных индивидуализированных целевых и обеспечивающих АС предприятия.

При этом задачей системного проектирования профиля АС предприятия является поиск таких ψ_A и ψ_C, при которых преобразование $\psi_A, \mapsto \psi_C$ существует при заданном (желательно оптимальном) качестве функционирования АС и при условии минимизации ее сложности на всех стадиях жизненного цикла системы.

Связи между элементами моделей ψ_A и ψ_C определяются семантической моделью предметной области деятельности базовой АС в виде И/ИЛИ графа, который определяет обобщенный многоместный предикат функциональной целостности преобразования «функция управления – средства реализации».

Для снятия неопределенности в системе могут использоваться специальные процессы экспериментальных исследований и экспертиз специалистов. Обобщенная структура ядра АС проектирования системы управления ОТС представлена на рис. 5.1.

Инструментальные средства проектирования профиля системы управления ОТС предусматривают настройку на объекты проектирования с применением классификаторов типовых модулей информационного, технического и программного обеспечения. В классификаторе выделены группы типовых функций системы управления ОТС: ввод данных, предварительная обработка, вторичная обработка (расчет параметров и показателей), построение математических моделей процессов и функциональных зависимостей, расчеты управляющих воздействий, координация и согласование решений, формирование выходных документов, сигналов и команд управления для исполнительных органов и отображения информации.

Классификатор построен по иерархическому принципу и может быть детализирован до конкретных модулей и процедур, реализуемых на различных программно-аппаратных платформах и языках программирования.

При этом изменяться может, в основном, внутреннее содержание используемых в системе модулей, реализующих те или иные функции в зависимости от особенностей объектов управления. Применение классификатора функций и унификация внешних описаний модулей и общесистемных интерфейсов открывает хорошие возможности для сборочного проектирования системы управления ОТС на основе применения модулей общеотраслевого и отраслевого назначения.

Таким образом, задача проектирования сводится к формированию спецификаций требований к системе и поиску в базе данных разработчика системы управления ОТС структурных решений и модулей минимальной сложности при заданных показателях качества функционирования ОТС.

Иерархия спецификаций дает определение системы (подсистемы, модуля), описание требований к назначению системы (подсистемы, модуля), условиям функционирования, математическим методам и вычислительным моделям, функциям элементов, входным и выходным данным, ограничения по методам реализации функций, требования к качеству реализации элементов, а также составу диагностических сообщений и диалоговым процедурам «оператор-ЭВМ», сведения об используемых в системе типовых проектных решениях и модулях.

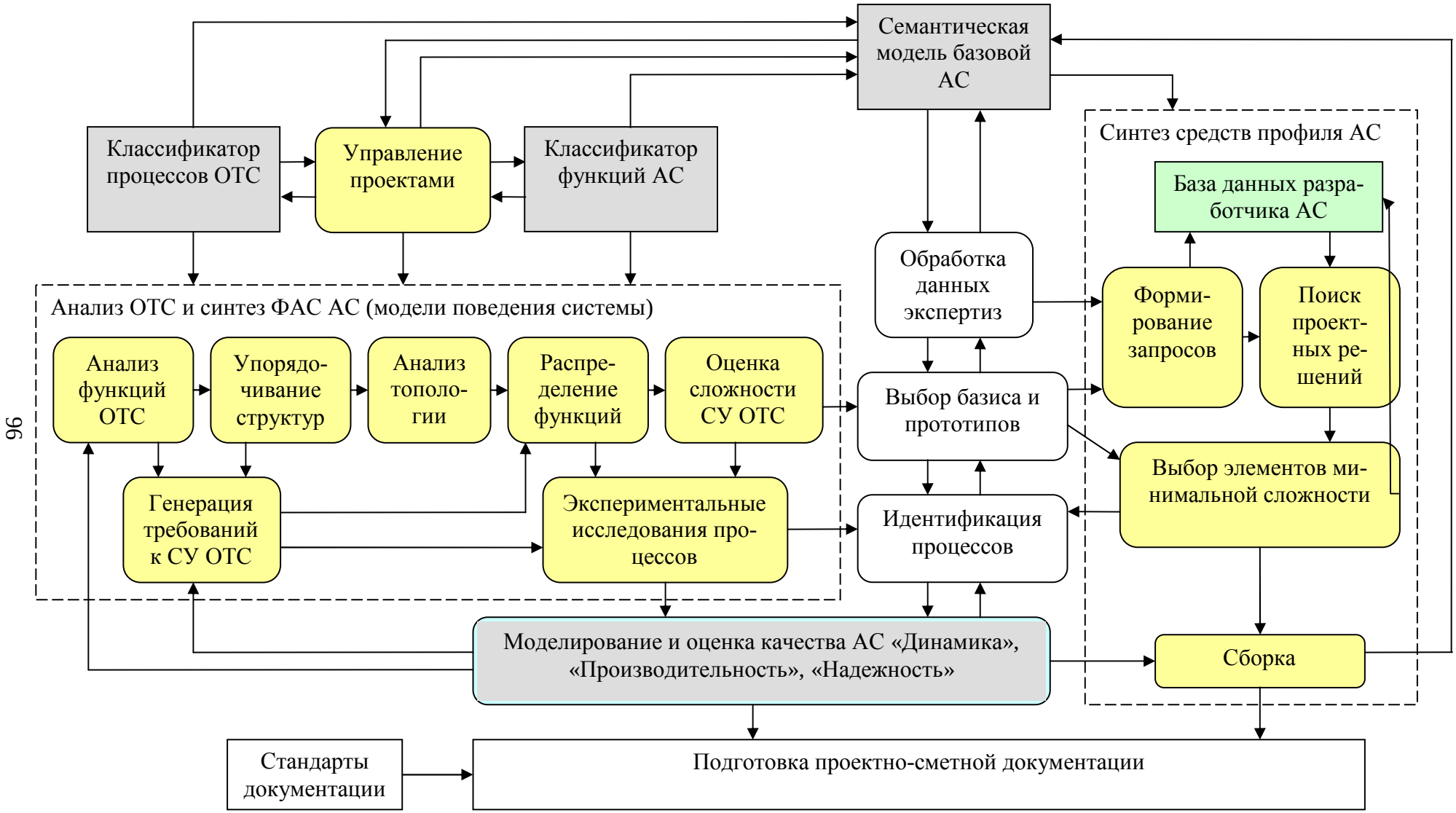

Рис. 5.1. Структура автоматизированной системы анализа и проектирования профилей системы управления ОТС

Спецификации, доведенные до уровня конкретных фактических значений параметров компонента, составляют основу общесистемной документации, построения диаграмм потоков данных, схем баз данных и др. материалов, необходимых для реализации проекта.

Реальные проектировщики и специалисты по управлению проектами АС часто вынуждены действовать в условиях неопределенности, недостатка, а также и избыточности информации, необходимой для принятия решений. Частичное либо полное снятие неопределенности может быть достигнуто за счет использования доступных баз данных и знаний, дополнительных теоретических исследований и экспериментов, применения специализированных систем идентификации и оценивания параметров.

Опыт показывает возможность выделения ряда типовых ситуаций, для которых априори можно определить возможные стратегии действий активного элемента системы управления ОТС и сформировать нормативную модель принятия решений в сложившейся ситуации. Информационная ситуация определяет уровень неопределенности выбора внешней средой своих состояний из заданного ограниченного множества, известного органу управления на момент принятия решений.

Предлагается использовать следующие классы информационных ситуаций:

- I_1 – орган управления располагает точным знанием распределения вероятностей состояния среды;
- I_2 – известно заданное распределение вероятностей состояния среды с неизвестными параметрами распределения;
- I_3 – известна система предпочтений выбора состояния среды из априорных вероятностей распределения множества элементов состояния;
- I_4 – неизвестно распределение вероятностей элементов множества состояний среды и отсутствует активное противодействие среды целям функционирования ОТС;
- I_5 – явно выраженные антагонистические интересы среды;
- I_6 – смешанные ситуации.

Оценка информационной ситуации позволяет построить таблицы принятия решений, определяющие стратегии действий в соответствии с оценкой уровня неопределенности состояния среды и объекта, характеристиками наблюдаемости и управляемости

отдельных подсистем и контуров системы управления ОТС, выбрать необходимые методы и средства реализации.

Предложенная в [22] структура профиля прикладных АС является функционально-полной, обеспечивает реализацию замкнутых контуров управления объектами и процессами и может быть положена в основу разработки специализированных автоматизированных информационных систем обеспечения безопасности для различных ОТС предприятия. В общем случае в состав контура управления могут входить организационные, технические и программные компоненты-модули.

Рациональность синтезированной структуры профиля АИС обеспечения безопасности предприятия может определяться методами моделирования, среди которых целесообразно выделять три класса моделей:

- моделирование и оценка динамических характеристик основных процессов при отработке различного рода возмущений и реагировании на события внутренней и внешней среды ОТС (ДИНАМИКА),
- оценка производительности вычислительных средств и средств электронных коммуникаций (ПРОИЗВОДИТЕЛЬНОСТЬ),
- надежность функционирования, оценка, рисков качества функционирования компонент, включая статистические модели оценки зрелости предприятия и модели оценки деятельности должностных лиц (НАДЕЖНОСТЬ).

К настоящему времени накоплен достаточно большой опыт применения методов моделирования АС и инструментальных средств их поддержки [20], что позволяет также говорить и об их типизации и стандартизации на международном, национальном и корпоративном уровнях.

По результатам моделирования, при больших отклонениях сложности и качества, синтезированных АС могут корректироваться структурные решения, функции элементов и параметры прикладных модулей, реализующих специфические методы управления процессами, такие как оценивание характеристик реальных сигналов, сообщений и возмущений, идентификация математических моделей объектов, расчет управляющих воздействий и др.

Для обеспечения функциональной полноты в составе профиля системы управления ОТС выделяются:

- структурные подсистемы, соответствующие основным структурам объектов, процессов и ресурсам ОТС;
- функциональные подсистемы, соответствующие функциям управления, принятым в базовой модели архитектуры целевых и обеспечивающих автоматизированных систем предприятия;
- программно-методические комплексы (ПМК) для реализации прикладных задач управления (в общем случае могут распространяться на несколько смежных АС предприятия);
- программно-технические комплексы (ПТК) для реализации распределенной среды функционирования ОТС;
- функциональные модули реализации прикладных задач обработки данных и управления;
- информационные модули ведения баз данных о состоянии объектов управления и баз знаний о методах, правилах применения терминов, инструментальных средств, функциональных зависимостях параметров объектов и процессов управления.

По результатам ряда научно-исследовательских работ по развитию методологии открытых систем и инструментальных средств автоматизации проектирования информационных систем, а также опыта их применения в разработках автоматизированных систем различного назначения в работе [21] предложена унифицированная структура базового профиля прикладных АС предприятий, приведенная на рисунке 5.2.

Анализ реальных потребностей предприятий в упорядочении средств управления в целевых и обеспечивающих АС, обеспечении их устойчивой работы и интеграции, стремление к сокращению затрат на их комплектацию, техническое обслуживание и сопровождение показывает возрастание роли унификации и стандартизации элементов информационных технологий (ИТ) и обеспечения их стандартами на конструкцию, технологии проектирования, эксплуатации и сопровождения.

В то же время опыт показывает наличие серьезных проблем в использовании различных стандартов на изделия ИТ и процедуры управления реальными проектами автоматизации предприятий. Требуется согласование понятий, применяемых в международных и национальных стандартах разного уровня.

Рис. 5.2. Пример структуры базового функционально-полного профиля прикладных автоматизированных систем предприятия

Для упорядочения понятийного аппарата в СУ ОТС должны предусматриваться средства, обеспечивающие построение и использование семантических моделей базовых моделей АС, онтологий описания предметной области деятельности, унификации и стандартизации терминов и связей между ними в рамках конкретных проектов.

В основу построения базовых профилей АС предприятий и в том числе профиля прикладных информационных систем обеспечения комплексной безопасности предприятия положены следующие принципы:

- интеграция – создание правовых, методических, технических, технологических, организационных и экономических условий для совместного применение гармонизированных регламентов, отраслевых (корпоративных)стандартов описания продукции, процессов, технологий и ресурсов различных средств автоматизации, комплексов и систем предприятия;
- профессионально-ориентированный доступ к компонентам прикладных АС пользователей, осуществляющих непосредственное управление процессами предприятия;
- необходимый уровень защиты от несанкционированного доступа;
- использование унифицированных структур преставления информационных ресурсов предприятия общего и специального назначения;
- разграничение прав доступа различных групп пользователей к информационным и защита от НСД;
- распределённая обработка информации по узлам принятия решений;
- информационная прозрачность и ориентация на клиента (клиент ориентированная архитектура SOA);
- инвариантность программной реализации и инструментальных средств;
- системная оптимизация функционирования АС и ориентация на минимизацию полной стоимости системы на всех стадиях жизненного цикла конкретной системы.

Открытая архитектура АС и применение унифицированных интерфейсов между подсистемами и базовыми модулями, возможности внешнего дополнения и детализации типовых компонент обеспечивает выбор необходимых и достаточных средств организационного, информационного, программного и технического

обеспечения, позволяет решать задачи формирования базовых функциональных профилей целевых и обеспечивающих систем предприятий.

Следует также отметить актуальность этих работ в связи с развитием систем электронного взаимодействия предприятий и инфраструктуры поддержки инноваций при реализации национальных проектов, систем электронного правительства и других социально-значимых проектов [4], в которых может использоваться продукция производственного цикла.

В состав базового прикладного профиля АС предприятий включаются:

- функциональные модели деятельности субъектов предприятия;
- модели распределения материальных и информационных ресурсов предприятия;
- информационные модели внутреннего и внешнего документооборота (диаграммы потоков данных);
- форматы и процедуры обработки запросов пользователей для решения задач управления;
- информационно-логические модели баз данных;
- модели актуализации данных и обеспечения информационной безопасности;
- соглашения и интерфейсы по обмену данными и взаимодействию смежных информационных систем;
- базовые модели деятельности подразделений и служб обеспечения безопасности и регламенты работ пользователей;
- расчетно-аналитические модели для решения прикладных задач обработки данных о состоянии объектов безопасности в целевых и обеспечивающих АС предприятия;
- модели управления проектами;
- модели оценки деятельности организаций и должностных лиц.

Применение базовых функциональных профилей АС предприятий позволяет обеспечивать единство методологических подходов к управлению процессами обеспечения безопасности, соблюдение общих регламентов, а также возможности использования функций, которые ранее не могли быть выполнены без применения функций интеллектуальной обработки данных.

Прежде всего, это функции прогноза и обоснования принятия рациональных или оптимальных решений на основе применения модельных описаний объектов угроз безопасности и сценариев

мероприятий по их обнаружению и принятию мер по ликвидации потенциального ущерба. При этом важно, обеспечение достоверности данных, их согласованности, а также методов статистической оценки текущего уровня состояния объектов безопасности и зрелости процессов служб обеспечения безопасности на предприятии.

Важно отметить, что средства безопасности должны применяться в каждой целевой АС предприятия в соответствии с их назначением, функциями, важностью для предприятия и допустимым уровнем риска нарушения целостности. В таблице приведены экспертные оценки целесообразности разработки «услуг безопасности» для основных процессов предприятия и соответствующих им целевых АС. Наивысший приоритет целесообразности – 5.

В составе функционально-полных автоматизированных систем предприятия выделяются:

- структурные подсистемы, соответствующие основным организационным структурам предприятия;
- функциональные подсистемы, соответствующие функциям управления, принятым в базовой модели деятельности предприятия;
- программно-методические комплексы (ПМК) для реализации прикладных задач управления текущими процессами и инновационными проектами предприятий;
- программно-технические комплексы (ПТК) в составе среды функционирования АС предприятия;
- функциональные модули реализации прикладных задач обработки данных и управления;
- информационные модули ведения баз данных о состоянии портфеля проектов, баз знаний о методах, правилах применения терминов, инструментальных средствах, функциональных зависимостях и др. характеристик объектов управления.

Опыт показывает наличие серьезных проблем в использовании различных стандартов на процедуры управления инновационными проектами предприятий. Требуется согласование понятий, применяемых в международных и национальных стандартах разного уровня. Для упорядочения понятийного аппарата в конкретных профилях ИС инфраструктурных организаций должны предусматриваться средства, обеспечивающие построение и использование семантических моделей проектирования различных АС предприятия, онтологий описания

предметной области их деятельности, унификации и стандартизации терминов и связей между ними в рамках конкретных проектов.

Следует отметить актуальность работ по созданию профилей прикладных информационных систем наукоемких предприятий в связи с развитием Систем электронного взаимодействия предприятий и инфраструктуры поддержки инноваций при реализации национальных проектов, систем электронного правительства и других социально значимых проектов [5, 6].

Таблица 5.1 – Оценки значимости применения типовых функций ядра ИСОКБП относительно объектов контроля безопасности основных процессов (целевых автоматизированные систем) предприятия

Типовые функциональные модули ИСОКБП	**Управление предприятием**	**Техническая подготовка производства**	**Управление инфраструктурой**	**Управление ресурсами**	**Управление производством**	**Оценка показателей деятельности**	**Управление качеством продукции**	**Управление инф. ресурсами**	**Оценка значимости функции**
Ввод данных об объектах	5	5	3	3	4	4	5	5	34
Оценка сложности объектов и угроз безопасности	5	5	4	4	3	3	5	5	34
Планирование	4	4	4	4	3	3	3	4	29
Проектирование процессов обеспечения безопасности	3	4	3	4	3	3	5	5	30
Моделирование (оценка эффективности мер)	4	5	3	3	4	4	3	4	30
Контроль сроков, результатов, ресурсов	3	3	5	4	5	4	4	4	32
Статистика и анализ зрелости	4	4	3	5	4	4	5	4	33
Документирование и коммуникации	4	5	5	4	3	5	4	4	34
Значимость объекта	32	35	30	31	29	30	34	35	

6 Архитектура интегрированной системы обеспечения комплексной безопасности предприятия

Организационное, методическое, техническое и программное обеспечение процессов управления комплексной безопасностью предприятия строится с применением комплексов типовых проектных решений в области видеонаблюдения, охранной и пожарной сигнализации, контроля и управления технологическими процессами предприятий, информационно-коммуникационных технологий управления распределенными объектами предприятия, средств связи и передачи данных в локальных, корпоративных и глобальных сетях ЭВМ общего и специального назначения.

В основу архитектуры интегрированной системы обеспечения комплексной безопасности положены рассмотренные выше принципы с выделением в АС программно-технических комплексов (ПТК) и программно-методические комплексов (ПМК).

ПТК, как правило, предназначены для решения задач, связанных с автоматическим управлением техническими объектами, и характеризуются довольно жесткой структурой технического и программного обеспечения и алгоритмами функционирования. В любом ПТК основа – «железо», которым управляют специализированные программные средства.

ПМК решают организационно-управленческие задачи обеспечения деятельности и координации работ различных служб предприятия, – в них довольно велик вес слабоформализуемых процедур и они более подвержены человеческому фактору при принятии решений на разных уровнях управления.

Программные средства ПМК в своей основе должны ориентироваться и реализовывать принятые на предприятии методики и модели управления процессами, основными элементами которых являются люди, а также решать задачи поддержки и технического обслуживания базовых ПТК. (В любом ПМК основа – «Прикладные программы», а «железо» выбирается исходя из функций этих программ).

Необходимые связи и обмены данными межу ПМК и ПТК реализуются посредством использования базовых профилей среды реализации и служб информационных систем предприятия, унифицированных интерфейсов, баз данных общего и специального назначения. С учетом рассмотренного в разделе базового профиля прикладных

АС предприятий, а также этих замечаний и сформирована базовая архитектура ИСОКБП.

В состав базовой архитектуры ИСОКБП включаются компоненты, приведенные в таблице 6.1. Следует иметь в виду, что конкретный состав компонент может уточняться, детализироваться и масштабироваться в общесистемном и частных проектах обеспечения безопасности предприятия применительно к условиям предприятия, характеристикам наследуемых информационных систем, составу целевых и обеспечивающих АС, потенциальному составу угроз и риску в деятельности предприятия и подразделений, а также предпочтений ЛПР и наличия необходимых ресурсов для комплектации и эксплуатации выбранных средств безопасности.

При этом рекомендуется готовить именно проекты ИСОКБП с необходимым обоснованием и подготовкой системной и эксплуатационной документации организационного, методического, программного и технического обеспечения, а не отдельные технические решения на закупку приглянувшихся и широко разрекламированных средств обеспечения безопасности.

В состав базового комплекса интегрированной системы обеспечения комплексной безопасности предприятия входят программно-технические комплексы:

- ПТК-1 «Видеонаблюдение, пожарная сигнализация, и локальные системы управления техникой безопасности (видеокамеры камеры, средства доступа, сигнализация и др.)»;
- ПТК-2 «Проектирование конфигурации, инсталляция и настройка ядра ИСОКБП на условия предприятия»;
- ПТК-3 «Видеоконференцсвязь предприятия»;
- ПТК-4 «Связь и обслуживание электронных коммуникаций (доступ в ИСОКБП с КПК, сотовых телефонов и др.)»;
- ПТК-5 «Организация и обслуживание баз данных информационных ресурсов предприятия в корпоративных и глобальных сетях (Интранет, Интернет, сайт, портал предприятия)»;
- ПТК-6 «Ведение геоинформационных баз данных общего и специального назначения и организация хранилищ данных мониторинга территориально-распределенных объектов предприятия».

Для обеспечения эффективности использования средств ИСОКБП в условиях конкретных предприятий, их интеграции с целе-

выми АС предприятий и внешними контрагентами планируется развитие модульных структур базовых ПТК, типизации отдельных модулей, обеспечении интерфейсов с оборудованием ИСОКБП, поставляемым различными другими производителями. Для решения вопросов интеграции планируется проектирование, разработка, постановка на производство и организация поставок потребителям следующих программно-методических комплексов:

- ПМК-1 «Комплекс средств информационных технологий управления деятельностью служб безопасности предприятия»;
- ПМК-2 «Идентификация и анализ объектов угроз и рисков обеспечения деятельности предприятия»;
- ПМК-3 «Обеспечение безопасности формирования и управления информационными ресурсами предприятия»;
- ПМК-4 «Мониторинг состояния и обеспечение надежности и безопасности эксплуатации целевых автоматизированных систем предприятия (АСУ технологическими процессами, энергоустановками, транспортными системами, спецтехники и др.)»;
- ПМК-5 «Мониторинг состояния территориально распределенных объектов предприятия», включая средства:
  - интегральной обработки событий и фактов (ведение журнала инцидентов-угроз безопасности, закрепленных за объектами повышенной опасности вне их ведомственной принадлежности);
  - поиска связанных (корреляции) объектов и субъектов угроз безопасности (адресный сигнализатор);
  - оценки рисков и последствий инцидентов угроз безопасности;
  - принятия оперативных решений и планирования мероприятий и действий;
- ПМК-6 «Оперативное взаимодействие ИСОКБП предприятия с клиентами и внешними пользователями», включая организационные и электронные регламенты, соглашения о взаимодействии, стандарты и форматы обмена данными и программные средства поддержки и обеспечения:
  - патрулирования и охраны объектов;
  - инспекции и профилактики оборудования ИСОКБП на объектах;
  - информационного обеспечения оперативных мероприятий;
  - ведения архивов данных, истории инцидентов угроз безопасности и принятых решений, статистики и отчетности.

На рисунке 6.1 приведена структура базового профиля интегрированной системы обеспечения комплексной безопасности предприятия.

Таблица 6.1 – Компоненты ИСОКБП

Вид и наименование компоненты ИСОКБП	**Основной «Владелец» и другие пользователи**	**Рекомендуемые места размещения**	**Приоритет реализации (условно)**
Программно-технические комплексы			
ПТК-1 Видеонаблюдение, пожарная сигнализация, и локальные системы управления техникой безопасности (видеокамеры камеры, средства доступа, сигнализация и др.)	Служба безопасности Подразделения инфраструктуры предприятия	Периметр предприятия, зданий и сооружений. Пожароопасные объекты; Помещения спецподразделений	Высокий
ПТК-2 Проектирование конфигурации, инсталляция и настройка ядра ИСОКБП на условия предприятия	Информационная служба Служба безопасности Аккредитованная консультационная фирма-разработчик ИСОКБП	Информационная служба Служба безопасности	Низкий; Средний – для предприятий, большим количеством модификаций ИСОКБП
ПТК-3 Видеоконференцсвязь предприятия	Информационная служба Руководство структурных подразделений Служба безопасности Организаторы общих совещаний и PR-акций	Помещения для совещаний и переговоров, в том числе на других удаленных площадках предприятия	Средний
ПТК-4 Мониторинг состояния автоматизированных систем предприятия (САПР, АСУТП, энергоустановками, транспортными системами, медтехники и др.)	Служба автоматизации и технического обслуживания АС предприятия Операторы АС	Помещения службы Рабочие станции АС на объектах контроля	Средний для отдельных процессов – высокий
ПТК-5 Связь и обслуживание электронных ком-	Служба связи Служба безопасности	Серверы предприятия с уста-	Средний Высокий –

Вид и наименование компоненты ИСОКБП	Основной «Владелец» и другие пользователи	Рекомендуемые места размещения	Приоритет реализации (условно)
муникаций (доступ в ИСОКБП с применением КПК, ноутбуков, сотовых телефонов и др.)	Информационная служба Персонал предприятия с необходимым уровнем доступа	новленными на них межсетевыми экранами	при большом количестве удаленных пользователей
ПТК-6 Организация баз данных (хранилищ) информационных ресурсов предприятия и их обслуживания в корпоративных и глобальных сетях	Информационная служба, Администраторы баз данных Служба безопасности Службы-владельцы информационных ресурсов (по закрепленным направлениям)	Серверы информационной службы предприятия	Высокий
ПТК-7 Геоинформационная база данных территориально-распределенных объектов предприятия	Служба безопасности Спецподразделения	Центр мониторинга безопасности (ситуационная комната)	Средний
Программно-методические комплексы			
ПМК-1 Комплекс средств информационных технологий управления деятельностью служб безопасности предприятия	Служба безопасности	Подразделения службы	Высокая
ПМК-2 Идентификация и анализ объектов угроз и оценка рисков обеспечения деятельности предприятия	Рабочая группа (совет) по обеспечению безопасности предприятия Аналитики и эксперты службы обеспечения безопасности (по закрепленным направлениям)	Рабочие станции (персональные ЭВМ аналитиков), Ситуационная комната	Высокий
ПМК-3 Формирование и управление информационными ресурсами и интеллектуальной собственностью предприятия	Информационная служба; Подразделения-владельцы информационных ресурсов; Служба безопасности	Хранилища распределенных ресурсов предприятия	Средний

Вид и наименование компоненты ИСОКБП	Основной «Владелец» и другие пользователи	Рекомендуемые места размещения	Приоритет реализации (условно)
ПМК-4 Организация и ведение базы данных объектов и субъектов безопасности	Служба безопасности; Информационная служба; Совет (рабочая группа) безопасности предприятия	Сервер службы безопасности	Средний Для особо опасных процессов – высокий
Мониторинг состояния территориально распределенных объектов предприятия			
ПМК-5 Интегральная обработка событий и фактов (Ведение журналов инцидентов-угроз безопасности, закрепленных за объектами повышенной опасности предприятия вне их принадлежности к отдельным структурным подразделениям)	Служба безопасности; Информационная служба; Рабочая группа (совет) по обеспечению безопасности предприятия; Аналитики и эксперты службы обеспечения безопасности (по закрепленным направлениям)	Рабочие станции	Высокий
ПМК-6 Поиск связанных (коррелированных) событий по объектам и субъектам угроз безопасности			Средний
ПМК-7 Оперативная оценка рисков и последствий инцидентов угроз безопасности с формированием адресных рекомендаций для оперативного реагирования и принятия мер	Служба безопасности Ситуационный центр безопасности предприятия		Высокий
ПМК-8 Подготовка и принятие оперативных решений (планирование мероприятий, действий и необходимых ресурсов)	Ситуационный центр		Средний
ПМК-9 Оперативное взаимодействие ИСОКБП с контрагентами и внешними пользователями, включая организационные и электронные регламенты, соглашения о взаимодействии, стандарты и форматы обмена данными и программные средства обеспечения:			

Вид и наименование компоненты ИСОКБП	Основной «Владелец» и другие пользователи	Рекомендуемые места размещения	Приоритет реализации (условно)
Патрулирование и охрана объектов	Служба безопасности; Служба охраны предприятия; Закрепленные подразделения МЧС, МВД		Низкий
Инспекции и профилактики оборудования ИСОКБП на объектах	Служба безопасности Служба технического обслуживания средств безопасности Аккредитованные фирмы – поставщики средств безопасности		Высокий
Информационное обеспечение мероприятий обеспечения безопасности	Служба безопасности Служба охраны предприятия Закрепленные подразделения МЧС, МВД, Медслужба		Средний
Ведение архивов данных, истории инцидентов угроз безопасности, принятых решений, статистики и отчетности.	Информационная служба		Средний
Другие			
ПМК-10. Автоматизированный учебный курс «Интегрированные системы обеспечения комплексной безопасности предприятия» отдельные (модификации для служб обеспечения безопасности и персонала предприятия)	Служба безопасности Подразделения предприятия Разработчики базовых средств безопасности	Служба безопасности ИТ Служба управления персоналом Библиотека Портал (Сайт) предприятия	Высокий
Комплект инструктивно-методических материалов по составу и применению средств ИСОКБП на предприятии	Совет (рабочая группа) безопасности предприятия	Библиотека с ограниченным доступом	Высокий

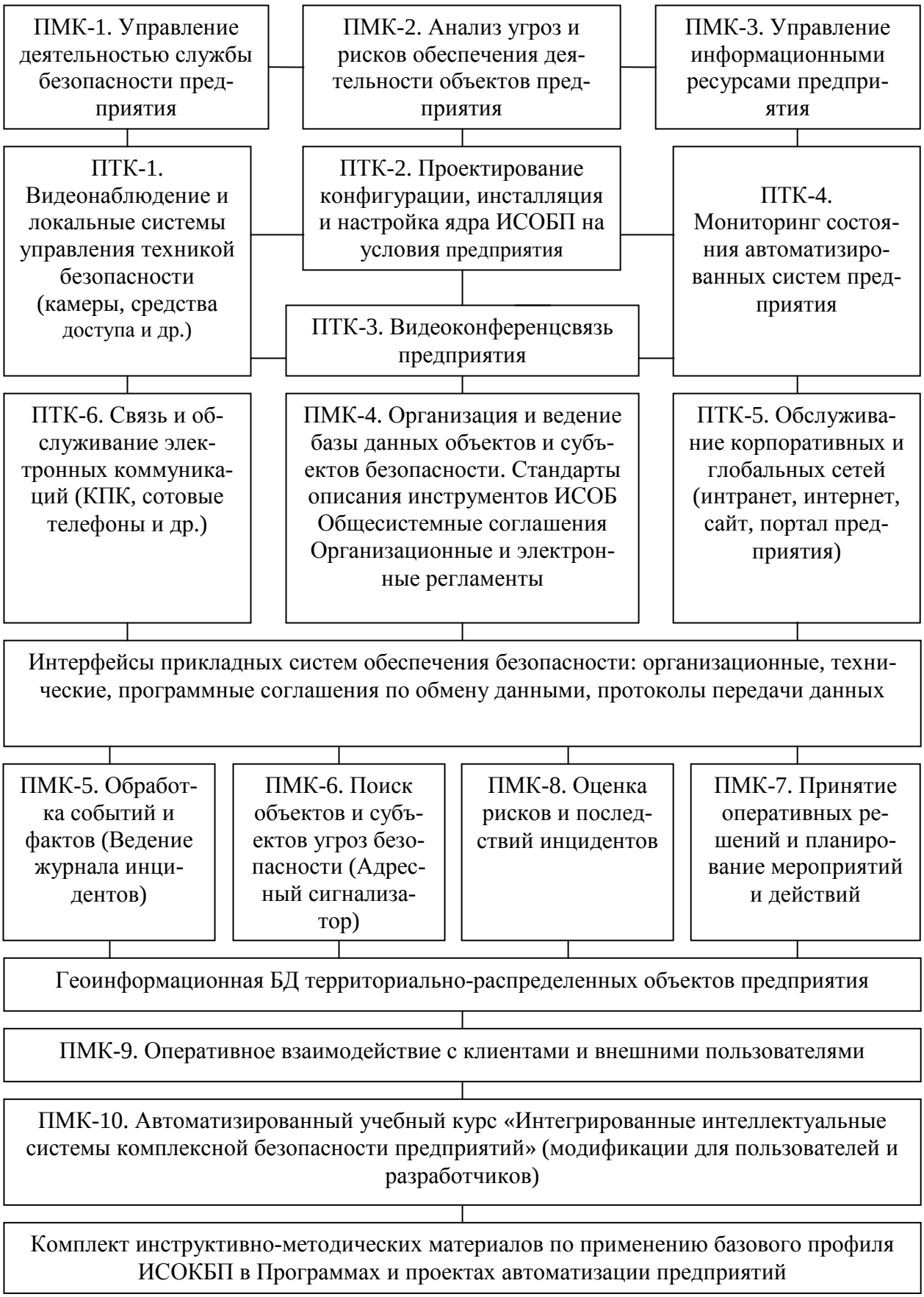

Рис. 6.1. Обобщенная функциональная структура интегрированной системы обеспечения безопасности предприятия

7 Средства обеспечения безопасности предприятий и проблемы их типизации, унификации и интеграции

7.1 Описание проблемы

Одним из наиболее эффективных способов «вхождения в новый этап автоматизации» является приобретение проектных и технических решений фирм, занимающих серьезные позиции в производстве технического и программного обеспечения систем автоматизации. Естественно, что подобные процессы чрезвычайно сложны с точки зрения управления проектами, порождают большое число проблем в части организации бизнеса, технологий, кадров, управленческого учета и т.п.

В рамках этих процессов существует главенствующий субъект (руководство и ведущие специалисты предприятия), который может формулировать и диктовать свои условия о том, каким решениям следует руководствоваться в ходе адаптации новых продуктов, процессов, персонала, отчетности по работе в рамках единой стратегии.

Целесообразным решением в данной ситуации является анализ стандартов разного уровня и изучение имеющихся “лучших практик” родственных предприятий, выбор приемлемых решений, которые наиболее соответствует бизнес-стратегии и ИТ-стратегии предприятия. В настоящее время одним из наиболее приемлемых подходов является анализ (аудит) наследуемых ОТС предприятий на основе международного стандарта Cobit 4.0.

При подготовке решений о применении в ИСОКБП новых информационных технологий и средств автоматизации предприятия необходимо учитывать следующие, указанные ниже факторы.

7.2 Оценка возможности использования стандартных процедур описания процессов обеспечения безопасности в подразделениях

Для управления процессом стадии выбора процедур и инструментальных средств описания процессов предприятия необходимо произвести оценку того, насколько предприятие и его подразделения и партнеры мотивированны и готовы к участию в совместных работах, фактического наличия необходимых ресурсов и степени их соответствия стандартам, применяемым для управления текущей деятельностью и инновационными проектами предприятий.

Во избежание неэффективного изучения ситуации в подразделениях, естественно сопровождающегося пассивным, а иногда и активным сопротивлением персонала, желающего максимально приукрасить ситуацию, а также скрыть недостатки и недоработки разработчиков, поставщиков комплектующих и материалов, оборудования и программного обеспечения, желающих подчеркнуть достоинства именно своих продуктов и их эффективности и т.п., в ходе анализа необходимо руководствоваться максимально формализованными, легитимными, стандартными методиками, документами, алгоритмами оценки технических предложений.

На начальной стадии создания ИСОКБП необходимо сформировать единые или реорганизовать имеющиеся на предприятии органы управления проектами обеспечения безопасности предприятия (комитет, рабочая группа и т.п.). Основной задачей органов управления проектами является анализ формализованных методик оценки, используемых в проектах обеспечения безопасности предприятия, выбор наиболее соответствующего по качеству и трудоемкости использования и формирование пакета стандартов, на основе которого будут приниматься решения, в частности – выбираться профиль средств обеспечения безопасности.

Необходимым в данном процессе является создание специализированных рабочих групп специалистов по отдельным направлениям обеспечения безопасности. Объектами деятельности Рабочих групп являются проекты эксплуатации целевых АС предприятия на основе принятых стандартов, в рамках которых осуществляются конкретные мероприятия по обеспечению безопасности, определяются и контролируются цели, сроки и ресурсы, выделяемые для каждого из направлений. Именно такой подход должен найти отражение в разрабатываемых предприятиями целевых и обеспечивающих АС предприятия, внутренних и корпоративных стандартах (желательно гармонизированных с необходимыми национальными и международными стандартами описания продукции, ресурсов и услуг предприятия).

7.3 Определение единого реестра средств обеспечения безопасности с учетом продуктов и услуг предприятия

Основным критерием эффективности принимаемых решений в области обеспечения комплексной безопасности предприятия является соответствие их существующей стратегии и вытекающим из нее целям и задачам. Для решения этих задач потребуются соответст-

вующие технологии, процессы, организационные и аппаратно-программные решения.

Стратегия содержит в себе количественную и качественную оценку планируемых на краткосрочную и долгосрочную перспективу показателей безопасности предприятия, его продукции, технологий, работ и услуг, а также определение зон их влияния на общие ключевые показатели деятельности предприятия. Необходимо уточнить, насколько имеющиеся в наличии средства безопасности и ИТ продукты пересекаются или дополняют друг друга. Необходимо достаточно-подробное описание характеристик средств обеспечения безопасности, т.к. за формально одинаковыми названиями продуктов, их внешними потребительскими функциями скрыты различные процессы их настройки и операции обслуживания, различающиеся по трудоемкости и эффективности в конкретных условиях.

В связи с этим необходимо констатировать, что необходимым стандартом должно являться наличие на предприятии единого Реестра средств безопасности и ИТ-продуктов, рекомендованных для применения на предприятии. Наличие единого реестра процессов и средств безопасности позволяет обеспечить должный учет и порядок, оптимизировать использование ресурсов предприятия, оперативно фиксировать состояние безопасности деятельности подразделений, уровень зрелости процессов на определенный момент и сравнить их качественное состояние для принятия решений в зависимости от уровня развития текущих и/или прогнозируемых опасных ситуаций.

Особое внимание составлению реестров должно уделяться в подразделениях обеспечения безопасности и ИТ-службе предприятия, которые являются структурой, обладающей наиболее полной и точной информацией о процессах, узких местах и проблемных точках развития предприятия и обладают определенными полномочиями оптимизации и распределения ИТ-ресурсов для повышения эффективности деятельности предприятия в целом.

7.4 Описание процессов функционирования подразделений с позиций обеспечения безопасности

В рамках Рабочих групп по безопасности необходимо обеспечить анализ процессов подразделений и определить перечни угроз безопасности. В этом процессе чрезвычайно эффективно могут применяться стандартизованные документы, описывающие текущую деятельность и перспективы развития подразделений:

- организационная структура с описанием базовых процедур принятия решений по типовым инцидентам угроз безопасности и взаимодействия с внешними подразделениями субподразделений (управлений, отделов, секторов) в процессе выполнения функциональных обязанностей;
- план развития подразделений с количественной и качественной оценкой показателей состояния безопасности и их соответствия общей концепции безопасности и политике безопасности (в том числе ориентированность на внутренние ресурсы или аутсорсинг);
- паспорт безопасности подразделения предприятия, который дает полную картину состояния системы обеспечения безопасности объектов, в том числе критически важных, и определяет ряд конкретных мероприятий по усилению защищенности объектов;
- методика оценки рисков деятельности подразделения с количественными оценками их влияния на ключевые показатели деятельности (например, производительность, объемы выполняемых работ услуг, качество, вероятностные оценки срывов работ, нарушений регламентов, обороты и неоперационные расходы на сотрудника, динамика долей в штатном расписании и стоимости бюджетов в подразделениях и службах сопровождения, соглашения и режим взаимодействия со смежными подразделениями, соисполнителями проектов и другими контрагентами).

Паспорт безопасности может включать следующие основные разделы: общие сведения, сведения о персонале, анализ и моделирование возможных кризисных ситуаций, мероприятия по обеспечению безопасности функционирования объекта (в том числе технические) по годам (обычно на 5 лет), силы и средства охраны, ситуационные планы и схемы, характеристики систем жизнеобеспечения, организация взаимодействия с органами обеспечения безопасности (ФСБ, МВД и МЧС), а также с аварийными службами, выводы и рекомендации.

Паспорт безопасности определяет минимально необходимый и финансово обоснованный набор инженерно-технических средств и информационных систем обеспечения безопасности объекта, что позволит с наибольшей вероятностью и эффективностью решить проблему защиты объекта от всего спектра реализации возможных угроз исходя из критерия «эффективность – стоимость».

7.5 Унификация регламентов, порядков, введение нормативно-справочной информации и информационных ресурсов предприятия

Еще одной зоной внимания участников рабочей группы по безопасности процессов предприятия является упорядочивание и унификация нормативно-справочной документации, используемой в различных подразделениях предприятия. Опыт показал, что эта область деятельности является наиболее «продвинутой». Практически любое предприятие имеет свою собственную систему инструкций, регламентов, порядков, процедур и т.п. В этой части необходимо определить общие требования к документам, их форматы, шаблоны, представления и т.п. Хорошим выходом в такой ситуации является использование стандартов в области делопроизводства и документооборота. Чем более внутренние стандарты компаний соответствуют принятым отраслевым, национальным и международным стандартам, тем безболезненнее происходит процесс формирования единых подходов к решению проблем безопасности.

Отдельной задачей является оценка документооборота предприятия с позиций обеспечения безопасности, как внешнего – с клиентами, так и внутреннего – между подразделениями и сотрудниками (приказы, распоряжения, протоколы, описания технических решений, конструкторско-технологическая документация и др.). В силу ряда причин в этих документах могут присутствовать т.н. «вирусы в текстах», которые могут содержать угрозы безопасности того или иного типа.

При этом в силу своей компетентности/некомпетентности отдельные исполнители часто могут и не подозревать о наличии такого вируса в подготавливаемом ими документе. В этой связи службой безопасности предприятия должны быть инициированы действия по определению контролируемых объектов в текстах конструкторско-технологической документации, являющихся предметом коммерческой тайны предприятия, объектами защиты интеллектуальной собственности, НОУ-ХАУ и т.п.

За основу модели контроля текстов можно принять существующие перечни сведений, подлежащих защите, а также модель, рекомендованную ГОСТ РВ 51987-2002 «Информационная технология, Комплекс стандартов на АС. Требования и показатели качества функционирования информационных систем». В этом стандарте предусмотрены специальные процедуры и методы контроля документа-

ции с использованием контролеров – специалистов по предметам деятельности или специализированных программных средств интеллектуальной обработки данных, включая экспертные системы согласования отношений между понятиями, контроль целостности и непротиворечивости данных, контроль вкладок, недозволенных текстовых вложений и др.

В связи с высоким развитием аппаратно-программного обеспечения электронного документооборота в подразделениях, большими капиталовложениями, уже произведенными в эту область, достаточно высоким уровнем профессиональной подготовки и специализацией персонала, задача унификации средств информационной безопасности с одновременным сокращением издержек и сохранением инвестиций в основные процессы предприятия чрезвычайно усложняется. В каждом случае ее нужно решать отдельно, с учетом конкретной специфики. Какие-либо универсальные подходы пока предложить в этой сфере затруднительно.

Основная проблема – стандартизация уникальных для конкретных процессов и объектов справочников при объединении множества автоматизированных систем, частью которых они являются. Эти локальные проблемы должны решаться в ходе выполнения проектов интеграции автоматизированных систем. В этом ряду особняком стоит проблема объединения справочников клиентов, являющаяся фундаментальной на нынешнем клиентоориентированном этапе развития предприятий машиностроительного комплекса

Без решения этой проблемы невозможна «сквозная автоматизация процессов», создание полноценных безопасных систем взаимоотношений с клиентами. В качестве стандартов в этой области на перспективу, с определенными ограничениями можно рассматривать требования Комитетов ИСО / МЭК по промышленным стандартам. В качестве примера можно привести стандарт Ростехнологий «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

7.6 Оценка совместимости ИТ платформ в подразделениях предприятия и его контрагентах

Важнейшим резервом повышения эффективности использования разных вариантов аппаратно-программного и организационного обеспечения, объектов управления и снижения издержек, является

стандартизация ИТ-платформ, использующихся в подразделениях предприятия, в том числе и службой обеспечения безопасности. Задача осложняется, если помимо аппаратно-программных решений, используемых на предприятии, существует развитая сеть территориально разнесенных подразделений.

Даже в процессе обычного функционирования предприятия, без учета процессов интеграции средств обеспечения безопасности, стандартизация аппаратно-программных решений в этой части позволяет резко снизить издержки на поддержку и сопровождение путем централизации службы поддержки, уменьшить количество персонала, добиться скидок от поставщиков «железа» на основе тиражируемости решения, обеспечения возможности централизованно проводить тестирование и обновление версий ПО, что резко снижает требования к квалификации специалистов на местах.

Расчет общей стоимости владения целевых АС предприятия и соответственно АС обеспечения деятельности службы безопасности, позволяет объективно сравнить используемые решения и выбрать наиболее эффективное. Более того, эта методология позволяет также косвенно оценить эффективность организационного обеспечения решаемых задач, т.к. в показатели стоимости владения входят не только затраты на комплектацию, но и затраты подразделений на поддержку и сопровождение сравниваемых комплексов, учитываемые в системах управленческого учета предприятий. Конечно, для этого на предприятии должна существовать какая-либо система управленческого учета, качественно организованный процесс планирования, бюджетирования и распределения ресурсов деятельности подразделений.

7.7 Унификация стандартов на оборудование рабочих мест служб обеспечения безопасности

Следующим этапом формирования профиля безопасности предприятия должны стать проведение анализа и утверждение стандартов предприятия на оборудование рабочих мест, включающее в себя стандарты на модели и характеристики компьютеров, программное обеспечение (редакторы, электронные таблицы, браузеры, нормативно-справочные БД и т.п.). Оборудование и программные средства обеспечения безопасности должны быть сертифицированы на соответствие нормам и правилам безопасности Федеральной службы по технической эксплуатации и контролю (ФСТЭК).

Разработка стандарта предприятия, регламентирующего порядок применения различных средств безопасности на предприятии, как одного из элементов профиля безопасности предприятия, особенно важна в связи с ускоренным процессом амортизации такого оборудования. Эффективность резко возрастает при унификации оборудования рабочих мест, на которых используются дорогостоящие средства САПР- Конструкций и САПР- Технологий, АС измерений и испытательных стендов. Своевременная замена техники позволят добиться снижения удельной стоимости на объемах поставок технического и программного обеспечения, на уменьшении трудоемкости инсталляции ПО и подключения к сетевым ресурсам, удаленном администрировании и сопровождении пользователей.

Сложнее добиться унификации используемых СУБД и серверного оборудования, которые имеют гораздо большие сроки использования, требуют высококвалифицированных администраторов, регламентных процедур. Тем не менее, и в этой области есть возможность создать стандарт предприятия и следовать ему при принятии решений о развитии информационных технологий и реализации проектов обеспечения безопасности.

Важно отметить, что стремление к поголовной унификации технического и программного обеспечения для средних и крупных предприятий машиностроения, имеющих множество различных информационных систем, опыт их эксплуатации и сложившиеся традиции взаимодействия с контрагентами (особенно с вышестоящими организациями) затруднено: многочисленные попытки создания единой гетерогенной ИТ-среды предприятий не увенчались успехом – естественный выход – применение технологи открытых систем (открытость, не есть вседоступность).

Одним из перспективных направлений развития технологий открытых систем и архитектуры среды реализации прикладных АС предприятия является постепенный по мере морального и технического износа эксплуатируемых в подразделениях средств АИС переход на технологии «тонкого клиента» для рабочих мест исполнителей и достаточно мощных серверов для хранения баз данных общего и специального назначения, работающих в локальных и глобальных сетях ЭВМ и обеспечивающих современный уровень «виртуализации» – способности работать в различных операционных системах и поддерживающих работу программ, написанных на различных языках проектирования и программирования.

Особая роль при решении задач обеспечения безопасности отводится средствам развития коммуникаций. По данным исследования, проведенного журналом CIO Magazine, 30% компаний по всему миру уже полностью внедрили, а 46% - частично внедрили системы IP-телефонии. В 74% случаев в стратегию внедрения IP-телефонии пытались включить планы, которые могли бы быть связаны с технологиями унифицированных коммуникаций. Между тем, термин «унифицированные коммуникации» пока еще часто толкуется поразному. Аналитики Gartner Research в 2007 году обозначили его как некую совокупность оборудования, программных средств и сервисов, способных повысить продуктивность сотрудников и групп сотрудников в масштабах целых организаций, так как одновременно упрощается управление и контроль за этим процессом путем использования нескольких корпоративных методик.

Принципиальной особенностью унифицированных коммуникаций является конвергенция различных каналов, сетей, сервисов и бизнес-приложений, причем не ограничиваясь лишь телекоммуникационной составляющей, а выходя на прикладной уровень. Речь идет о встраиваемости функций коммуникации в различные корпоративные бизнес-процессы и соответствующие им целевые и обеспечивающие АС предприятия.

А когда объединяются сети и системы, то унифицируется и управление ими, а это соответственно открывает новые возможности в мониторинге состояния безопасности процессов предприятия. Исследования показывают, что отечественные пользователи оказываются готовы к внедрению абсолютно любых телекоммуникационных инноваций, причем гораздо более восприимчивы к подобным переменам, чем многие их зарубежные коллеги.

На языке информационных технологий преимущества от внедрения унифицированных коммуникаций достигаются за счет лучшей координации различных телекоммуникационных каналов, интеграции коммуникационных функций с целевыми прикладными АС и повышения отказоустойчивости средств связи.

В результате применения унифицированных коммуникаций повышается производительность труда, ускоряются процессы, и сокращается цикл производства благодаря росту продуктивности сотрудников, улучшения обслуживания клиентов и так далее. Но в тоже время эксперты Gartner вынуждены констатировать, что сейчас нет оснований признать технологии унифицированных коммуникаций

зрелыми. Для этого есть ряд препятствий, в частности, недостаточная просвещенность пользователей и недостаточный набор лучших практик.

В результате непродуманных решений, без учета сложившейся на предприятии инфраструктуры, инвестиции, которые уже были сделаны, подвергаются риску, (например, частичного обесценивания). Процесс тормозит и сложность оценки инвестиций в унифицированные коммуникации.

По мнению ряда экспертов, задача осложняется и отсутствием стандартов. Если в вопросах электронной почты, IP-телефонии или видеоконференцсвязи имеются общепринятые стандарты и протоколы, то когда речь идет о едином комплексе, в котором собраны решения разных компаний, их совместимость оказывается неполной.

В результате 61% респондентов, опрошенных CIO Magazine, считают решения в области унифицированных коммуникаций дорогими. Кроме того, по их мнению, возникают проблемы с защитой данных, не очевидна их надежность, а также необходимо учитывать ряд инфраструктурных ограничений, в том числе отсутствие мотивации, сопротивление персонала изменением и др. Тем не менее, 19% опрошенных считают, что технологии унифицированных коммуникаций на подъеме. Еще 21% считает, что потенциал данных технологий очевиден, однако они недостаточно зрелые. А вот 12% полагают, что эти технологии просто не зрелые и начнут в скором времени вытесняться решениями следующего поколения. На фоне таких полярных мнений аналитики Gartner Research делают вывод, что к 2010 году 80% компаний придут к практическому использованию унифицированных коммуникаций.

7.8 Организация взаимодействия службы безопасности, ИТ и других подразделений

Модели взаимодействия подразделений определяются значимостью продукции и услуг предприятия для общества, потребителей и государства, принятой на предприятии сквозной технологией разработки, постановки на производство, изготовления, реализации и технического сопровождения продукции и услуг. В зависимости от этого и выбирается приемлемая модель обеспечения комплексной безопасности предприятия, которая должна соответственно отражать модель деятельности предприятия, его структурных подразделений и соот-

ветствует модели деятельности. Роль технологических подразделений, аутсорсинга, проектного подхода.

В задачах обеспечения комплексной безопасности особая роль должна отводиться повышению эффективности деятельности ИТ подразделения предприятия, от его места в информационно-технологическом обеспечении процесса достижения стратегических целей развития предприятия и обеспечения безопасности информационных систем. Диапазон этой роли может простираться от стандартных функций поддержки функционирования аппаратно-программного обеспечения, локальных сетей до реализации бизнес-задач, в основе которых лежат ИТ- решения, без которых принципиально невозможен процесс производства наукоемкой продукции. Существует несколько параметров, по которым можно определить модель функционирования ИТ подразделения и его взаимодействия со службой безопасности и другими основными подразделениями предприятия:

- отношение к разработкам технического и прикладного программного обеспечения: своими силами, закупка на стороне или передача этих работ на аутсорсинг;
- отношение к наличию технологических (аналитических) функций в службах обеспечения безопасности, подразделениях и роль ИТ-службы в проектах обеспечения безопасности;
- отношение к использованию методов управления проектами предприятия.

На сегодняшний день существуют примеры успешных разработок и внедрений как «самодельного» программного обеспечения, так и продуктов внешних разработчиков, примеры эффективности разработанных технологических решений для предприятий специалистами ИТ и участия «продвинутых» бизнес-заказчиков в ИТ проектах.

Поэтому невозможно дать однозначный ответ на выбор стандарта управления ИТ- проектами для конкретного предприятия без проведения соответствующего анализа. В зависимости от стратегии возможен любой из полярных вариантов или их комбинация. Опыт однозначно показывает лишь, что такая модель должна обязательно существовать, должна быть оформлена и утверждена в документах, четко описывающих ИТ- стратегию предприятия, концепции и политику обеспечения безопасности в рамках каждой целевой АС предприятия и обобщенную модель стратегии обеспечения комплексной безопасности предприятия в целом. Решения по безопасности долж-

ны быть отражены в организационных и электронных регламентах (должностных инструкциях, описаниях процессов, схемах и таблицах) основных подразделений, проектно-конструкторских службах, ИТ-службах с учетом их взаимодействия с другими подразделениями.

Отсутствие материальных свидетельств наличия такой модели неоспоримо свидетельствует об отсутствии самой модели, какие бы правильные слова не произносились в обоснование правильности той или иной неформально существующей концепции функционирования ИТ предприятия. Детализация различных сторон функционирования модели, ее апробацию в реальном процессе, документированность и обоснованность являются решающими факторами выбора направлений работ в этой области.

7.8 Совершенствование процессов планирования и ресурсообеспечения проектов обеспечения безопасности предприятия

Последней по порядку, но не по важности идет проблема обеспечения стандартизации процессов планирования и обеспечения ресурсами. На этот процесс влияют практически все проблемы, присущие другим областям деятельности, для которых жизненно важна стандартизация – проблемы многопрофильности основных подразделений, их географического расположения и различной корпоративной культуры, несовпадение и бизнес-процессов и Реестров продуктов и услуг, различие ИТ-платформ и моделей функционирования целевых АС предприятия.

Следовательно, стандартизация планирования и своевременная оценка потребности в ресурсах на обеспечение безопасности оценка должна быть неотъемлемой частью работ по созданию ИСОКБП и на каждом этапе завершать этап.

Процессы рациональной организации и управления проектами автоматизации предприятий промышленного сектора затрагивают множество областей и объектов их деятельности, среди которых одной из важнейших является информационно-технологическая инфраструктура и принципы управления ею. Сложности и проблемы, возникающие в оценке необходимых и достаточных ресурсов для обеспечения безопасности текущих мероприятий и инновационных проектов, подходы к их решению, методики управления ими, представляют интерес для руководителей промышленных предприятий, переживающих непростые процессы поглощения и объединения и реше-

ние которых принципиально невозможно без учета множества факторов обеспечения безопасности и поиска мер по снижению рисков в деятельности любого предприятия.

Как и в других областях человеческой деятельности, здесь могут быть использованы общие подходы, стандарты, унифицированные решения, рекомендации опробованные на реальных объектах и процессах. В концепции обеспечения безопасности и проектах оснащения служб и подразделений средствами безопасности достойным образом должны быть представлены доступные и действенные методики анализа и моделирования процессов обеспечения безопасности в подразделениях для обоснованного выбора технических и программных средств ИСОБКП и минимизации общей стоимости владения этим средствами.

Зачастую справиться с этими задачами специалистам предприятий не удается по многим причинам (загруженность основной деятельностью, недостаток знаний и опыта, отсутствие данных о современном состоянии средств безопасности и ИТ индустрии и др.). И в этой связи перспективным направлением является привлечение к этим работам независимых экспертов и специалистов в той или иной сфере деятельности и обеспечения того или иного вида безопасности, а том числе передача отдельных работ и услуг на аутсорсинг внешним организациям, например традиционный и давно апробированный вид аутсорсинга – вневедомственная охрана. В современных условиях спектр услуг аутсорсинга существенно расширяется – антивирусная защита, техническое обслуживание средств ИКТ, видеонаблюдения, экспертиза проектов и др.

Структура комплекса безопасности включает

- периферийное оборудование (контроллеры, считыватели, охранные извещатели, видеокамеры, электромагнитные замки, турникеты, картоприемники, и т.п.);
- серверное оборудование подсистем охранной и пожарной сигнализации, видеонаблюдения, контроля доступа (на базе персональных компьютеров);
- удаленные рабочие места интегрированного комплекса безопасности и отдельных подсистем (охранная и пожарная сигнализация, видеонаблюдение, контроль доступа);
- локальная сеть системы безопасности (оптоволокно), активное и пассивное сетевое оборудование.

Вопрос о типизации проектных решений и определении рационального состава модулей любых автоматизированных систем, и в частности, интегрированных интеллектуальных систем обеспечения безопасности предприятий является центральным вопросом организации должного взаимодействия заказчиков, разработчиков, поставщиков компонент и пользователей. К сожалению, до настоящего времени, несмотря на наличие многих теоретических и достаточно обоснованных работ по анализу и синтезу АС на основе типовых решении, в ИТ сообществе не сложилось единого понимания, что такое «Типовое решение» и, что такое «Модуль АС». Разные разработчики и поставщики базовых компонент АС по-разному трактуют эти понятия. На наш взгляд модули могут выделяться на разных уровнях описания процессов.

Основные принципы организации интегрированной системы безопасности включают обмен данными и взаимодействие подсистем безопасности через модуль интеграции, распределенную архитектуру, визуализацию объекта посредством трехмерных планов с указанием расположения периферийного оборудования, обеспечение режима видеоконференции для общения должностных лиц, выдачу рекомендаций операторам системы безопасности по действиям в сложившейся обстановке и др.

Весьма острым и часто дискуссионным вопросом является отношение лиц принимающих решения на предприятии к применению типовых и индивидуальных решений к проектированию, комплектации и «закупкам» автоматизированных систем. Использовать готовое программное обеспечение или разрабатывать свое?

Каждый из подходов имеет свои преимущества и недостатки. предприятие должно определить, что ей больше подходит, готовые массовые ИТ и средства обеспечения их безопасности или специализированные, созданные под конкретные задачи предприятия. Чем можно поступиться, сроками и стоимостью или уникальностью и неповторимостью. В ИТ вполне жизнеспособна и комбинация этих подходов.

О некоторых предпочтениях ряда предприятий говорят результаты исследований по стандартизации, унификации разработок и использования типовых и индивидуальных проектных решений в проектах автоматизированных систем предприятий [17]. Обобщение результатов этих работ, а также неформальные опросы и анкетирование ряда ведущих специалистов и лиц, принимающих решения, на пред-

приятиях по вопросам применения АС и использования средств ИКТ показывает, что предприятия предпочитают при создании АС ориентироваться на целевые установки, представленные ниже, а в качестве комплексных критериев оценки проектных решений по техническому и особенно прикладному программному обеспечению использовать соответствующие критерии.

Предпочтения предприятий по использованию типовых проектных решений в целевых АС предприятий в порядке их значимости для большинства респондентов включают

1. Создание полной и адекватной картины функционирования объектов автоматизации предприятия;
2. Увеличение гибкости и адаптивности, возможности изменять модели процессов предприятия;
3. Снижение остроты проблемы нехватки квалифицированного персонала для обслуживания процессов предприятия;
4. Сохранение или приобретение контрагентов и клиентов, улучшение работы с клиентами (предоставление улучшенных услуг клиентам - внутренним и внешним пользователям АС);
5. Построение управленческой вертикали, а также горизонтальных взаимосвязей между подразделениями;
6. Снижение себестоимости продукции и услуг, обеспечение контроля затрат ресурсов;
7. Расширение производства, создание новых продуктов и услуг (том числе «сервисов безопасности» для служб предприятия) с применением новых или модифицированных АС;
8. Повышение капитализации компании.

Критерии выбора программного обеспечения АС предприятий (в порядке предпочтения большинства респондентов) включают:

1. Функциональная полнота прикладного программного обеспечения АС;
2. Архитектура: многоплатформенность, интеграция с существующим на предприятии программным обеспечением и инфраструктурой ИКТ;
3. Стоимость эксплуатации и качество поддержки (полная стоимость владения на всем жизненном цикле АС);
4. Длительность и простота внедрения;
5. Вертикальный опыт работы разработчика/поставщика и учет специфики отрасли (сферы основной деятельности предприятия);

6. Существующие отношения/прошлый опыт работы с разработчиком/ поставщиком;
7. Удобство и простота в использовании системы;
8. Цена поставки компонент технического и программного обеспечения АС.

Интересно также, отметить, что на вопрос о том, в каких сферах деятельности предприятия планируется создание АС, более 30 % предприятий среди прочих традиционных сфер применения АС, указали такие направления как «обеспечение комплексной безопасности предприятия и «обеспечение информационно безопасности».

Анализ реальных потребностей служб управления в системах обеспечения комплексной безопасности предприятий показывает возрастание роли унификации и стандартизации элементов информационных технологий и обеспечения их стандартами на конструкцию, технологий проектирования, эксплуатации и сопровождение.

В то же время опыт показывает наличие серьезных проблем в использовании различных стандартов на изделия и процедуры управления реальными проектами создания систем управления безопасностью предприятий. Требуется согласование понятий, применяемых в международных и национальных стандартах разного уровня.

Для упорядочения понятийного аппарата в ИСОКБП должны предусматриваться средства, обеспечивающие построение и использование семантических моделей базовых моделей автоматизированных систем, описания предметной области деятельности, унификации и стандартизации терминов и связей между ними в рамках конкретных проектов.

Эффективность процессов обеспечения безопасности деятельности предприятия в значительной мере определяется организационно-технологическим уровнем совместных работ служб обеспечения безопасности предприятия, служб информационных технологий, охраны, а также качеством средств и систем обеспечения безопасности, уровнем обоснованности и полнотой задания всего комплекса работ по обеспечению безопасности предприятий, своевременности подготовки объектов и оперативного персонала к внедрению.

В этой связи особое внимание должно уделяться подготовке и переподготовке специалистов в области проектирования средств и систем обеспечения безопасности, а также специалистов – конечных пользователей ИТ в части применения доступных методов формали-

зованных описаний продуктов, процессов и ресурсов конкретных организационно-технических систем.

Требования индивидуализации проектов обеспечения комплексной безопасности предприятия будут стимулировать развитие следующих сценариев подготовки и выбора проектных решений. Предприятие с привлечением независимых консультантов и экспертов выполняет анализ стратегии развития предприятия, уточняет архитектуру предприятия, разрабатывает концепцию обеспечения безопасности и применения необходимых организационных, методических, технических и программных средств обеспечения безопасности,, проводит анализ наследуемых ИС, типовых проектных решений разного уровня и формирует наборы системных спецификаций - требований к компонентам АИС обеспечения безопасности, которые рассылаются потенциальным внутренним и внешним исполнителям проекта и поставщикам средств.

Далее проводится тендер по отдельным проектным направлениям. Победители тендера и включаются в рабочую группу реализации системного проекта. Общее управление и координацию работ по проекту осуществляет служба безопасности предприятия как владелец и основной пользователь основного проекта. ИТ-служба предприятия обеспечивает подготовку общих соглашений по использованию базовых средств информационных технологий предприятия.

Рабочая группа в соответствии с компетенциями своих членов готовит индивидуальный системный проект АИС обеспечения безопасности предприятия, при этом используются общие для проекта соглашения по использованию проектных решений в соответствии с принятыми критериями оценки качества компонент АС.

По результатам общесистемного проекта предприятие может также проводиться второй тендер на поставку необходимого оборудования и разработку отдельных компонентов технического и программного обеспечения по согласованным спецификациям базового профиля прикладных целевых и обеспечивающих АС предприятия, гармонизированного с национальными и отраслевыми профилями.

8 Методы и средства разработки интегрированной информационной среды обеспечения комплексной безопасности предприятия

Реализация основных положений концепции проекта создания ИСОКБП в силу естественной сложности организации взаимодействия и согласования интересов участников требует применения специальных технологий организации общесистемного проекта и отдельных субпроектов обеспечения безопасности в подразделениях.

Совершенствование технологий проектирования ИСОКБП затрагивает вопросы взаимодействия многих лиц с разными взглядами, целевыми установками и мнениями относительно реальных объектов и событий в деятельности современных предприятий со сложной структурой управления. Центральной проблемой является определение реальной сложности объектов, необходимость согласования процедур принятия решений на основе отбора наиболее информативных параметров и достоверных данных об объектах деятельности в реальных социально-экономических условиях. В этой связи важно в составе технологий иметь средства, обеспечивающие:

- идентификацию инцидентов угроз безопасности, регистрацию событий и измерение факторов риска в деятельности предприятия и его процессов;
- ранжирование (упорядочение) инцидентов-угроз безопасности, событий и факторов риска по степени их влияния на ключевые целевые показатели развития предприятия;
- сегментацию (разделение области значений фактора на сегменты по подразделениям и территориям, основным и обеспечивающим процессам деятельности для проведения дальнейшего, более детального, анализа) и принятия решений на соответствующем уровне управления;
- профилирование угроз безопасности и выделения «наилучших» достижений для перспективного планирования мероприятий по обеспечению безопасности деятельности;
- выявление ассоциаций (поиск факторов появляющихся вместе);
- выявление исключений (поиск элементов, выпадающих из общей картины, нештатных ситуаций, необычных ситуаций, несогласованных мнений экспертов и т.п.);
- оценку сложности объектов контроля и процессов обеспечения их безопасности (поиск групп значений факторов, определяющих

комплексный показатель для принятия решений по распределению ограниченных ресурсов на реализацию мероприятий по безопасности с учетом технико-экономического потенциала объектов и их влияния на общие показатели деятельности;

- прогнозирование последствий и оценку потребностей в ресурсах для обеспечения безопасности и ликвидации последствий нарушений угроз безопасности.

В соответствии с предлагаемой системной моделью архитектуры предприятия и основными стадиями жизненного цикла сложных ОТС, а также общими методологическими основами построения профилей прикладных АС предприятий в основу построения комплекса средств обеспечения безопасности предприятием могут быть положены следующие обобщенные процедуры:

- диагностический анализ состояния безопасности и упорядочение целевых показателей деятельности подразделений, классификация процессов и определение организационных структур обеспечения безопасности предприятия и его основных процессов;
- построение схем материальных и информационных потоков между подразделениями предприятия и упорядочение документооборота служб обеспечения безопасности предприятия;
- описание объектов контроля безопасности и субъектов системы обеспечения безопасности и выделение системоообразующего ядра архитектуры интегрированной системы обеспечения комплексной безопасности предприятия (ИСОБКП), состава и требований к базовым программно-техническим (ПТК) и программно-методическим комплексам (ПМК) средств обеспечения безопасности предприятия и сбалансированных показателей оценки их состояния, уровня безопасности и зрелости процессов;
- построение модели управления процессами обеспечения безопасности предприятия, исходя из необходимости определения «сервисов безопасности» для основных целевых и обеспечивающих АС предприятия, определение их взаимосвязей между собой и внешним окружением;
- определение рациональных организационных структур службы обеспечения безопасности предприятия, распределение функций, обязанностей и ответственности исполнителей;

– формирование организационно-технических мероприятий и прикладных технических задач в проектах обеспечения безопасности основных процессов предприятия;
– выявление внутренних и внешних факторов, инцидентов угроз безопасности и построение моделей оценки их влияния на показатели деятельности и риски.
– оценка и прогноз статистических характеристик потоков данных об инцидентах угроз безопасности предприятия;
– построение математических моделей оценки рисков в деятельности предприятия, выбор алгоритмов обработки данных и логики принятия решений в ситуациях обнаружения угроз безопасности в подсистемах;
– разработка расчетных моделей влияния угроз безопасности текущей деятельности и инновационных проектов предприятия на состояние и основные показатели деятельности;
– разработка моделей принятия и согласования решений в различных информационных ситуациях и способов их реализации в условиях предприятия;
– оценка эффективности мероприятий по обеспечению безопасности, оценка потребностей в ресурсах и их распределение между ведущими подразделениями – владельцами отдельных целевых АС предприятия и внешними контрагентами;
– подготовка организационной структуры распределенной структуры служб обеспечения безопасности предприятия;
– разработка проектов технического и программного обеспечения комплексов средств обеспечения безопасности;
– управление проектами обеспечения безопасности предприятий, принятие решений о применении средств обеспечении безопасности в подразделениях, оценка потребностей в ресурсах, контроль сроков выполнения работ, результативности и качества услуг – сервисов обеспечения безопасности для основных процессов предприятия.

Эти процедуры служат основой для разработки системного проекта ИСОКБП, системной и эксплуатационной документации проектов целевых и обеспечивающих систем. Состав документации проектов предприятия может уточняться и детализироваться в зависимости от сложности объектов, состояния разработки и внедрения компонентов проекта по различным видам обеспечения

деятельности (организационное, методическое, нормативно-правовое, техническое, программное и др.).

В проектах также рассматриваются вопросы выбора программно-аппаратных средств и информационной среды реализации проектов: типы ЭВМ, операционных систем, СУБД, базовых инструментальных средств и прототипов прикладных программ в зависимости от конкретных организационно-технических условий, состояния наследуемых информационных систем и потенциала объекта управления, организационные, технические и программные интерфейсы по обмену данными, соглашения по форматам и регламенту взаимодействия со смежными системами и внешним миром, которые выбираются в соответствии с функциональными профилями международных стандартов ISO и МЭК

В проектах обеспечения безопасности предприятий уточняются, актуализируются и прогнозируются на предполагаемый срок жизни проекта, как минимум на 3 – 5 лет:

- геополитические роли предприятия и сферы его влияния на экономику региона;
- структура потребностей в товарах и услугах;
- структура и расчетный уровень потребления ресурсов;
- демографическая ситуация региона и состояние подготовки персонала;
- собственные и привлекаемые интеллектуальные ресурсы;
- состояние средств информационного, технического и программного обеспечения целевых АС предприятия;
- состояние материально-технической базы и товарных запасов;
- структура программных мероприятий и спецификации требований к результатам работ по видам обеспечения;
- состояние финансов и источники инвестиций для реализации ИТ-проектов предприятия

Для решения задачи построения системы обеспечения безопасности в проектах должны быть предусмотрены:

- организационно-методические материалы по экспертизе технических предложений и проектных решений, методам испытаний и приемки компонент и др. материалы, необходимые для организации и координации работ по реализации отдельных мероприятий;
- нормативные документы для разработчиков, пользователей и служб эксплуатации средств безопасности по унификации структур различных видов обеспечения проектов, протоколов связи, со-

глашений по использованию общих информационных и коммуникационных ресурсов;
- типовые организационно-технические мероприятия по подготовке объектов и базовые программы подготовки персонала;
- специальные методики тестирования, моделирования и оценки качества функционирования отдельных наиболее ответственных компонентов систем;
- рекомендации по методам обеспечения эксплуатационной надежности комплексных систем сопровождения наиболее ответственных проектов меж регионального и федерального уровня (в том числе при работе в составе корпоративных и глобальных сетей ЭВМ).

В настоящее время вопросам создания интегрированной информационной среды предприятия, включающей методическое, алгоритмическое информационное техническое и программное обеспечение информационных систем предприятия уделяется особое внимание. [25]. Сложность задачи создания интегрированной информационной среды заключается в необходимости использования большого количества разнообразных автоматизированных систем, предоставляющих разную функциональность.

Разнородность применяемых технических и программных средств, протоколов и форматов обмена данными приводит к возникновению гетерогенной среды, требующей интеграционной основы, обеспечивающей переносимость приложений, взаимодействие систем и их функциональное расширение.

Одним из наиболее эффективных подходов, позволяющих построить интегрированную информационную среду предприятия, является системная интеграция информационных ресурсов. Общетеоретическим обоснованием системной интеграции является концепция открытых систем, достаточно давно известная и хорошо себя показавшая при автоматизации крупных предприятий [8].

Под открытой системой будем понимать систему, реализующую открытые спецификации или стандарты для интерфейсов, служб и форматов, с тем, чтобы облегчить должным образом созданному прикладному программному средству перенос с минимальными изменениями в широком диапазоне систем, полученных от одного или нескольких поставщиков; взаимодействие с другими приложениями, расположенными на местных или удаленных системах; взаимодейст-

вие с людьми в стиле, облегчающем переносимость пользователя. (ИСО/МЭК 14252).

В соответствии с определением комитета IEEE POSIX 1003.0 [50] открытая система есть система, реализующая открытые спецификации на интерфейсы, сервисы и поддерживаемые форматы данных, достаточные для того, чтобы обеспечить должным образом разработанным приложениям возможность переноса с минимальными изменениями на широкий диапазон систем, совместной работы с другими приложениями на локальной и удаленных системах и взаимодействия с пользователями в стиле, облегчающем тем переход от системы к системе.

Ключевой момент в этом определении – использование термина «открытая спецификация», что в свою очередь определяется как общедоступная спецификация, которая поддерживается открытым, гласным согласительным процессом, направленным на постоянную адаптацию новой технологии, и соответствует стандартам.

По данному определению открытая спецификация несильно зависит от технологии, т.е. от специфического аппаратного и программного обеспечения или от продуктов конкретного производителя. Она одинаково доступна любой заинтересованной стороне. Более того, открытая спецификация находится под контролем общественности и поэтому все, кого она затрагивает, могут участвовать в ее разработке.

Основополагающим документом, в котором изложены основные принципы открытых систем, является ISO/IEC TR 14252-1995. Согласно этому документу основной принцип открытых систем состоит в создании среды, включающей программные и аппаратные средства, службы связи, интерфейсы, форматы данных и протоколы, которая в своей основе имеет развивающиеся, доступные и общепризнанные стандарты и обеспечивает переносимость, взаимодействие и масштабируемость приложений и данных. Второй принцип предполагает использование методов функциональной стандартизации: построение и применение профиля – согласованного набора базовых стандартов, необходимых для решения конкретной задачи или класса задач.

Использование концепции открытых систем позволяет провести проектирование бизнес-процессов предприятия, и при этом избежать излишней привязанности к текущим особенностям производства. Бизнес-процессы рассматриваются не как источник знаний о предприятии, а как источник информационных потоков в открытой сис-

теме. При этом высокая адаптивная способность открытой системы позволяет существенно упростить переход между существующим и новым решениями.

Использование технологий открытых систем с одной стороны обеспечивает необходимую гибкость в конструировании интегрированной информационной среды и позволяют выполнить требования по производительности и надежности системы, но с другой стороны могут привести к нарушению безопасности предприятия. Однако применение открытых спецификаций не относится непосредственно к данным, которые могут и в необходимых случаях иметь соответствующие средства защиты от несанкционированного доступа.

При этом в первую очередь следует говорить о нарушении информационной безопасности, в виде появления новых каналов утечки информации, подлежащей защите. Вместе с тем при условии активного использования единого информационного пространства предприятия в качестве источника знаний, необходимых для управления комплексной безопасностью предприятия, возникают новые требования к методам создания интегрированной информационной среды.

Несмотря на сложность поставленной задачи и большое разнообразие видов деятельности предприятий, на которых используются открытые системы при построении интегрированной информационной среды, в целом, требования по обеспечению безопасности выдвигаются достаточно схожие. Действительно, требования по организации работы с информацией, подлежащей защите, а также набор знаний, необходимых для управления безопасностью предприятия, для многих промышленных предприятий одинаковы, и скорее определяются объемом производства, нежели его спецификой.

Конечно, для машиностроительных предприятий, выполняющих государственные заказы и оперирующих информацией, представляющей собой особую важность, следует обеспечить и особый режим ее защиты, а, следовательно, и предъявлять к интегрированной информационной среде специфические требования. Однако, список требований к интегрированной информационной среде, не должен сильно отличаться от списка требований, предъявляемых для других предприятий, отличием будет лишь важность удовлетворения этих требований.

Таким образом, актуальной является задача создание унифицированной архитектуры интегрированной информационной среды

предприятия, в которую необходимо включить средства обеспечения безопасности.

Для решения этой задачи выделим типовые процессы предприятия, определенные стандартом ISO/IEC 15288:2002 Systems engineering – System life cycle processes. Эти обобщенные процессы включают задачи управления проектами (планирование, оценку, контроль, принятие решений, управление рисками и управление конфигурацией и информационное управление) и управление процессами (управление средой предприятия, инвестициями, процессами жизненного цикла, ресурсами и качеством), а также управление процессами согласования и техническими процессами.

Отметим, что управление процессами содержит также и управление средой предприятий, что включает в себя конфигурирование интегрированной информационной среды.

Требования к интегрированной информационной среде предприятия можно разделить на две категории. Во-первых, это необходимость обеспечения безопасности подлежащих защите данных, используемых в различных подразделениях предприятия, занимающихся как поддержкой основных процессов жизненного цикла изделия, так и вспомогательной деятельностью.

Во-вторых, это потребность в расширении интегрированной информационной среды путем включения программного и технического обеспечения, необходимого для управления безопасностью и информационного обеспечения, используемого при анализе рисков.

Таким образом, функции по обеспечению безопасности предприятия должны быть распределены между подразделениями- владельцами основных процессов предприятия, специализированными службами автоматизации и информационных систем предприятия и координироваться службой обеспечения безопасности, выполняемая подразделениями безопасности, связана с функциями по настройке и поддержке функционирования интегрированной информационной среды, выполняемыми подразделением информационных технологий.

Эта взаимосвязь на стадии формирования требований к интегрированной системе обеспечения безопасности приведена на рис. 8.1. На этом рисунке показаны основные направления сотрудничества подразделений предприятия: обеспечение защиты информации и функционирование технических средств, хранение данных, необходимых для управления рисками и обеспечение финансовой безопасности.

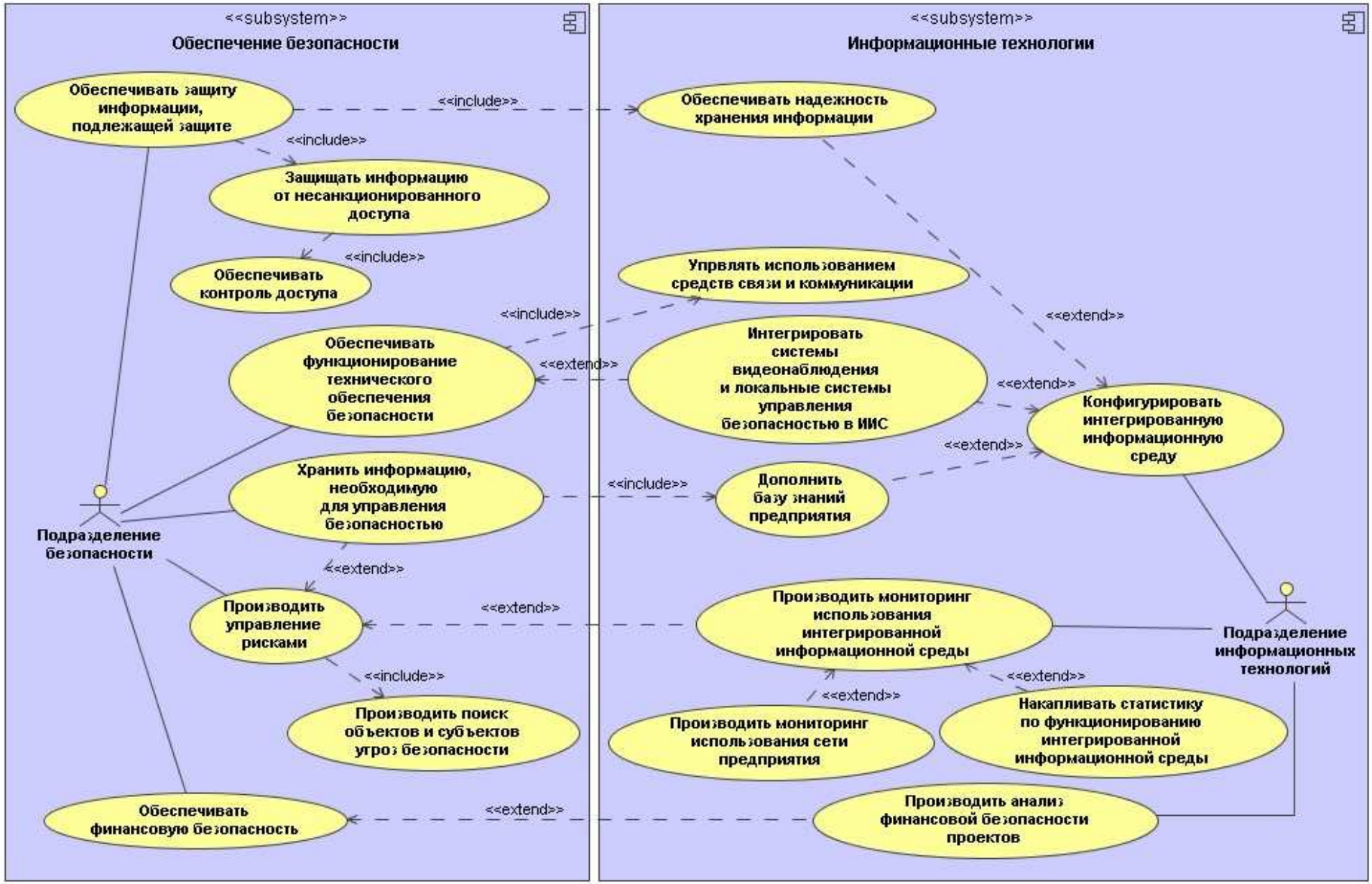

Рис. 8.1. Основные требования к системе безопасности

Основные задачи подразделений службы безопасности предприятия связаны с функциями по настройке и поддержке функционирования интегрированной информационной среды, выполняемыми подразделением информационных технологий.

Согласно современным стандартам [28 – 30], процессы установления, оценки и контроля уровня целостности системы включают определение, анализ и контроль рисков, в том числе расчет рисков и оценка ущерба и обоснование приемлемых (допустимых) рисков.

Отметим, что в последовательности указанных процессов устанавливается обратная связь, которая позволяет на основе анализа возникающих на этапе контроля рисков угроз сформировать необходимость корректирующих воздействий на этапе определения рисков.

Исходя из приведенных выше рассуждений, основные функции системы обеспечения безопасности в составе интегрированной информационной среды предприятия можно выделить в отдельную подсистему, которая структурно представляет собой набор взаимосвязанных программно-технических и программно-методических комплексов.

Эти комплексы вместе образуют базовый профиль интегрированной системы обеспечения комплексной безопасности предприятия (ИСОКБП).

Принятие стандарта ГОСТ Р ИСО/МЭК 15408 создало новые условия для совершенствования процессов обеспечения безопасности информационных технологий в России. Несмотря на то, что стандарт, прежде всего, нацелен на обеспечение безопасности ИТ, и называется «Критерии оценки безопасности информационных технологий», сфера его применения гораздо шире и охватывает все этапы жизненного изделия.

Одной из наиболее важных его сторон является возможность задания требований к безопасности ИТ, адекватных их особенностям и условиям их применения. Это позволяет повысить эффективность защитных механизмов и минимизировать затраты на обеспечение безопасности изделий, необходимые для достижения требуемого уровня их защищенности.

Обоснованность требований безопасности к процессам предприятия и обеспечивающим их ИТ достигается детальным учетом существующих и потенциальных угроз безопасности и правил политики безопасности предприятия. Это заставляет заказчиков и разработчиков изделия ИТ на этапе формирования требований проводить все-

сторонний анализ возможных рисков нарушения безопасности и вырабатывать те меры безопасности, которые обеспечивали бы снижение этих рисков до приемлемого уровня.

Для представления требований безопасности в общих критериях (ОК), как известно, предусмотрено две конструкции: профиль защиты (ПЗ) и задание по безопасности (ЗБ). Они образуют два крайних полюса представления требований безопасности. Профиль защиты предназначен для наиболее общего описания типовых требований безопасности для определенного класса продуктов и систем информационных технологий.

Задание по безопасности содержит описание требований безопасности, которые реализованы в конкретном продукте или системе ИТ, а также краткую спецификацию, которая предназначена для описания того, каким образом требования безопасности реализованы в продукте или системе ИТ.

Если провести сопоставление с используемыми в настоящее время формами представления требований безопасности, то профили защиты в определенном смысле соответствуют классам защищенности действующих РД Гостехкомиссии России, а задания по безопасности – техническим условиям. Однако эта аналогия касается только места этих документов в структуре нормативной базы, а не их сути.

Представление требований безопасности основывается, прежде всего, на детальном описании всех особенностей и условий применения продукции.

Требования безопасности для наукоемкой продукции включают как требования к функциям, которыми оно должны обладать, так и требования к мерам обеспечения безопасности, которые должны приниматься при разработке, испытаниях, поставке и сопровождении изделия, так называемые требования доверия к безопасности.

Опыт работы ЦБИ [17] по адаптации значительного количества зарубежных ПЗ и разработки ПЗ и ЗБ в интересах Гостехкомиссии, МПС и Минобороны России свидетельствует о том, что для качественной разработки ПЗ и ЗБ необходимо не только глубокое знание самих Общих критериев, а также освоение специфической технологии выполнения этих работ.

В первую очередь это относится к описанию продуктов или систем ИТ и среды их безопасности. При описании продукции наиболее важно правильно структурировать и описать активы, которые подлежат защите. Это описание должно быть представлено в таком форма-

те, который позволял бы в дальнейшем использовать описание активов при выборе требований безопасности.

Описание среды безопасности должно содержать такие аспекты, как угрозы безопасности, политика безопасности предприятия и предположения об условиях применения продуктов и систем ИТ.

Для описания моделей угроз безопасности разработана базовая модель угроз безопасности, которая содержит совокупность классификационных схем, на основе которых формируется модель процесса реализации угрозы, начиная от ее источника и кончая возможными последствиями нарушения безопасности активов ИТ.

Наиболее сложным моментом является определение целей безопасности изделий ИТ. Их выбор осуществляется на основе проведения анализа риска нарушения информационной безопасности с учетом определенных в описании среды безопасности угроз, политик и предположений и имеющихся финансовых и временных ограничений по созданию и оценке безопасности изделий ИТ.

Формируемые требования безопасности должны в полной мере обеспечивать достижение установленных целей безопасности. При этом необходимо учитывать, что как одна цель может достигаться различными требованиями безопасности, так и одно требование безопасности может использоваться для достижений различных целей безопасности. Кроме того, должны быть также учтены зависимости, которые существуют между различными требованиями безопасности.

Из краткого обзора технологии разработки ПЗ и ЗБ видно, что для их качественной разработки необходимо наличие комплекса методического и инструментального обеспечения. В ЦБИ это методическое и инструментальное обеспечение объединено в «Инструментальный комплекс автоматизации разработки ПЗ и ЗБ «ИКАР». Использование разработанного методического и инструментального обеспечения позволяет не только повысить качество разработки ПЗ и ЗБ, но сократить время и затраты на их разработку, что является немаловажным для заказчиков.

Помимо ПЗ и ЗБ, которые, как уже говорилось, являются двумя крайними полюсами представления требований безопасности, существуют и другие промежуточные формы их представления. В частности, при задании разработки продукта или системы ИТ требования безопасности включаются в техническое задание на разработку, содержание которого определено соответствующими ГОСТами, в част-

ности ГОСТами 34-й серии при разработке автоматизированных систем. При переходе к заданию требований безопасности на основе ГОСТ Р ИСО/МЭК 15408 уже недостаточно указать при разработке АС, что она должна соответствовать, например, классу 2А по РД Гостехкомиссии на АС и, тем самым, определить все необходимые требования безопасности, которым она должна удовлетворять. Требования безопасности должны быть заданы либо на основе существующих профилей защиты, либо сформированы в полном объеме, если необходимые ПЗ отсутствуют.

ОК не регламентируют представление требований безопасности в других видах документов кроме ПЗ и ЗБ. Вместе с тем в целях наиболее точного отображения требований безопасности на различных стадиях создания продуктов и систем ИТ их целесообразно представлять в структуре определенной для профиля защиты.

Опыт разработки требований безопасности показывает также, что хорошего результата можно достичь только при тесном взаимодействии заказчика и разработчика требований безопасности. Особенно важен хороший контакт при разработке требований безопасности для систем ИТ и, прежде всего, на этапе описания системы ИТ и среды ее безопасности. За то время, которое отводится разработчику ПЗ, как правило, достаточно трудно овладеть необходимым объемом знаний в отношении системы ИТ. Поэтому разработчик требований безопасности должен иметь отработанную методику проведения анализа системы ИТ и среды ее безопасности, а заказчик должен быть готов предоставить все необходимые для такого анализа данные.

В самом ГОСТе Р ИСО/МЭК 15408 содержатся только требования к структуре, содержанию материалов ПЗ и ЗБ и критерии их оценки. Организационные и процедурные аспекты разработки, оценки и регистрации ПЗ и ЗБ ГОСТом не регламентированы. Для этих целей на этапе апробации ГОСТа по заданию Гостехкомиссии России

В ЦБИ был разработан комплекс необходимых руководящих и методических документов, который включает:

- Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности;
- Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты;
- Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты;

– Руководство по разработке профилей защиты и заданий по безопасности.

Положение по разработке ПЗ и ЗБ определяет порядок разработки, оценки, регистрации и публикации ПЗ и ЗБ для продуктов и систем информационных технологий, предназначенных для обработки информации, отнесенной к информации ограниченного доступа в соответствии с законодательством Российской Федерации.

В Положении изложены:

– общие положения по назначению, содержанию и организации разработки профилей защиты и заданий по безопасности;
– порядок разработки, оценки, сертификации, регистрации и публикации профилей защиты;
– порядок разработки и оценки заданий по безопасности.

Отдельно в Положении определен порядок разработки ПЗ, регламентирующих минимальные обязательные требования для продуктов и систем ИТ, предназначенных для обработки информации ограниченного доступа.

Руководство по формированию семейств профилей защиты устанавливает порядок формирования семейств ПЗ, предназначенных для группирования и классификации профилей защиты одного типа изделий. В Руководстве изложены:

- назначение, состав и структура семейств профилей защиты;
- состав классов защищенности изделий информационных технологий и соответствующих им базовых пакетов требований доверия и уровней стойкости функций безопасности;
- порядок разработки профилей защиты на основе семейств профилей защиты.

Руководство по разработке ПЗ и ЗБ представляет собой методический документ по разработке профилей защиты и заданий по безопасности. В Руководстве изложены:

– общие положения и рекомендации по представлению материалов разделов профилей защиты и заданий по безопасности;
– рекомендации по представлению материалов профилей защиты и заданий по безопасности для составных изделий ИТ и изделий ИТ, входящих в состав других изделий ИТ;
– рекомендации по формированию функциональных пакетов требований и пакетов требований доверия к безопасности изделий ИТ.

Можно сделать следующие общие выводы.

1. Использование ГОСТ Р ИСО/МЭК 15408 позволяет обеспечить задание требований к безопасности продуктов и систем ИТ, адекватных их особенностям и условиям применения.
2. В настоящее время разработаны необходимые нормативные и методические документы, регламентирующие процедуры разработки, оценки, регистрации и публикации ПЗ и ЗБ.
3. Разработка требований безопасности на основе ГОСТ Р ИСО/МЭК 15408 требует глубокого знания его положений и наличия развитого методического и инструментального обеспечения. Для качественной разработки ПЗ и ЗБ целесообразно привлечение организаций, специализирующихся в этой области деятельности.

9 Функциональная структура базового программно-методического комплекса службы обеспечения безопасности предприятия

В соответствии с принятой методологией разработки профилей прикладных автоматизированных систем, опытом разработки отдельных комплексов средств ИТ предприятий, современными подходами и тенденциями интеграции целевых и обеспечивающих автоматизированных систем [21] и основными функциональными требованиями к архитектуре и базовым программно-техническим и программно методическим комплексам интегрированных систем обеспечения комплексной безопасности предприятий сформирована функциональная структура ядра базового ПМК службы обеспечения безопасности предприятия.

Ядро этого комплекса построено с применением классификатора объектов автоматизации, классификатора функций и библиотеки типовых проектных решений, методических и инструментальных средств проектирования профилей прикладных автоматизированных систем. При разработке ядра учитывались работы в области стандартизации технических и программных средств информационных технологий, состояние рынка средств безопасности, а также мнения ведущих специалистов информационных служб, служб обеспечения безопасности и конечных пользователей ключевых целевых АС ряда предприятий машиностроения относительно целесообразности и возможностей использования в реальных проектах типовых проектных решений, предлагаемых ведущими организациями разработчиками и поставщиками средств ИКТ.

В таблице 9.2 описаны основные задачи базового ПМК службы обеспечения безопасности предприятия.

Следует отметить, что предлагаемая функциональная структура профиля прикладных АС может применяться практически во всех целевых и обеспечивающих АС предприятия, а также при реализации базовых ПТК и ПМК обобщенной архитектуры ИСОКБП. При этом в зависимости от характеристик объектов управления (процессов предприятия) может изменяться, в основном, только конкретное содержание, реализуемых в отдельных модулях методов, а сама структура (архитектура) является достаточно устойчивой и обладает свойствами функциональной полноты с позиций общей теории управления.

Таблица 9.1 – Состав основных задач обработки данных базового ПМК «Обеспечение деятельности подразделения безопасности предприятия»

№ п/п	Имя типовой функции модуля	Объект (аргумент)	Примечание
1	Ввод данных: от датчиков: видеосигнал (изображение); аналоговый сигнал; аудиосигнал; дискретный сигнал; кодовый сигнал; от оперативного персонала; от лиц принимающих решения по объектам; от подразделений и служб инфраструктуры предприятия	Термины и понятия ИСОКБП; Наименование объекта; Состав объектов и субъектов обеспечения безопасности; Координаты объектов контроля и управления на картах – схемах объектов; Временная диаграмма контролируемого процесса; Описание типовых ситуации – инциденты и угрозы безопасности; Признаки аварийных и критических ситуаций на объектах; Состав оборудования ИСОКБП; Наименование канала измерения и тип сигнала; Наименование канала управления исполнительными механизмами ИСОКБП; Типовые настройки оборудования и программного обеспечения компонент ИСОКБП; Правила обработки типовых событий (сценарии обработки); Состав ЛПР по мероприятиям ликвидации критических ситуаций и обеспечения безопасности; Типовые решения (действия) ЛПР; Регламент обслуживания ИСОКБП; Временные диаграммы (расписание) основных элементов ИСОКБП; Описание формализованного запроса пользователя; Признаки объектов для особого контроля угроз безопасности («черные спи-	Уточнение и детализация объектов вводимых данных и форматы их представления определяются в рамках проектов базовых ПТК и ПМК ИСОКБП. Содержание вводимых данных определяется для каждого конкретного проекта ИСОКБП для условий конкретного предприятия с учетом выполнения принципа однократного ввода данных «владельцами» основных процессов, сигналов и сообщений и автоматической идентификации записей в базы данных ИСОКБП с указанием источника данных.

№ п/п	Имя типовой функции модуля	Объект (аргумент)	Примечание
		ски», ключевые выражения, фотографии и др.)	
2	Первичная обработка и упорядочение данных: преобразования сигналов в цифровой кодированный сигнал; сглаживание сигналов, исключение выбросов и ложных срабатываний, подавление помех и др.	По приоритетам объектов контроля; По типам сигналов (каналов); По уровню значимости событий – инцидентов угроз; По ЛПР.	Постановка задач первичной обработки данных выполняется для каждого ПТК ИСОКБП с учетом характеристик применяемого оборудования и условий эксплуатации на объектах контроля
3	Вторичная обработка данных (вычисления показателей безопасности по вычислительным моделям) по запросам пользователей: устройств идентификации и сигнализации инцидентов угроз безопасности; ЛПР; программных модулей базовых ПТК и ПМК ИСОКБП	Оценка «сложности» объектов угроз безопасности предприятия; Поток событий-инцидентов угроз безопасности; Поиск коррелированных событий-инцидентов угроз безопасности, связанных с ним объектов, других событий, фактов и субъектов; Планирование мероприятий и оценка ресурсов по сопровождению и профилактике оборудования ИСОКБП; Статистика инцидентов-угроз безопасности; Оценка рисков предприятия (подразделения); Расчет ресурсов на мероприятия по ликвидации угроз и снижению рисков.	Постановка прикладных задач обработки данных приводится в отдельном документе для каждого процесса предприятия с достаточно интенсивным потоком потенциальных угроз безопасности
4	Построение моделей (функциональных зависимостей между переменными состояния объектов и показателями безопасности процессов)	Схемы данных объектов контроля; Схемы процессов обеспечения безопасности предприятия; Сценарии оценки информационных ситуаций и логики взаимодействия ЛПР по инцидентам; Функциональные зависимости уровня безопасности объекта от условий и факторов	Постановки задач построения моделей обеспечения безопасности описываются в отдельном документе, разрабатываемым для определенного класса (типа) процессов предприятия:

№ п/п	Имя типовой функции модуля	Объект (аргумент)	Примечание
		обеспечения безопасности предприятия (территории); Оценка актуальности и своевременности представления данных о состоянии объектов контроля безопасности предприятия; Оценка конфигурации и производительности комплекса средств ИСОКБП; Оценка полной стоимости владения ИСОКБП; Оценка защищенности информации от несанкционированного доступа и ошибок операторов; Оценка деятельности должностных лиц и эксплуатационного персонала ИСОКБП.	процессы эксплуатации зданий и сооружений и систем их жизнеобеспечения; процессы проектирования изделий и технологий; процессы изготовления продукции; транспорт; энергообеспечение; спецобъекты; управление персоналом и соглашениями с контрагентами и др.
5	Контроль, анализ и диагностика процессов	Атрибуты объектов контроля; Уровень доступа пользователей; Период и длительность времени сеансов контроля и мониторинга состояния отдельных объектов контроля; Время работы оборудования ИСОКБП; Длительность сеанса работы пользователей; Граничные значения контролируемых параметров объекта.	Состав контролируемых параметров, процедур мониторинга и диагностики состояния безопасности выбирается для каждого объекта контроля в соответствии с принятой для него моделью оценки угроз безопасности.
6	Координация и согласование решений (взаимодействие со смежными системами)	Служба безопасности предприятия; Информационная служба; Служба эксплуатации зданий и сооружений; Проектно-конструкторские службы; Производственные подразделения; Охрана; Пожарная служба; Транспорт; МВД; МЧС; Поликлиника; Прочие	Импорт-экспорт данных при подготовке и принятии согласованных решений выполняется по соглашениям об обмене данными, принятыми регламентами и форматами передачи данных
7	Формирование управляющих воздействий (сообще-	Указания по установке оборудования и инсталляции программного обеспечения	Форматы сообщений определяются в соответствии со схе-

№ п/п	Имя типовой функции модуля	Объект (аргумент)	Примечание
	ний)	ИСОКБП на объектах предприятия; Программа действий и мер по оценке ситуации на объекте; Команда (сигнал) отключения (включения) канала контроля и управления; Кодированные сигналы для управления исполнительными механизмами отдельных устройств ИСОКБПП	мой взаимодействия подразделений безопасности и типовым документооборотом предприятия
8	Вывод информации	На экран монитора рабочих станций ИСОКБП; На принтер; В базу данных состояний объектов ИСОКБП; В Интернет; В канал сотовой связи; На экран КПК и сотового телефона	Форматы вывода определяются в соответствии с базовыми стандартными интерфейсами соответствующих устройств вывода данных и сценариями обработки данных
9	Системное обслуживание баз данных ИСОКБП: локальных баз данных состояния объектов контроля; распределенных геоинформационных баз данных объектов предприятия; оборудования и технических характеристиках компонент ИСОКБП	Заданный период текущего обслуживания в соответствии с сеансами работ пользователей; Дополнение, обновление и актуализация данных по временному регламенту функционирования объектов контроля и интенсивности потоков; Периодическая сверка данных с внешними базами данных и наследуемыми информационными системами и целевыми АС предприятия	
10	Организация процедур обработки данных	По факту обнаружения события – инцидента угроз безопасности; В соответствии со сценарием диалога и запросами пользователей; Навигация по приложению с минимальным количеством сообщений на экране	

По мере появления новых методов и средств реализации модули могут заменяться на более эффективные, с лучшими характеристиками качества, производительности и эксплуатационной надежности. Следует отметить, что такой подход хорошо согласуется концептуальными положениями сервис-ориентированной архитектуры автоматизированных интегрированных информационных систем предприятий (SOA) и позволяет «встраивать» относительно независимые модули в действующую ИТ инфраструктуру предприятия путем использования имеющихся наработок и наследуемых ИС предприятий, унификации интерфейсов, общих шин обмена данными, распределенных баз и хранилищ данных единого информационного пространства предприятия.

На рис. 9.1 приведена функциональная структура ядра комплекса средств информационных технологий для обеспечения деятельности службы обеспечения безопасности предприятия в составе ПМК-1 «Управление деятельностью службы безопасности предприятия».

Приведем краткое описание отдельных функциональных модулей ядра базового программно-методического комплекса обеспечения безопасности и отдельные рекомендации по их реализации в составе ИСОКБП и взаимодействию с целевыми АС предприятия.

Основными пользователями системы являются руководство службы безопасности предприятия, аналитики службы по отдельным направлениям, а также члены рабочих групп обеспечения безопасности (Совет безопасности) предприятия, администраторы баз данных информационных ресурсов предприятия и ответственные за эксплуатацию целевых АС. В системе предусмотрена также организация доступа к отдельным данным внешних пользователей и владельцев ресурсов, необходимым для деятельности предприятия.

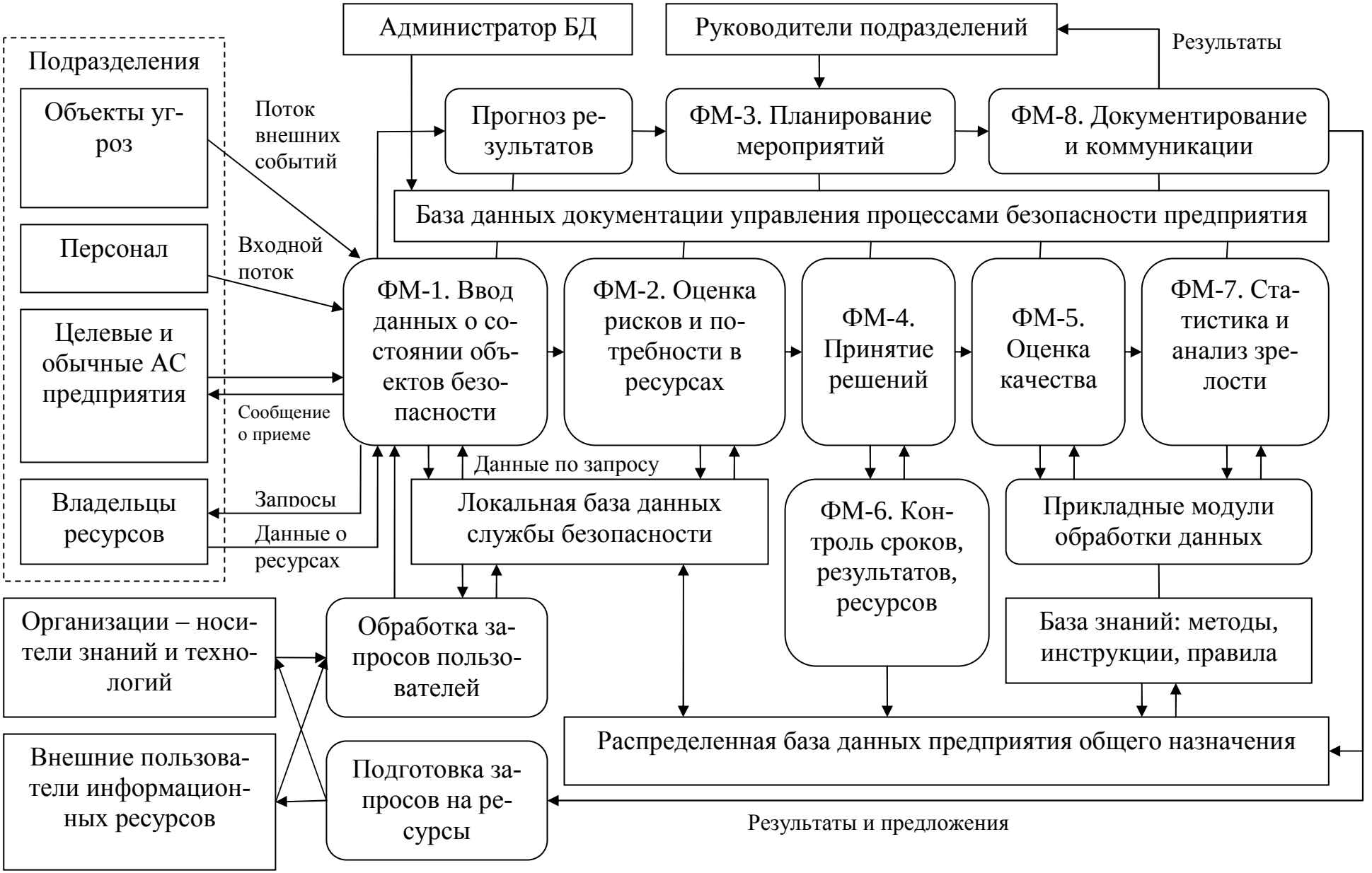

Рис. 9.1. Функциональная структура ядра комплекса средств ИТ службы обеспечения безопасности

В состав системы включаются следующие функциональные модули:

ФМ1 – Ввод данных о состоянии объектов и процессов обеспечения безопасности предприятия. В модуле реализуются функции ручного (или со сканера) ввода данных об основных характеристиках объектов контроля (паспорта безопасности), автоматического ввода измеряемых и контролируемых параметров технических объектов, данные мониторинга состояния отдельных особо опасных объектов и процессов предприятия (по сигналам от систем видеонаблюдения, охранной и пожарной сигнализации и др.), а также данные о событиях – инцидентах угроз безопасности по физическим и информационным «периметрам» безопасности на различных объектах и в подразделениях предприятия.

ФМ2 – Упорядочение данных, оценка сложности объектов контроля, рисков и оценка потребности в ресурсах на обеспечение безопасности предприятия. В модуле реализуются процедуры классификации объектов и субъектов безопасности, экспертной оценки значимости отдельных факторов-угроз безопасности, расчетные модели оценки сложности взаимосвязанных событий-угроз безопасности, уровня рисков, а также выполняются оценочные расчеты потребностей в ресурсах для реализации возможных стратегий, политик и тактик реализации мероприятий по безопасности отдельных объектов или их взаимосвязанной группы.

ФМ3 – Планирование мероприятий по обеспечению безопасности предприятий. В модуле реализуются функции подготовки и согласования Программ и проектов / планов по обеспечению безопасности предприятия и его отдельных подразделений, проверяется наличие паспортов безопасности, проектов и технических предложений по проектированию, комплектации и техническому обслуживанию средств обеспечения безопасности, состояние ресурсов, назначаются исполнители и сроки, определяются ключевые даты для контроля, одобрения или корректировки планов служб обеспечения безопасности и смежных подразделений. Для реализации модуля могут использоваться действующие на предприятии системы планирования текущих и инновационных проектов с учетом соответствующего определения объектов проектирования, применения специализированных терминов и соответствующего уровня конфиденциальности проектов в сфере обеспечения безопасности предприятия.

ФМ4 – Принятие оперативных решений по мероприятиям обеспечения безопасности. В модуле реализуются функции подготовки и согласования индивидуальных и групповых решений по фактам наступления событий - инцидентов угроз безопасности на различных объектах контроля, готовятся планы оперативных мероприятий и действий для снижения рисков в деятельности предприятия, проверяется готовность служб и специалистов по обеспечению безопасности и устранению последствий наступления прогнозируемых или фактических событий- угроз безопасности (блокирование доступа к объектам и информационным ресурсам предприятия, отключение / включение систем энергообеспечения, изменение технических решений и др.). Для реализации модуля могут использоваться известные модели согласования решений в условиях исходной неопределенности, знание статистических характеристик возмущений внешней среды, а также игровые методы ситуационного управления и проблемно-ситуационные штабные игры специалистов.

ФМ5 – Моделирование и оценка качества проектов обеспечения безопасности, технических решений и состояния средств безопасности. В модуле реализуются функции построения моделей функциональных зависимостей выходных показателей состояния безопасности предприятия (и его отдельных процессов) от измеряемых, или каким либо образом оцениваемых характеристиках состояния безопасности, интенсивности наступления событий - инцидентов угроз безопасности, других возмущений внутренней и внешней среды предприятия, наличия необходимых ресурсов для снижения рисков и ликвидации последствий. Специфической особенностью данного модуля является проверка и согласование с применением этих моделей общих системотехнических требований к функционированию предприятия как сложной ОТС [16] технических, методических и организационных решений по архитектуре средств обеспечения безопасности (а в принципе и любых других АС предприятия). Для реализации модуля можно использовать основные положения стандартов [28], а также известные инструментальные средства моделирования динамики, надежности и производительности и качества информационных систем, которые в совокупности и определяют уровень функциональной целостности и безопасности ОТС [21, 29, 30].

ФМ6 – Контроль сроков, результатов, качества и ресурсов проектов и текущего состояния средств обеспечения безопасности. В модуле выполняется периодический или регламентированный опрос со-

стояния заданных объектов контроля и определяются отклонения от «нормативных» плановых заданий или моделей типовых проектов, мероприятий и действий по обеспечению безопасности предприятия, рассчитываются «меры близости» и готовятся адресные рекомендации для принятия решений в сложившейся проектной, модельной или фактической ситуацией на объектах контроля.

ФМ7 – Статистика и анализ зрелости процессов обеспечения безопасности предприятия. В модуле выполняются расчеты статистических характеристик, в общем случае нестационарных временных рядов, случайных процессов в системе обеспечения безопасности, таких как частота событий- инцидентов угроз безопасности, их кластеризация, интенсивность потоков, дисперсионные и корреляционные отношения между отдельными процессами. Анализ зрелости процессов предполагает оценку вероятности выполнения в системе безопасности заданных целевых установок и показателей состояния безопасности отдельных объектов контроля и процессов в заданные сроки и, желательно, с минимальными затратами ресурсов. Для реализации модуля можно использовать отдельные технические решения и распространенные специализированные комплексы программ [35 – 37], а также модули универсальных статистических систем, с обязательной привязкой и настройкой для условий применения в службах безопасности предприятия.

ФМ8 – Документирование и обслуживание коммуникаций службы обеспечения безопасности предприятия. В модуле выполняется ведение реестров типовой документации распределенной службы обеспечения безопасности, проверяется авторизация (в том числе электронная подпись) и комплектность документов по проектам и текущим процессам службы, наличие в документах недозволенных вставок, «вирусов в текстах», конфиденциальных данных, технических ошибок, влияющих на безопасность объектов и процессов предприятия. Реализация модуля может выполняться на основе любых текстовых редакторов, применяемых на предприятии офисных систем и СУБД. Целесообразно интегрировать этот модуль с системами электронной почты, электронной цифровой подписи, шифрования данных, ведения общих и специализированных информационных ресурсов предприятия, а также обеспечить доступ к основным целевым АС предприятия (САПР-конструкций, САПР-технологий, АС управления материальными ресурсами, АС управления персоналом и др.)

Таблица 9.2 – Основные направления применения методов многомерного статистического анализа

Основные направления анализа	**Применяемые методы**	**Примеры прикладных задач**
Статистические исследования зависимостей между показателями.	Корреляционный анализ. Дисперсионный анализ. Факторный анализ. Таблицы сопряжения	Построение функциональных зависимостей.
Классификации объектов по многомерным статистическим признакам.	Кластерный анализ. Распознавание образов. Многомерное шкалирование. Таксономия	Выявление типологии
Снижение размерности и выявление наиболее информативных признаков.	Исключение дублирования данных. Расчет информативности признаков (определение весовых оценок признаков). Анализ мер близости.	Выбор состава и числа датчиков системы. Декомпозиция систем на элементы.
Сжатие больших массивов данных.	Группировка данных Агрегирование. Косвенные вычисления. Взвешивание (определение приоритетов хранения). Нормализация данных.	Системы статистической отчётности.

В качестве основных элементов интеграции в ИСОКБП предусмотрены модули организации и ведения трех относительно независимых, но согласованных по стандартам и интерфейсам обмена данными баз данных: локальная база подразделения безопасности, база данных управления проектами безопасности предприятия, распределенная база данных информационных ресурсов общего назначения.

В локальной, и особо защищенной, базе данных службы безопасности предприятия хранятся сведения об объектах и субъектах безопасности предприятия, нормативной документации, основных терминах и понятиях безопасности, рекомендуемых для применения на предприятии, характеристиках средств обеспечения безопасности, результаты текущего мониторинга состояния безопасности основных объектов и процессов (подразделений) предприятия, Программы и планы работ Совета по безопасности предприятия, история инциден-

тов угроз безопасности и результатов по их нейтрализации, а также другая информация с ограниченными правами доступа.

В базе данных управления проектами безопасности хранятся сведения о состоянии технических предложений по разработке инновационных проектов средств обеспечения безопасности для предприятия, решения и планы работ по проектированию, состояние работ по этапам, исполнителям, срокам и выделенным ресурсам для реализации проектов, а также сведения о технических характеристиках установленных в подразделениях предприятия технического и программного обеспечения средств безопасности и документация по их техническому обслуживанию в нормальных и критических ситуациях.

В распределенной базе данных общего назначения хранятся сведения о метаданных информационных ресурсов предприятия, адресные ссылки на места хранения этих ресурсов в составе целевых АС или общих хранилищ информационных ресурсов предприятия, таких как общие характеристики продукции, процессов и услуг предприятия, которые должны быть доступны (с соответствующим уровнем доступа) для специалистов, занятых в основных проектах и управлении реальными процессами предприятия.

Дополнительно в состав системы могут также входить специализированные интеллектуальные базы знаний в отдельных сферах деятельности предприятия, в которых хранятся методы, инструкции и правила действий в той или иной информационной ситуации по типу «Если на объекте О наступило событие А и/или А1, фактическая или прогнозная ситуация о наличии ресурсов на объекте – R, то следует выполнить инструкцию Д или серию действий Д1, Д2, Д5».

Применение интеллектуальных баз знаний может быть положено в основу создания специализированных экспертных систем для формирования и принятия решений по обеспечению безопасности отдельных в заданной предметной области и достаточно ограниченной сфере деятельности, в частности, для расследования происшествий, формирования списков мероприятий и назначения исполнителей. Реализация таких экспертных систем может быть выполнена как в рамках специализированных приложений в среде типовых СУБД общего назначения, так и с применением известных типовых оболочек экспертных систем. Наиболее сложным и ответственным элементом таких систем является формирование адекватного набора таких правил, полнота и корректность которого и определяет целесообразность и эффективность экспертной системы.

Выбор программно-аппаратной платформы и СУБД для реализации комплекса во многом определяется характеристиками прикладных целевых АС предприятия, структурой и объемами информационных ресурсов предприятия, интенсивностью обмена данными с другими службами и целевыми АС предприятия, а также и имеющимися ресурсами техники, персонала, финансов, уровнем подготовки персонала и наличии осознанных потребностей пользователей в информации для принятия решений.

В качестве среды реализации этой базы для предприятий с особым режимом можно рекомендовать сертифицированные Гостехкомиссией желательно отечественные СУБД, например СУБД ЛИНТЕР [46].

ЛИНТЕР – это система управления базами данных, обеспечивающая поддержку реляционной модели данных автоматизированных систем управления различного назначения, систем реального времени и систем, где необходимы повышенные требования к надёжности, безопасности и секретности данных. В соответствии с реляционной моделью данные базы логически представлены в виде двумерных таблиц, что обеспечивает высокую степень независимости пользовательских программ от физического представления данных и удобство для неподготовленного пользователя.

Данные в таблицах физически хранятся построчно. В одну строку могут входить данные разных типов (символы, целые и вещественные числа, строки символов различной длины, и т.д.). ЛИНТЕР позволяет выполнять следующие действия:

- удалять/изменять/добавлять объекты базы (данные, индексы, таблицы, хранимые процедуры, триггеры);
- вводить/изменять/удалять ограничения целостности данных;
- использовать полный набор возможностей стандартного языка SQL;
- работать с большими (до 2-ух гигабайт) байтовыми объектами (BLOB);
- импортировать/экспортировать данные из/в ASCII и DBF файлов;
- блокировать/деблокировать доступ к таблице/записи;
- использовать (в приложениях и хранимых процедурах) различные режимы обработки транзакций;
- организовывать (и использовать) гибкую и надежную систему безопасности и секретности информации (сертифицирован Государственной технической комиссией при Президенте РФ на соот-

ветствие 2 классу защиты информации от несанкционированного доступа, что соответствует уровню В3 по американскому национальному стандарту orange book);

- сохранять/восстанавливать базу данных целиком или некоторые её объекты выборочно, устанавливать расписание и алгоритмы сохранения;
- транслировать запросы (с параметрами и без) и использовать уже оттранслированные запросы для ускорения работы приложения;
- создавать, отлаживать и запускать хранимые процедуры и триггеры;
- использовать возможности реального времени (приоритеты выполнения транзакций, асинхронное выполнение запросов, отслеживание процессов, проходящих в системе, приостановка и полная остановка работы указанной транзакции и пр.).

Достаточно полный набор функций СУБД и инструментальных средств разработки и поддержки прикладных задач на различных языках программирования дают возможность пользователям реализовать сложные многозадачные прикладные системы и настроить ЛИНТЕР на конкретное приложение.

Реализация рассмотренных выше функций слабо зависит от применяемых на предприятии технических средств и практически может быть выполнена на любой программно-аппаратной платформе современных средств ИКТ. При этом выбор конкретной технической архитектуры, состава оборудования и операционной среды реализации комплекса определяется сложностью ИТ инфраструктуры предприятия, количеством объектов контроля угроз безопасности, интенсивностью негативных воздействий внутренней и внешней среды предприятия.

На рис. 9.2 приводится обобщенная техническая архитектура ИСОКБП для предприятий наукоемкого машиностроения. На левой части рисунка показаны элементы собственно комплекса безопасности предприятия, а на правой – элементы общей ИТ инфраструктуры предприятия. Реализация ядра ПМК-1 «Управление деятельностью подразделений безопасности» предусматривается на рабочих станциях подразделений безопасности, а отдельные клиентские модули могут быть установлены в основных подразделениях предприятия – владельцах ключевых процессов с повышенным риском угроз безопасности.

В технической архитектуре ИСОКБП предусмотрены следующие основные структурные элементы:

- рабочая станция руководства подразделений безопасности;
- рабочая станция аналитиков безопасности ключевых процессов предприятия;
- рабочая станция администратора информационных ресурсов;
- сервер базы данных подразделений безопасности.

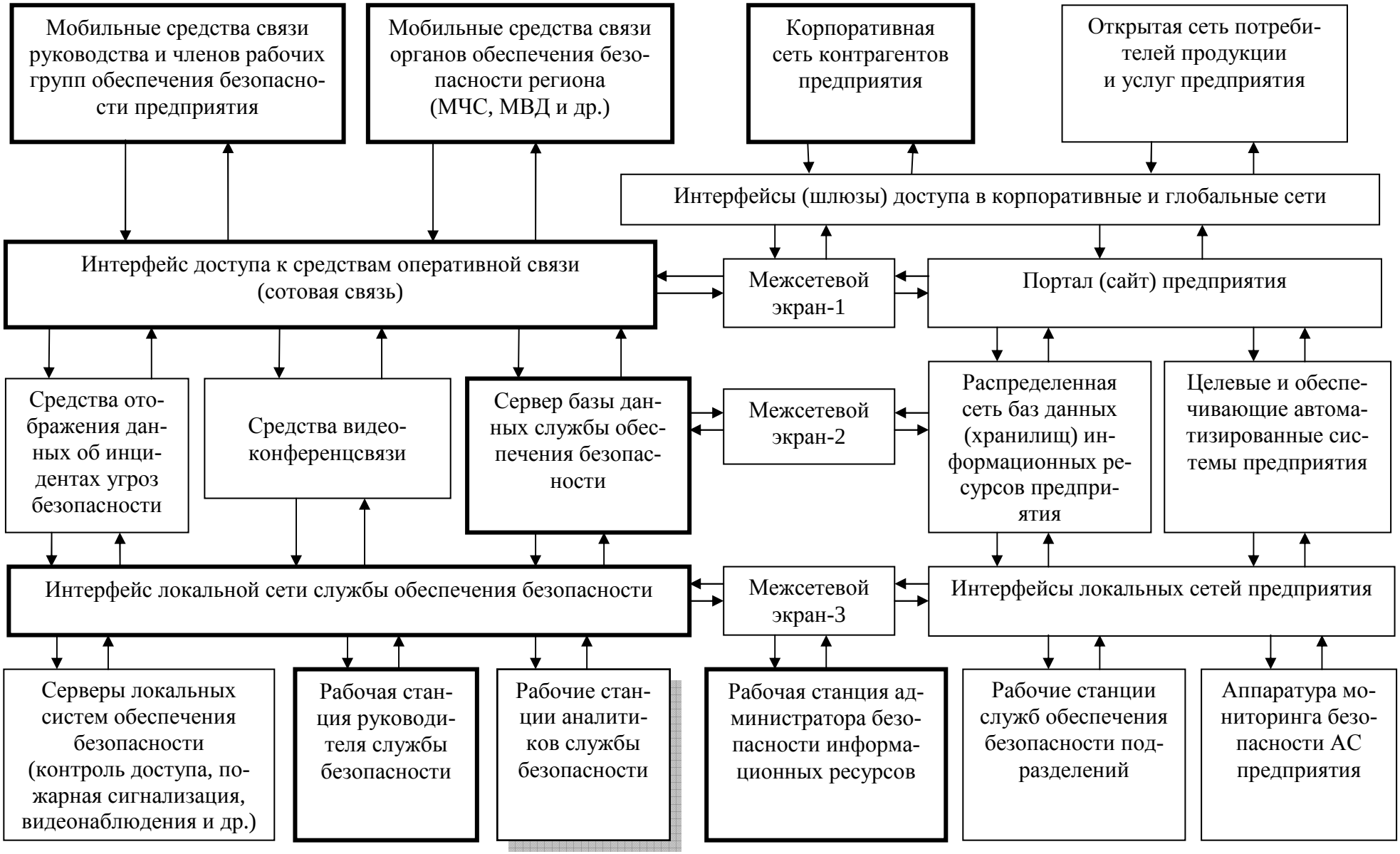

Рис. 9.2. Техническая архитектура (структура) ИСОКБП

(жирным цветом выделен минимально необходимый состав технического обеспечения службы безопасности предприятия)

10 Организация разработки и внедрения интегрированной системы обеспечения безопасности машиностроительного предприятия

Организация интегрированной системы безопасности включает также проектирование систем защиты и комплекса безопасности.

Проектирование систем защиты периметров требует использования комплексного подхода. Применяемые средства и методы должны быть разумно достаточны, адекватны возможной угрозе, а меры противодействия должны быть сбалансированными, то есть распределены по возможности в соответствии с вероятностью угроз и важностью защищаемой зоны. Кроме того, устанавливаемые средства и системы не должны создавать препятствий для нормального функционирования объекта и тем более быть опасными для сотрудников или других людей, проходящих рядом с периметром [45].

Структура комплекса безопасности включает:

- периферийное оборудование (контроллеры, считыватели, охранные извещатели, видеокамеры, электромагнитные замки, турникеты, картоприемник, и т.п.);
- серверное оборудование подсистем охранной и пожарной сигнализации, видеонаблюдения, контроля доступа (на базе персональных компьютеров);
- удаленные рабочие места интегрированного комплекса безопасности и отдельных подсистем (охранная и пожарная сигнализация, видеонаблюдение, контроль доступа);
- локальная сеть системы безопасности (оптоволокно), активное и пассивное сетевое оборудование.

Для анализа показателей деятельности служб безопасности предприятия предлагается использовать таблицу, форма которой приведена в Таблице 10.1.

Таблица 10.1 – Показатели деятельности подразделений безопасности
(уточняется на предприятии, конфиденциально по заполнении)

1	2	3	4	5	6	7	8
Наименование показателя	**Обозначение**	**Ед. изм.**	**Источник данных**	**Диапазон изменений**	**Факторы, влияющие на показатель**	**Метод определения**	**Влияние на показатели предприятия**
1. Показатели результативности деятельности							
Количество подразделений (объектов), обслуживаемых службой	$N_{0К}$	ед.	Приказ	10 – 50	Уровень рисков предприятия	Профессионально-логический анализ процессов	
Количество мероприятий по проектам обеспечения безопасности	*Nмб*					Факт	
Количество контролируемых процессов и услуг безопасности	*Nпб*					Факт	
Количество выявленных угроз безопасности	*Nуб*					Факт	
Количество установленных устройств средств обеспечения безопасности за период	*Nтс*		Реестр средств ИСОКБП				
Количество инсталляций новых про-	*Nпс*		Реестр				

1	2	3	4	5	6	7	8
граммных средств обработки данных			средств ИСОКБП				
Количество документов, подготовленных для приятия решений на уровне предприятия	*Nдб*		Отчет подразделения				
Количество рассмотренных экспертиз (проверок) документов (сообщений) текущего, контроля безопасности и мониторинга состояния процессов	*N мб*	число сообщений за период	Отчет подразделения				
2. Показатели качества работ и услуг подразделений безопасности предприятия							
Среднее время реагирования на событие-инцидент угроз безопасности, в том числе по типам угроз:	*Трсиб*	Минуты, часы, сутки	Журнал регистрации событий			Факт-прогноз	
Нарушение режима доступа на предприятие							
Несанкционированное использование ИР и программного обеспечения							
Ошибки персонала							
Отказы основного оборудования							
Аварии на объектах и чрезвычайные ситуации							
Средняя частота отказов оборудования и программного обеспечения ИСОКБП за период	*Fотк*	Кол. отказов в ед. времени	Журнал регистрации отказов				
Среднее время восстановления обо-	*Твост*	Минуты	Журнал				

1	2	3	4	5	6	7	8
рудования ИСОКБП после обнаружения неисправности, в том числе по типам устройств (с учетом замены блоков) - пожарной и охранной сигнализации - видеокамер - рабочих станций - серверов - коммуникационного оборудования и средств связи		часы, сутки	ремонтов				
3. Показатели использования ресурсов							
Количество штатного персонала подразделения безопасности	*Псбш*	Человек.					
Количество внештатных сотрудников и ответственных за безопасность в основных подразделениях предприятия	*Псбп*	Человек					
Объем и количество зарегистрированных средств обеспечения безопасности в базе данных ИР подразделений безопасности	*Vирб* *Nзирб*	Кол-во записей Объем записи	Реестр средств ИСОКБП				
Количество договоров на обслуживание средств ИСОКБП с внешними организациями	*Дсб*						
Количество единиц установленного оборудования средств ИСОБКП, в	*Nоб*		Реестр средств				

1	2	3	4	5	6	7	8
том числе по типам устройств: - пожарной и охранной сигнализации - видеокамер - рабочих станций - серверов - коммуникационного оборудования и средств связи			ИСОКБП				
Транспорт							
Фонд заработной платы							
Объем финансирования подразделений безопасности, в том числе по источникам: – бюджет предприятия; – бюджет подразделения; – региональные и федеральные госпрограммы - по договорам с внешними организациями-заказчиками	*Тыс. руб*						
В том числе по источникам: – бюджет предприятия; – бюджет подразделения; – региональные и федеральные госпрограммы - по договорам с внешними организациями-заказчиками							
4. Показатели зрелости процессов безопасности (с учетом основных положений ГОСТ РВ 51987) (заполнение этой части таблицы целесообразно выполнить для процессов (объектов) с повышенными требова-							

1	2	3	4	5	6	7	8
ниями к безопасности)							
Вероятность выполнения запланированных мероприятий в заданные сроки и с заданным качеством	*Рсб*		План-отчет	0,5 – 0,9			
Средняя наработка объекта контроля на отказ или сбой (по показателям безопасности)	*Тнар*	Часы, сутки	Отчет о ремонтах				
Среднее время восстановления объекта после отказа или сбоя	*Твос*		Отчет о ремонтах				
Коэффициент готовности объекта	*Кг*						
Вероятность надежного представления и/или доведения запрашиваемой (выдаваемой принудительно) выходной информации в течение заданного периода функционирования ИС *Тзад*	*Рнад*	Вероятность	Результаты моделирования	0,8 -0,9			
Среднее время реакции системы при обработке запроса и/или доведении информации до ЛПР или вероятность своевременной обработки информации за заданное время *Тзад*	*Тполн Рсв*	Минуты, часы, сутки	Результаты системотехнического анализа объектов				
Вероятность обеспечения полноты оперативного отражения в ИС новых реально существующих объектов учета (угроз безопасности)	*Рполн*	Шкала оценок Вероятности	Результаты моделирования	0,5 -0,8			
Вероятность сохранения актуальности информации на момент ее использования	*Ракт*	Шкала оценок Вероят-	Результаты моделиро-				

1	2	3	4	5	6	7	8
		ности	вания				
Вероятность отсутствия ошибок во входной информации на бумажном носителе при допустимом времени на процедуру контроля *Тзад*	*Рбум после*	Шкала оценок Вероят-ности					
Вероятность отсутствия ошибок во входной информации на машинном носителе при допустимом времени на процедуру контроля *Тзад*	*Рмаш после*	Шкала оценок Вероят-ности					
Вероятность получения корректных результатов обработки информации за заданное время *Тзад*	*Ркорр*	Шкала оценок Вероят-ности					
Вероятность сохранения конфиден-циальности информации в течение периода ее объективной конфиденци-альности *Тконф*	*Рконф*	Шкала оценок Вероят-ности					
Вероятность безошибочных действий должностных лиц в течение заданно-го периода функционирования ИС *Тзад*	*Рчел*	Шкала оценок Вероят-ности	Модели-рование процессов обслужи-вания сис-тем чело-веком				
Вероятность отсутствия опасного воздействия в течение заданного пе-риода функционирования ИС *Тзад*	*Рвозд*	Шкала оценок Вероят-ности	Анализ за-конов рас-пределе-ния слу-				

1	2	3	4	5	6	7	8
			чайных потоков данных				
Вероятность сохранения защищенности информационных и программных ресурсов ИС от несанкционированного доступа (НСД)	$P_{НСД}$	Шкала оценок Вероятности	Моделирование средств защиты				

Таблица 10.2 – Примерная схема документооборота служб обеспечения безопасности машиностроительного предприятия

1	2	3	4	5	6	7	8	9	10	11	12	13
Типы документов: В – корпоративного применения; А – внутреннего применения, унифицированный; П – документация группы исполнителей не унифицированная; Р – регионального или отраслевого применения; Г – общегосударственного применения.		Применяемость в службах: И – документ применяется для информирования персонала о внешних событиях, решениях; О – документ, требующий ответа или отчета по внешнему запросу; Ф – формирование исходного текста или заполнение унифицированной формы; Т – технологический документ обеспечения деятельности подразделения (инструкции, правила и т. п); К – документ контролируется (отслеживается) данной службой; С – согласование решений и документов; У – утверждение документов										
Наименование вида документа	Тип	Применяемость документа										
		В службах предприятия								Во внешних организациях		
		Руководство предприятия	Службы инфраструктуры жизнеобеспечения	Разработчики изделий и технологий	Экономическая служба	Производство	Снабжение	ИТ-служба	Служба безопасности	Мин-во	Поставщики	Потребители
Документация по объектам контроля безопасности												
Техническое описание угроз безопасности объекта	А	У	Ф	Ф	Ф	Т	И	У, К	Т, С	С	С	-

1	2	3	4	5	6	7	8	9	10	11	12	13
Схема размещения объектов	В	С, И	Ф	И	И	-	-	У, К	Ф, Т	-	-	-
Описание процессов и услуг безопасности	В	У	Ф	Ф	Ф	Ф	Ф-	С, К	Ф, Т	-	С	И
Реестр средств безопасности		У, И	И, Т	И	И	И	И	Т	Ф	С	С	С
Регламент использования комплекса средств безопасности	Р	У	Т	Т	Т	Т	Т	Ф, К	Ф, К	-	Ф	-
Паспорт безопасности объекта		У	Ф	Ф	Ф	Ф	В	С, И,Т	С, И, К	И	И	И
Список атрибутов источников и признаков инцидентов угроз безопасности	А		Ф	Ф	Ф	Ф		С, К, Т	С, К			
Журнал регистрации событий-инцидентов угроз безопасности		И	Т, О	Т, О	Т, О	Т, О	Т, О	И, Ф	С, Ф, К			
Список лиц принимающих решения по инцидентам угроз безопасности	А	У	Ф, И	Ф, И	Ф, И	Ф, И	Ф, И					
Сценарий – план действий по обеспечению безопасности объекта (для процессов с повышенным уровнем риска)	А	У	Ф, С	И	Ф, С			С, И, Т	С, Т, К			
Схема взаимодействия и связи по оперативным мероприятиям обеспечения безопасности в критических ситуациях		У	Ф	Ф	Ф	Ф	Ф	Ф	Ф, К			

1	2	3	4	5	6	7	8	9	10	11	12	13
Документация проектов комплексов средств обеспечения безопасности предприятия												
Результаты предпроектного анализа рисков основных процессов предприятия	А	К, У	Ф	И	И	И	С	И	С	-	-	И
Концепция (политика) обеспечения безопасности	А	Ф, У	С		-	-	С	И		-	-	-
Техническое задание	А	У	Ф		-	-	-	-	-	-	-	-
Спецификация требований к компонентам	А	Ф	И, С	И	-	-	С	-	С	-	-	-
План разработки	В	Ф, У	С	И, С	И, С	-	-	-	-	-	-	-
Системный проект комплекса средств безопасности		У	Ф	И	И	-	С	-	-	-	-	-
Описание информационного обеспечения (базы данных)		И	И	И	И	-	-	У	-	-	Ф	-
Описание алгоритма (сценария анализа рисков)		У	С, И	С, И	С, И	С, И	С, И	-	-	-	-	-
Документация на прикладной компонент		У	-	И, С	Ф	-	-	С, Т	С, Т, К	-	Ф	-
Руководство по документированию проекта		Ф, У	И	И	И	-	-	-	-	-	И	-
Технологические инструкции по монтажу, инсталляции и наладке (настройке) средств безопасности		У	С	-	Ф	-	-	С,Т,-	-	-	-	-
Программа и методика испытаний компонент		У	И, С	И, С	И, С	И, С	И, С	С, Т,К	С, Т, К	И	Ф	И
Описание изделия (средства)		Ф										

1	2	3	4	5	6	7	8	9	10	11	12	13
безопасности												
Руководство пользователя		У	-	-	Ф, К	-	-	-	Т, С	-	Ф, С	-
Документация текущего административного управления		Ф, У	С, К	С, И	С, И	-	-	-	-	-	-	-
Инструкция по формированию и ведению базы данных		У			Ф							
Паспорт на программное средство		Ф, У	С	С	С	-	-	-	-	-	-	-
Разрешительная документация (сертификаты)		Ф, У	С	С	С	-	-	-	-	-	-	-
Документация управления проектами безопасности предприятия												
Технические предложения по проекту												
Технико- экономическое обоснование (бизнес-план)										Ф		
Решение научно технического совета или координационного совета (рабочей группы) по безопасности предприятия		У						Ф	Ф			
Приказ о производстве работ	В	-	-	-	-	-	-	Ф, У	И	И	И	И
План-график производства работ	А	-	-	-	-	-	-	У	Ф	-	И	С
Список исполнителей												
Отчёт о состоянии работ	П	-	-	-		-		У	Ф		С	
Технические условия на по-												

1	2	3	4	5	6	7	8	9	10	11	12	13
ставку компонент (тендер)												
Договор на разработку (поставку) оборудования и программного обеспечения	П	-	-	-	-	-	-	С, У	Ф, С	-	С	Ф
Протокол заседаний группы реализации проекта	А	-	-			-	-	У	Ф	И	И	
Протокол испытаний (системных, предварительных, эксплуатационных и др.)	Р	-	-			-	-	У	С	И	И	Ф
Акт приёмки-сдачи	А, В	-	-	-		-	-	У, К	Ф	И	С	С
Отчет по результатам опытной эксплуатации		У	С	С	С	С	С	Ф, Т	Ф		С	
Приказ о внедрении и развитии системы		У						Ф, Т	Ф			

Рис. 10.1. Диаграмма потоков данных

Разработка действенных ИТ-проектов предприятия и, в частности, интегрированных систем обеспечения комплексно безопасности – многоплановая задача с повышенными требованиями к качеству разработки и социальным результатам, влияющим на уровень зрелости процессов предприятия. Качество проектов обеспечения безопасности предприятия, их функциональная полнота определяет их реализуемость (именно низкое качество ИТ- проектов, часто не учитывающих отдельные аспекты деятельности и сводящиеся к перечислению слабо связанных между собой «мероприятий» и затрат на их реализацию, является бедой многих Программ развития, так и не воплотившихся в жизнь).

Для решения этих задач в проектах ИСОКБП должны быть предусмотрены:

- организационно-методические материалы по экспертизе технических предложений и проектных решений, методам испытаний и приемки компонент и др. материалы, необходимые для организации и координации работ по реализации ИТ- проектов и отдельных мероприятий;
- нормативные документы для исполнителей по унификации структур различных видов обеспечения проектов, протоколов связи, соглашений по использованию общих информационных и коммуникационных ресурсов;
- типовые организационно-технические мероприятия по подготовке объектов и базовые программы подготовки персонала.

Эффективность процессов обеспечения безопасности деятельности предприятия в значительной мере определяется организационно-технологическим уровнем совместных работ служб обеспечения безопасности предприятия, служб информационных технологий, охраны, пожарной и, а также качеством средств и систем ИТ обеспечения безопасности, уровнем обоснованности и полнотой задания всего комплекса работ по обеспечению безопасности предприятий, своевременности подготовки объектов и оперативного персонала к внедрению.

В этой связи особое внимание должно уделяться подготовке и переподготовке специалистов в области проектирования средств и систем ИТ, а также специалистов – конечных пользователей ИТ в части применения доступных методов формализованных описаний продуктов, процессов и ресурсов конкретных ОТС.

Требования индивидуализации ИТ проектов обеспечения комплексной безопасности предприятия будут стимулировать развитие следующих сценариев подготовки и выбора проектных решений. Предприятие с привлечением независимых консультантов и экспертов выполняет анализ стратегии развития предприятия, уточняет архитектуру предприятия, разрабатывает концепцию обеспечения безопасности и применения необходимых организационных, методических, технических и программных средств обеспечения безопасности,, проводит анализ наследуемых ИС, типовых проектных решений разного уровня и формирует наборы системных спецификаций - требований к компонентам АИС обеспечения безопасности, которые рассылаются потенциальным внутренним и внешним исполнителям проекта и поставщикам средств.

Далее проводится тендер по отдельным проектным направлениям. Победители тендера и включаются в рабочую группу реализации системного проекта. Общее управление и координацию работ по проекту осуществляет служба безопасности предприятия как владелец и основной пользователь основного проекта. ИТ- служба предприятия обеспечивает подготовку общих соглашений по использованию базовых средств информационных технологий предприятия. Рабочая группа в соответствии с компетенциями своих членов готовит индивидуальный системный проект АИС обеспечения безопасности предприятия, при этом используются общие для проекта соглашения по использованию проектных решений в соответствии с принятыми критериями оценки качества компонент АС.

По результатам общесистемного проекта АИС предприятия может также проводиться второй тендер на поставку необходимого оборудования и разработку отдельных компонент программного обеспечения по согласованным спецификациям базового профиля прикладных АС предприятия, гармонизированного с национальными и отраслевыми профилями.

Большое количество, разнородность и распределенность по территории критически важных для безопасности объектов и процессов предприятия диктует необходимость проведения ряда комплексных общесистемных работ (мероприятий) в направлении повышения их общей безопасности и защищенности.

Для того чтобы построить эффективную систему обеспечения безопасности и защищенности конкретного предприятия (объекта), необходимо сначала выполнить ряд этих предварительных мероприя-

тий, и только после этого осуществлять его комплектацию теми или иными средствами или системами безопасности.

Эти работы не требуют серьезных капитальных вложений, но именно они создают базис проекта, что позволит в последующем обеспечить реально необходимый и экономически оправданный выбор средств обеспечения безопасности процессов и их защищенности от различного вида угроз нарушения целостности системы.

Как показывает практика, в этих целях целесообразно выполнить следующие мероприятия.

1. Комплексное обследование предприятия и исходный аудит ключевых процессов с позиций выявления источников и угроз безопасности, их типизация, разработка и согласование модели угроз [42] и требований по защищенности объектов предприятий, определение опасных зон объекта, выявление уязвимых элементов предприятия с учетом как непосредственно его специфики, прилегающих территорий с расположенными на них другими объектами.

2. Разработка Концепции комплексной системы обеспечения безопасности предприятия - как основополагающего документа, определяющего политику в области обеспечения комплексной безопасности от реализации угроз различного характера на перспективу. Этот документ описывает требования по обеспечению безопасности объекта от реализации возможных угроз (террористических, криминальных, а также техногенного и природного характера) и рекомендаций по повышению его защищенности.

3. Разработка Паспортов безопасности предприятия. Эти документы не только дадут полную картину состояния безопасности объектов, в том числе опасных ситуаций, но и определят ряд конкретных мероприятий по усилению защищенности объектов. Паспорт безопасности должен включать следующие основные разделы: общие сведения, сведения о ЛПР и персонале, мероприятия по обеспечению безопасности предприятия (в том числе технические) по годам (обычно на 5 лет), ситуационные планы и схемы, характеристики систем жизнеобеспечения, организация взаимодействия с органами обеспечения безопасности (ФСБ, МВД и МЧС), а также с аварийными службами, выводы и рекомендации. Паспорт безопасности определяет минимально необходимый и финансово обоснованный набор инженерно-технических средств и информационных систем обеспечения безопасности объекта, что позволит с наибольшей вероятно-

стью и эффективностью решить проблему защиты объекта от всего спектра реализации возможных угроз.

4. Разработка ведущими специалистами предприятия Предложений к Программе создания интегрированной системы обеспечения комплексной безопасности. Здесь должны быть указаны варианты организационных и инженерно-технических решений обеспечения безопасности, а также мероприятия по физической защите объекта (где необходимо).

5. Создание интегрированной автоматизированной системы обеспечения комплексной безопасности предприятия позволит руководству держать вопросы обеспечения безопасности под постоянным контролем (центр безопасности функционирует в режиме реального времени), повысить дисциплину и ответственность персонала, сократить время реакции на реализацию необходимых мер при чрезвычайных ситуациях или возможности их возникновения.

Выполнение общесистемных работ позволит руководству предприятия системно и планово совершенствовать и развивать систему обеспечения безопасности, последовательно и согласованно повышая уровень эффективности системы безопасности предприятия.

Общесистемные мероприятия нужны, чтобы планомерно и последовательно строить систему обеспечения комплексной безопасности предприятия в целом, видеть перспективу и обоснованно распределять ресурсы на реализацию проектов обеспечения безопасности. Но, в то же время, это совсем не исключает «объектового» подхода к построению системы обеспечения комплексной безопасности. Именно разумное сочетание этих двух направлений деятельности, их согласованная и взаимоувязанная реализация, позволят в минимальные сроки и с наибольшим эффектом решить самые насущные проблемы обеспечения безопасности.

Выполнив перечисленные выше мероприятия как общесистемного, так и «объектового» характера, можно аргументировано решать, какие конкретные средства и системы мониторинга и обеспечения безопасности нужно и целесообразно применять на каждом конкретном объекте и в системе в целом.

Материалы системного проекта готовятся по всему предприятию в целом и по каждой его составной части (зданию, сооружению). В материалах должны быть отражены вопросы по разделам: физическая охрана объектов и персонала; инженерно-техническая оснащенность процессов и технические средства (системы) охраны и

контроля; безопасность проектов конструкторской и технологической документации, защита интеллектуальной собственности предприятия, технологическая безопасность, экологическая безопасность, безопасность изделий, продукции и услуг предприятия, средства связи и оповещения; предложения и рекомендации по укреплению защищенности объекта, нормативно-правовое обеспечение, состояние здоровья коллектива предприятия.

Таблица 10.1 – Типовая программа работ по созданию ИСОКБП

Этапы проекта	**Наименование работ**	**Сроки выполнения**	**Оценка затрат (тыс. руб.)**	**Результаты, отчетные документы**
1 этап. Системные исследования и разработка моделей обеспечения комплексной безопасности ключевых процессов предприятия				Разделы системного проекта
1.1	Системный анализ процессов предприятия и разработка концепции, политики и стратегии обеспечения безопасности			Концепция
1.2	Спецификация требований к базовым компонентам проекта			Требования к компонентам
1.3	Проектирование структур данных и рекомендаций по выбору среды реализации и инструментальных средств			Системная архитектура Структуры данных
1.4	Разработка проектов документации организационного и методического обеспечения			Рекомендации по составу методического обеспечения и выбору стандартов
1.5	Проектирование процессов, логики обработки данных и сценариев анализа инцидентов угроз безопасности			Описание процессов по стандартам IDEF, UML или аналогичных
1.6	Комплектация (закупки) базовых средств, включая международные и национальные стандарты			Решения по закупкам
1.7	Оценка и системные испытания базовых компонент			Программа и методика испытаний

Этапы проекта	Наименование работ	Сроки выполнения	Оценка затрат (тыс. руб.)	Результаты, отчетные документы
1.8	Подготовка документации системного проекта			Рекомендации по внедрению
2 этап. Разработка (выбор) средств реализации базовых ПТК и ПМК ИСОКБП				Системная документация
2.1	Системный анализ среды реализации и интерфейсов с целевыми и обеспечивающими автоматизированными системами предприятия			Профиль средств ИСОКБП
2.2	Формирование спецификаций требований к компонентам ИСОКБП			Спецификации требований
2.3.	Проектирование и настройка компонент организационного, программного и технического обеспечения			Технические предложения по компонентам
2.4	Разработка соглашений по обмену данными и интерфейсов пользователей			Проекты соглашений по взаимодействию Форматы представления данных
2.5.	Программирование и отладка модулей базовых компонент системного ядра ИСОКБП			Описания программных модулей
2.6	Комплектация и комплексирование компонент организационного, методического и программного обеспечения			Решения по комплектации
2.7	Системные испытания и опытная эксплуатация средств			Программы и методики испытаний. Протоколы и акты испытаний
2.8	Внедрение и разработка рекомендаций по развитию и модификации средств ИСОКБП			Рекомендации по модификации и развитию
3 этап. Проектирование распределенной интегрированной системы мониторинга состояния безопасности процессов предприятия				Комплект документации

Этапы проекта	Наименование работ	Сроки выполнения	Оценка затрат (тыс. руб.)	Результаты, отчетные документы
3.1	Системный анализ объектов и процессов мониторинга угроз безопасности и спецификаций требований к техническому и программному оснащению ситуационного центра ИСОКБП			Аналитический отчет-справка о потребностях в использовании компонент
3.2	Подготовка проектов организационно-распорядительной документации и регламентов деятельности центра			
3.3	Организация подготовки и обучение персонала и специалистов предприятий Проведение семинаров-совещаний с участниками проектов			Программа обучения. Отчет о проведении
3.4	Оборудование помещений центра			
3.5	Комплексирование средств базовых ПТК и ПМК			Программа и методика испытаний, Комплект образовательных программ
3.6	Системные испытания и опытная эксплуатация компонент			Акты и протоколы испытаний
3.7	Организация внедрения и сопровождения базовых компонент			Комплект форм договоров на услуги и сопровождение проектов
	Итого затрат на проект (тыс. рублей)			Оценочные сметы затрат на реализацию проекта уточняются на каждом этапе
	В т. ч. по источникам финансирования			
	Собственные средства			
	Внешние инвестиции			
	Средства консолидированного бюджета			

Заключение

По результатам системотехнического анализа состояния современных подходов, методов и средств обеспечения безопасности, а также выполненных работ по аудиту и по подготовке рабочих материалов к концепции системного проекта обеспечения комплексной безопасности машиностроительного предприятия можно сделать следующие рекомендации.

1. Организовать постоянно-действующую рабочую группу ведущих специалистов подразделений предприятия по вопросам обеспечения безопасности. Координацию работ рабочей группы и общее методическое обеспечение целесообразно закрепить за специализированной службой обеспечения безопасности, работы по техническому и программному обеспечению «Интегрированной системы обеспечения комплексной безопасности предприятия» (ИСОКБП) закрепить за ИТ-службой предприятия.

2. Закрепить за каждой целевой автоматизированной системой предприятия базовые подразделения (владельцев основных процессов) и сформировать рабочую группу управления системным проектом ИСОКБП под руководством заместителя генерального директора по безопасности. В состав группы реализации проекта ИСОКБП могут также включаться специалисты внешних организаций – разработчики средств методического, технического и программного обеспечения безопасности систем и ИТ-продуктов общего применения.

3. Руководителям структурных подразделений подготовить предложения по составу подсистем ИСОКБП, объектов и процессов управления, основных выходных документов, а также составу методического обеспечения.

4. Организовать работу по ведению словаря терминов и определений в сфере обеспечения безопасности проектов, конструкторско-технологической документации, материального обеспечения, сохранности зданий и сооружений, охраны объектов, производства и сопровождения продукции и услуг предприятия, рекомендуемых для применения на предприятии в составе целевых и обеспечивающих автоматизированных систем предприятия.

5. Уточнить состав потенциально опасных объектов и процессов предприятия, списки потенциальных источников внутренних и внешних угроз обеспечения целостности и

организовать разработку паспортов безопасности основных структурных подразделений в соответствии с рекомендациями службы безопасности и внешних консультантов в сфере разработок методических, технических и программных средств обеспечения комплексной и информационно безопасности предприятий.

6. По результатам выполненных работ сформировать концепцию обеспечения комплексной безопасности предприятия, Политики обеспечения безопасности ключевых процессов предприятия, а также схемы взаимодействия подразделений при инициализации и обнаружению угроз безопасности и оперативного принятия решений на соответствующем уровне управления, включая, при необходимости, соглашения с органами государственной власти, местного самоуправления, силовыми структурами и др.

7. По результатам подготовленных в подразделениях и рабочих группах схем взаимодействия и исходных таблиц документооборота службы обеспечения безопасности предприятия организовать разработку форм документов, рекомендуемых для применения в подразделениях, службах и в целевых автоматизированных системах предприятия .

8. Провести анализ технологических процессов в основных подразделениях предприятия с позиций обеспечения безопасности функционирования и сформировать основные требования к обеспечению безопасности эксплуатации применяемых и перспективных средств автоматизации процессов и установок.

9. Организовать работы по оценке применяемых в подразделениях программных средств и их тестирование на соответствие и функциональную совместимость в соответствии с общими требованиями стандартов открытых информационных систем и рекомендациями по стандартизации Р 50.1.41-2002 «Информационные технологии. Руководство по проектированию профилей среды открытой системы организации пользователей». По результатам оценки оформить соответствующие акты, протоколы испытаний и подготовить решения по их применению в составе целевых АС предприятия.

10. В концепции ИСОКБП и проектах целевых АС обеспечения безопасности процессов подразделений рассмотреть базовые постановки задач принятия решений в условиях исходной неопределенности состояния объектов, процессов и вносимых возмущений.

11. Организовать работу по подготовке исходных данных для оценки эффективности применяемых и перспективных средств обеспечения безопасности в подразделениях и эксплуатируемых в них целевых и обеспечивающих АС, их влияние на основные ключевые показатели деятельности подразделений, уменьшение угроз физической, технологической, производственной, экологической и экономической безопасности, снижение рисков нарушения устойчивости функционирования и минимизации ущерба. Подготовить предложения по оценке допустимых затрат на реализацию ИСОКБП в бюджете предприятия.

12. Подготовить решения об организации на предприятии информационно-аналитической службы обеспечения комплексной безопасности и разработать положение (стандарт предприятия) о взаимодействии этой службы с другими службами предприятия.

13. Организовать работы по проектированию и комплектации службы специализированными программно-методическими и техническими средствами обеспечения мониторинга систем обеспечения безопасности подразделений, оперативного и статистического анализа инцидентов – угроз безопасности и планирования мероприятий по обеспечению безопасности предприятия.

14. Информационной службе предприятия, подразделению безопасности и отделу стандартизации организовать подготовку и утверждение информационно-методического материала (стандарта предприятия) «Состав комплекса средств интегрированной системы обеспечения комплексной безопасности предприятия».

Приложение А Основные термины в сфере обеспечения комплексной безопасности предприятий

Актуальность безошибочной информации – свойство безошибочной информации (в том числе подлежащей последующей функциональной обработке или полученной в результате обработки) отражать текущее состояние объектов и процессов прикладной области деятельности ОТС предприятия со степенью приближения, достаточной для получения на ее основе достоверной выходной информации в интересах конечного пользователя. Актуальность характеризует старение информации во времени.

Безопасность объекта – состояние объекта (компонентов ОТС, ИС, штатного средства и др.), в котором жизнь человека, его здоровье, собственность или окружающая среда не подвергаются опасности.

Безопасность информации – состояние защищенности информации от различных угроз.

Безошибочность информации – свойство информации не иметь явных или скрытых ошибок и/или искажений.

Достоверность информации – свойство информации отражать реальное или оцениваемое состояние объектов и процессов прикладной области ИС со степенью приближения, обеспечивающей эффективное использование этой информации согласно целевому назначению системы. Достоверность выходной информации определяется истинностью исходных данных, безошибочностью входной информации, корректностью обработки, безошибочностью при хранении и передаче информации и сохранением ее актуальности на момент использования.

Доступность информации - состояние информации, ее носителей и технологий обработки, при котором обеспечивается санкционированный доступ к ней и надежность представления требуемой информации.

Инициирующее событие – событие, которое может привести к реализации угрозы.

Информационная система – автоматизированная система (АС), результатом функционирования которой является представление выходной информации для последующего использования.

Качество выходной информации – совокупность свойств выходной информации, обусловливающих ее пригодность для последующего использования в соответствии с целевым назначением.

Качество функционирования АС – совокупность свойств, обусловливающих пригодность АС в соответствии с ее целевым назначением.

Конфиденциальность информации – свойство информации быть сохраненной в течение заданного объективного периода конфиденциальности от ознакомления лицами, к ней не допущенными, и/или от несанкционированного считывания техническими средствами.

Корректность обработки информации – свойство АС обеспечивать получение правильных согласованных результатов или эффектов обработки информации.

Надежность представления информации (реализации технологической операции) – свойство АС обеспечивать прием, автоматическую обработку запроса или команды и представление или принудительную выдачу выходной информации (реализацию технологической операции) при соблюдении эксплуатационных условий применения и технического обслуживания компонент АС.

Наработка – продолжительность или объем работы объекта.

Наработка на отказ – наработка объекта от окончания восстановления его работоспособного состояния после отказа до возникновения следующего отказа. Для ПС, технически не изнашиваемых, это время в процессе эксплуатации ИС до возникновения таких условий функционирования системы, в которых обработка соответствующей входной информации приводит к отказу ПС.

Нарушитель безопасности - субъект, случайно или преднамеренно совершивший действие, следствием которого является возникновение и/или реализация угроз нарушения безопасности предприятия .

Несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа, принятые в ИС.

Полнота выходной информации – свойство выходной информации отражать состояния всех требуемых объектов учета предметной области ИС. Слагается из полноты реализации функций АС, полноты ввода первоначальных информационных ресурсов и полноты оперативного отражения в в АС объектов учета.

Полнота оперативного отражения в АС объектов учета - свойство АС отражать требуемые состояния реально существующих объек-

тов учета, в том числе впервые появляющихся в процессе функционирования АС и подлежащих учету в системе согласно ее функционального назначения.

Риск – возможная опасность неудачи предпринимаемых действий.

Своевременность представления информации – свойство ИС обеспечивать представление запрашиваемой или выдаваемой принудительно выходной информации в заданные сроки, гарантирующие выполнение соответствующей функции согласно целевому назначению системы.

Угроза – условие и/или фактор, определяющие воздействие на состояние системы, ее объекты и/или среду функционирования, которые могут привести к недопустимому ущербу или неспособности выполнения системой своих функций с требуемым качеством.

Уровень целостности – диапазон значений показателей целостности объекта, необходимых для удержания системных рисков в допустимых границах.

Ущерб системе – вред, потери, урон, наносимые системе и способные привести к невозможности выполнения или ненадлежащему выполнению своих функций и недостижению целей системы без дополнительных затрат материальных, трудовых и/или иных видов ресурсов.

Функция амортизации – функция, которая в случае ее успешного выполнения способствует предотвращению возникновения инициирующего события конкретной угрозы или нейтрализации опасных последствий реализации угрозы.

Целостность информации – состояние информации, при котором обеспечивается достижение целей ее функционального применения в системе.

Целостность системы – состояние системы, при котором обеспечивается достижение целей ее функционирования.

Внутренний нарушитель – лицо или группа физических лиц, обладающих правом доступа на объект и к материальным ценностям в силу выполнения служебных или иных обязанностей, при этом внутренних нарушителей можно классифицировать тремя категориями:

Одиночный нарушитель – это лицо из числа персонала, имеющее определенные служебные или иные обязанности с ограниченным доступом и ограниченными возможностями хищений и порчи мате-

риальных ценностей, осуществляемых в мелких масштабах, но систематически с нарастанием массы нарушений.

Неорганизованный групповой нарушитель – это группа лиц при наличии случайного «сговора» с представителем среднего звена руководства предприятия или охраны. Связи между членами группы неустойчивы, случайны, как правило, прекращаются после свершенного одного или нескольких преступлений;

Организованная преступная группировка – группа лиц, как правило, включающая руководителей среднего и верхнего звена, получившая открытый доступ к материальным ценностям и имеющая постоянного лидера. Возможны масштабные регулярные хищения крупных партий материальных ценностей с использованием специальных каналов транспортировки, связи и фальсификации учетно-отчетной документации.

Приложение Б Анкета оценки целесообразности проекта создания ИСОКБП

Для предварительного анализа и формирования четкой, ясной, логичной и конкретной структуры проекта ИСОКБП рекомендуется в каждой группе, ответственной за разработку подсистем комплекса, сформулировать ответы на следующие вопросы. Материалы ответов передать в группу управления проектом (отдел безопасности) в отпечатанном виде и копии в виде файла с заданным именем.

1. Почему необходим проект создания (модификации) интегрированной системы обеспечения комплексной безопасности предприятия и какие приоритетные задачи должны быть реализованы в проекте с позиций обеспечения устойчивой работы предприятия:

Формулировка проблемной ситуации в сфере комплексной безопасности предприятия в целом и Вашего подразделения (службы)	
Приоритетные задачи в сфере обеспечения надежности и безопасности деятельности:	
На уровне предприятия	
На уровне подразделений Вашей службы	
На уровне отдельных ключевых рабочих мест (процессов)	
В смежных подразделениях	

2. Какова основная цель подсистемы обеспечения безопасности в Вашем подразделении, ключевых процессах и автоматизированных системах, которые применяются в вашей деятельности.

Формулировка целевых показателей подсистемы обеспечения безопасности	Связи с основными задачами предприятия, подразделения, службы

3. Кто выиграет в результате реализации проекта

Базовое подразделение	Подразделения смежники	Внешние клиенты (поставщики и потребители)	Учредители и коллектив предприятия

4. Изменения, каких ключевых показателей деятельности вашего подразделения следует ожидать в период реализации проекта (ближайшие 2-3 года).

Наименование групп и состав показателей	Единица измерения	Диапазон оценок сейчас	Тенденции изменения до 2010г.
1.Показатели результативности деятельности			
2. Показатели качества работ и услуг			
3. Показатели использования ресурсов			
4. Показатели эффективности использования ресурсов			
5. Показатели экономической эффективности			
6. Показатели зрелости процессов подразделения (предприятия)			
7. Прочие			

5. Какие результаты (их характер, качественные и количественные характеристики) необходимо получить для достижения целей проекта

Наименование направлений проекта	Наименование рекомендуемых материалов и объектов (процессов) для их апробации	Наличие прототипов, аналогов или других заделов
Упорядочение документооборота и процессов обеспечения безопасности деятельности		
Обеспечение своевременности актуальности, надежности и качества сбора данных о событиях-инцидентах угроз безопасности		
Совершенствование структур баз данных и информационного обес-		

Наименование направлений проекта	Наименование рекомендуемых материалов и объектов (процессов) для их апробации	Наличие прототипов, аналогов или других заделов
печения		
Совершенствование прикладных программ обработки данных, подготовки и принятия решений в подсистемах		
Совершенствование, аппаратуры средств обеспечения безопасности, операционной среды и средств электронных коммуникаций		
Обеспечение надежности функционирования компонентов АС/ИС (САПР, АСУ ТП, и др.)		

6. Какие мероприятия Вы считаете необходимыми для получения значимых результатов проекта

Наименование групп мероприятий	Рекомендации по исполнителям, технологиям выполнения работ
Организационные	
Технические	

7. Укажите факторы риска, которые могут помешать реализации проекта.

8. Укажите, какие процессы являются (или могут быть) непрофильными для Вашего подразделения, и какие из них возможно передать на аутсорсинг специализированным подразделениям и службам Предприятия или внешним предприятиям.

9. Какие меры следует предусмотреть для обеспечения эффективного взаимодействия подразделений безопасности и «услуг безопасности», переданных на аутсорсинг внешним подразделениям и специализированным предприятиям.

10. Какие ресурсы должны/могут быть использованы для реализации проекта

Наименование вида ресурсов	**Источники ресурсов: имеются в наличии необходима закупка, собственная разработка, разработка с участием внешних исполнителей**	**Оценка допустимых затрат (тыс. руб.) на комплектацию или приемлемый процент от оборота ресурсов**
Эталонные модели описания процессов и сценариев обеспечения безопасности целевых процессов предприятия и обеспечивающих систем		
Международные, национальные и корпоративные стандарты безопасности де-факто		
Нормативно-правовые и директивные документы различных категорий		
Лучшая практика: учет имеющегося опыта проектирования и эксплуатации средств обеспечения безопасности		
Технические и программные средства обеспечения безопасности, рекомендованные для применения в отрасли		
Персонал по эксплуатации систем безопасности		

Список использованных источников

1. Аншина М.Л. Архитектура и информационные технологии // Открытые системы, 2006, № 3

2. Батоврин В.К., Зиндер Е.З. Результаты и перспективы «тихой революции» архитектуры предприятия и сервисного подхода // Материалы практической конференции «Стандарты в проектах современных информационных систем» – М.: ФОСТАС, 2007

3. Буч Г., Рамбо Дж., Джекобсон А. Язык UML. Руководство пользователя: Пер. с англ. М.: ДМК Пресс; СПб.: Питер, 2004 – 432 с.

4. Васильев В.А., Герасимов Б.Н., Денисов В.Ф. Концепция и технологии программы реабилитации, стабилизации и устойчивого развития территорий // Сборник материалов Всероссийской научно-практической конф. «Проблемы экономического роста», ч.1. – Самара: Гос. экон. акад., 1999 – с. 122-130.

5. Васильев В.А., Денисов В.Ф. Концепция и стратегии развития Систем Электронного Взаимодействия Предприятий // Сборник трудов IV Всерос. практ. Конф. «Стандарты в проектах современных информационных систем», М.: ФОСТАС, изд-во «Открытые системы», 2004

6. Васильев В.А., Денисов В.Ф. Архитектура и тенденции развития Систем Электронного Взаимодействия Предприятий // Экономика Самарской области. Перспективы развития отраслей инфраструктурного комплекса (информ. аналитическое издание) – Самара: Правительство Самарской области, РАСО, 2005 – с.47-51.

7. Галатенко В.А. Стандарты информационной безопасности / Под редакцией академика РАН В.Б. Бетелина // М.: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2004 – 328 с.

8. Гуляев Ю.В., Олейников А.Я. Технология открытых систем - основное направление информационных технологий // Информационные технологии и вычислительные системы, №3, М.: ИТиВС, 1997 – стр.4 – 14

9. ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения»

10. ГОСТ Р 6.30-2003 «Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»

11. ГОСТ ИСО 15489-1:2007 «Управление документами. Общие требования»

12. Гуляев Ю.В., Олейников А.Я. Открытые системы: от принципов к технологии // Информационные технологии и вычислительные системы 2003, № 3 – с.4

13. Гэйн К., Сарсон Т. Структурный системный анализ: средства и методы. В двух частях. Пер. с англ. под ред. Козлинского А.В. – М.: Научно-техническое предприятие ЭЙТЕКС, 1993

14. Денисов В.Ф. Алгоритмы упорядочения функций и оценка сложности структур систем управления с активными элементами //Автоматизация научных исследований // сборник научных трудов: Куйб. авиац. института, 1984

15. Денисов В.Ф. Инновации и управление интеллектуальной собственностью предприятий и проектов // Двойные технологии как стратегический ресурс инновационной экономики: сборник докладов Международной научно-практической конференции (24-25 мая 2007 г.) – Тольятти: ТВТИ, 2007 – с. 60-63.

16. Денисов В.Ф. Методы и средства проектирования функциональных профилей систем управления в организационно-технических системах // Перспективные информационные технологии в научных исследованиях, проектировании и обучении – Самара: СГАУ, 2006

17. Денисов В.Ф. Практика использования типовых и индивидуальных ИТ-решений на российских предприятиях // Волга бизнес, Ассоциация экономического взаимодействия субъектов РФ “Большая Волга”, .2007, № 11

18. Денисов В.Ф., Дерябкин В.П., Корнев, Кулаков Г.А., Лычев В.Ф. Концепция комплекса средств информационных технологий управления предприятием // Сборник трудов IV Всерос. практ. Конф. "Стандарты в проектах современных информационных систем", М.: ФОСТАС, изд-во «Открытые системы» 2004

19. Денисов В.Ф., Прохоров С.А. Методология открытых информационных систем, проблемы и перспективы применения распределенных систем принятия решений в региональных системах управления // Перспективные информационные технологии в научных исследованиях, проектировании и обучении, Сборн. научн. Трудов – Самара: СГАУ, 2001 – с.24 – 32.

20. Денисов В.Ф., Чекин В.И. Опыт использования промышленных и государственных образовательных стандартов при разработке базовых профилей информационных систем // Сборник трудов III Всерос. практ. гонф. "Стандарты в проектах современных

информационных систем" М.: ФОСТАС, изд-во «Открытые системы» 2003

21. Денисов В.Ф. Методы и средства упорядочения функций и формирования профилей распределенных автоматизированных систем Предприятий // Первая международная конференция «Стандартизация информационных технологий и интероперабельность» (СИТОП-2007)- М.: ОИТ и ВС РАН, ФАИТ и др., с 50-56

22. Денисов В.Ф., Куделькин В.А. Архитектура и профили автоматизированных систем обеспечения деятельности предприятий инфраструктуры инновационного развития региона./ Труды второй международной конф. "Стандартизация информационных технологий и интероперабельность"(СИТОП-2008)- М.: ОИТ и ВС РАН, ФАИТ и др., с. 42-48

23. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты – К.: ДиаСофт, 2005 – 614 с.

24. Зильбербург Л.И., Молочник В.И., Яблочников Е.И. Реинжиниринг и автоматизация технологической подготовки производства в машиностроении. – СПб: Компьютербург, 2003 – 152 с.: ил.

25. Интеграция данных об изделии на основе ИПИ/CALS – технологий. Часть первая. М.:ГОУ «ГМЦ CALS-технологий», 2002

26. Калентьев А.А., Денисов В.Ф., Кузнецов С.Ю. Об использовании информационно-аналитических систем и технологий в выявлении и расследовании преступлений в сфере экономики // Актуальные проблемы квалификации и расследования преступлений в сфере экономики: Материалы Всерос. научн. практ. конф. – Самара: изд-во Самарск. гос. экон. акад., 2001 – с.136-142

27. Колчин А.Ф., Овсянников М.В., Стрекалов А.Ф., Сумароков С.В. Управление жизненным циклом продукции. – М.: Ахарсис, 2002 – 304 с.

28. Костогрызов А.И. и др. Методическое руководство по оценке качества функционирования информационных систем (в контексте стандарта ГОСТ РВ 51987 «ИТ. КСАС. Требования и показатели качества функционирования информационных систем. Общие положения»). М. – 2004 – 352с.

29. Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и

сертификация в области системной и программной инженерии. М. Изд. «Вооружение, политика, конверсия», 2004 – 395с.

30. Костогрызов А.И., Пьявченко А.Н., Харауз Дж., Бикчентаев Т.Т., Токарева М.А., Львов В.М. Термины и определения международных стандартов в области системной и программной инженерии – М: Мир, 2003 – 168 с.

31. Морис Питер У.Г. Нерелевантность управления проектами как профессиональной дисциплины. / Управление проектами, 2005г., № 3, с.4-19.

32. Норенков И.П., Кузьмик П.К. Информационная поддержка наукоемких изделий. CALS-технологии – М.: МГТУ им. Н.Э. Баумана, 2002 – 320 с., ил.

33. Основы построения открытых систем. Учебное пособие / М.: ИРЭ РАН, 1999

34. Полукеев О., Коваль Д. Моделирование бизнеса и архитектура информационной систем» // СУБД, 1995, № 4

35. Прохоров С.А. Прикладной анализ неэквидистантных временных рядов. - Самара: СГАУ, 2001 .375 с. ил

36. Прохоров С.А., Иващенко А.В., Графкин А.В. Автоматизированная система корреляционно – спектрального анализа случайных процессов. - Самара: СНЦ РАН, 2002, 286с.,ил..

37. Прикладной анализ случайных процессов. Под ред. Прохорова С.А./ СНЦ РАН, 2007 – 582 с

38. Прохоров С.А., Федосеев А.А., Иващенко А.В. Автоматизация комплексного управления безопасностью предприятия/ Самара: СНЦ РАН, 2008 – 55 с., ил.

39. Р 50.1.41-2002 «Информационные технологии. Руководство по проектированию профилей среды открытой системы организации пользователей».

40. Рамбо Дж., Якобсон А., Буч Г. UML: специальный справочник. – СПб.: Питер, 2002 – 656 с.: ил.

41. Резников Г.Я. Рациональный мониторинг процессов менеджмента качества на предприятиях – М.: Мир, 2005 – 284 с.

42. Резников Г.Я., Бабин С.А., Костогрызов А.И., Родионов В.Н. Количественная оценка защищенности автоматизированных систем от несанкционированного доступа // Информационные технологии в проектировании и производстве, № 1, 2004 с. 11-22

43. Руководство по проектированию профилей среды открытой системы. М.: «Янус», 2002

44. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и Ко», 2004. – 336 с.

45. Станкевич В.И. Замысел построения комплексной системы обеспечения безопасности территории, М: НИИ автоматической аппаратуры им. академика В.С. Семенихина.

46. СУБД ЛИНТЕР. Технический обзор- Воронеж:Научно-производственное предприятие РЕЛЭКСwww.relex.ru

47. Судов Е.В. Интегрированная информационная поддержка жизненного цикла машиностроительной продукции. Принципы. Технологии. Методы. Модели. – М.: МВМ, 2003 – 264 с.

48. Трубачев А.П. Разработка требований к безопасности продуктов и систем информационных технологий на основе ГОСТ Р ИСО/МЭК 15408-2002 – М.: ООО "Центр безопасности информации

49. Шлычков Е.И., Кушников В.А, Резников А.Ф. Модели и методы поиска данных по производственным ситуациям в информационно-измерительных и управляющих системах – Саратов: СГТУ, 2002 г - 112 с.

50. http://standards.ieee.org/reading/ieee/std_public/description/posix/1003.0-1995_desc.html

Сергей Антонович Прохоров
Андрей Алексеевич Федосеев
Владимир Федорович Денисов
Антон Владимирович Иващенко

Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения

Издательство Самарского научного центра РАН
Лицензия на издательскую деятельность
ЛР № 040910 от 10.08.98 г.

Подписано в печать
Формат 60x84 1/8 Бумага офсетная. Печать офсетная.
Гарнитура Times New Roman. Усл. печ. л. 12,4
Тираж 300 экз. Заказ №

Отпечатано в типографии АНО «Издательство СНЦ РАН»
443001, г. Самара, Студенческий переулок, 3а
тел.: 42-37-07