ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное образовательное бюджетное

учреждение высшего профессионального образования

«САНКТ-ПЕТЕРБУРГСКИЙ

ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ

им. проф. М. А. БОНЧ-БРУЕВИЧА»

А.Н.Губин

Современные методы проектирования информационных систем

Краткий конспект лекций

Раздел 5. Управление проектами ИС.

САНКТ-ПЕТЕРБУРГ

2015

Содержание

Раздел 5. Управление проектами ИС.

5.1. Жизненный цикл ИС.

Одним из базовых понятий методологии проектирования ИС является понятие жизненного цикла ее программного обеспечения (ЖЦ ПО). ЖЦ ПО - это непрерывный процесс, который начинается с момента принятия решения о необходимости его создания и заканчивается в момент его полного изъятия из эксплуатации.

Основным нормативным документом, регламентирующим ЖЦ ПО, является международный стандарт ISO/IEC 12207 [1] (ISO - International Organization of Standardization - Международная организация по стандартизации, IEC - International Electrotechnical Commission - Международная комиссия по электротехнике). Он определяет структуру ЖЦ, содержащую процессы, действия и задачи, которые должны быть выполнены во время создания ПО.

Структура ЖЦ ПО по стандарту ISO/IEC 12207 базируется на трех группах процессов:

- основные процессы ЖЦ ПО (приобретение, поставка, разработка, эксплуатация, сопровождение);
- вспомогательные процессы, обеспечивающие выполнение основных процессов (документирование, управление конфигурацией, обеспечение качества, верификация, аттестация, оценка, аудит, решение проблем);
- организационные процессы (управление проектами, создание инфраструктуры проекта, определение, оценка и улучшение самого ЖЦ, обучение).

Разработка включает в себя все работы по созданию ПО и его компонент в соответствии с заданными требованиями, включая оформление проектной и эксплуатационной документации, подготовку материалов, необходимых для проверки работоспособности и соответствующего качества программных продуктов, материалов, необходимых для организации обучения персонала и т.д. Разработка ПО включает в себя, как правило, анализ, проектирование и реализацию (программирование).

Эксплуатация включает в себя работы по внедрению компонентов ПО в эксплуатацию, в том числе конфигурирование базы данных и рабочих мест пользователей, обеспечение эксплуатационной документацией, проведение обучения персонала и т.д., и непосредственно эксплуатацию, в том числе локализацию проблем и устранение причин их возникновения, модификацию ПО в рамках установленного регламента, подготовку предложений по совершенствованию, развитию и модернизации системы.

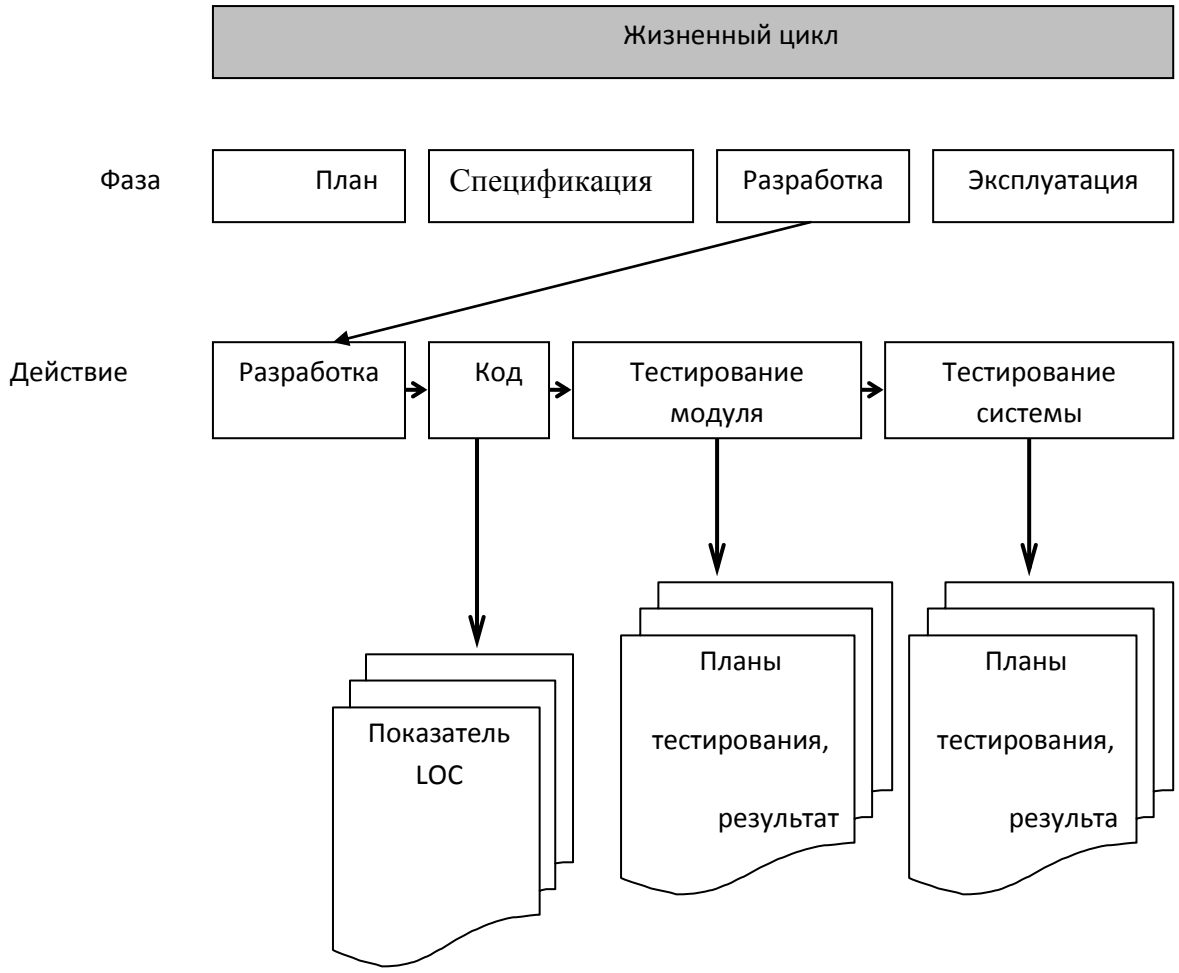

Рис. 5.1. Обобщенная схема жизненного цикла ПО

Управление проектом связано с вопросами планирования и организации работ, создания коллективов разработчиков и контроля за сроками и качеством выполняемых работ. Техническое и организационное обеспечение проекта включает выбор методов и инструментальных средств для реализации проекта, определение методов описания промежуточных состояний разработки, разработку методов и средств испытаний ПО, обучение персонала и т.п. Обеспечение качества проекта связано с проблемами верификации, проверки и тестирования ПО. Верификация - это процесс определения того, отвечает ли текущее состояние разработки, достигнутое на данном этапе, требованиям этого этапа. Проверка позволяет оценить соответствие параметров разработки с исходными требованиями. Проверка частично совпадает с тестированием, которое связано с идентификацией различий между действительными и ожидаемыми результатами и оценкой соответствия характеристик ПО исходным требованиям. В процессе реализации проекта

важное место занимают вопросы идентификации, описания и контроля конфигурации отдельных компонентов и всей системы в целом.

Управление конфигурацией является одним из вспомогательных процессов, поддерживающих основные процессы жизненного цикла ПО, прежде всего процессы разработки и сопровождения ПО. При создании проектов сложных ИС, состоящих из многих компонентов, каждый из которых может иметь разновидности или версии, возникает проблема учета их связей и функций, создания унифицированной структуры и обеспечения развития всей системы. Управление конфигурацией позволяет организовать, систематически учитывать и контролировать внесение изменений в ПО на всех стадиях ЖЦ. Общие принципы и рекомендации конфигурационного учета, планирования и управления конфигурациями ПО отражены в проекте стандарта ISO 12207-2 [1].

Каждый процесс характеризуется определенными задачами и методами их решения, исходными данными, полученными на предыдущем этапе, и результатами. Результатами анализа, в частности, являются функциональные модели, информационные модели и соответствующие им диаграммы. ЖЦ ПО носит итерационный характер: результаты очередного этапа часто вызывают изменения в проектных решениях, выработанных на более ранних этапах.
Стандарт ISO/IEC 12207 не предлагает конкретную модель ЖЦ и методы разработки ПО (под моделью ЖЦ понимается структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач, выполняемых на протяжении ЖЦ. Модель ЖЦ зависит от специфики ИС и специфики условий, в которых последняя создается и функционирует). Его регламенты являются общими для любых моделей ЖЦ, методологий и технологий разработки. Стандарт ISO/IEC 12207 описывает структуру процессов ЖЦ ПО, но не конкретизирует в деталях, как реализовать или выполнить действия и задачи, включенные в эти процессы.

К настоящему времени наибольшее распространение получили следующие две основные модели ЖЦ:

- каскадная модель (70-85 г.г.);
- спиральная модель (86-90 г.г.).

В изначально существовавших однородных ИС каждое приложение представляло собой единое целое. Для разработки такого типа приложений применялся каскадный способ. Его основной характеристикой является разбиение всей разработки на этапы, причем переход с одного этапа на следующий происходит только после того, как будет полностью завершена работа на текущем (рис. 5.2). Каждый этап завершается выпуском полного комплекта документации, достаточной для того, чтобы разработка могла быть продолжена другой командой разработчиков.

Положительные стороны применения каскадного подхода заключаются в следующем [2]:

- на каждом этапе формируется законченный набор проектной документации, отвечающий критериям полноты и согласованности;
- выполняемые в логичной последовательности этапы работ позволяют планировать сроки завершения всех работ и соответствующие затраты.

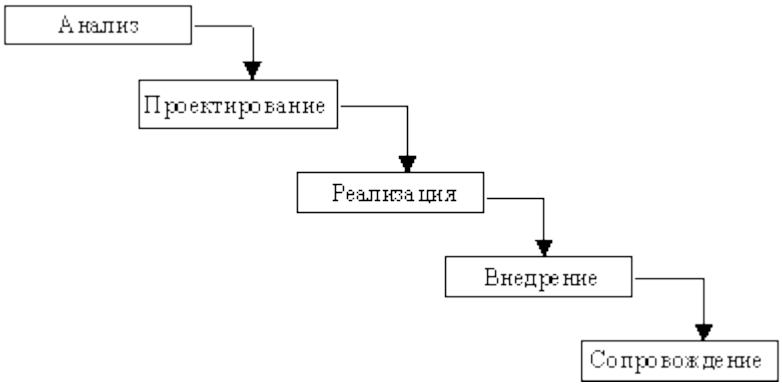

Рис. 5.2. Каскадная схема разработки ПО

Каскадный подход хорошо зарекомендовал себя при построении ИС, для которых в самом начале разработки можно достаточно точно и полно сформулировать все требования, с тем чтобы предоставить разработчикам свободу реализовать их как можно лучше с технической точки зрения. В эту категорию попадают сложные расчетные системы, системы реального времени и другие подобные задачи. Однако, в процессе использования этого подхода обнаружился ряд его недостатков, вызванных прежде всего тем, что реальный процесс создания ПО никогда полностью не укладывался в такую жесткую схему. В процессе создания ПО постоянно возникала потребность в возврате к предыдущим этапам и уточнении или пересмотре ранее принятых решений. В результате реальный процесс создания ПО принимал следующий вид (рис. 5.3):

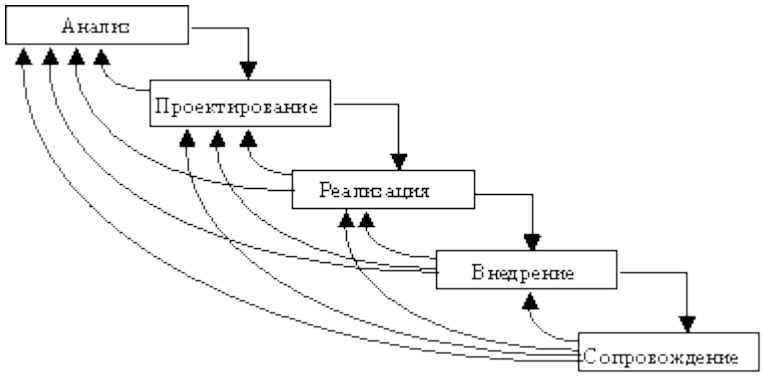

Рис. 5.3. Реальный процесс разработки ПО по каскадной схеме

Основным недостатком каскадного подхода является существенное запаздывание с получением результатов. Согласование результатов с пользователями производится только в точках, планируемых после завершения каждого этапа работ, требования к ИС "заморожены" в виде технического задания на все время ее создания. Таким образом, пользователи могут внести свои замечания только после того, как работа над системой будет полностью завершена. В случае неточного изложения требований или их изменения в течение длительного периода создания ПО, пользователи получают систему, не удовлетворяющую их потребностям. Модели (как функциональные, так и информационные) автоматизируемого объекта могут устареть одновременно с их утверждением.

Для преодоления перечисленных проблем была предложена спиральная модель ЖЦ (рис. 5.4), делающая упор на начальные этапы ЖЦ: анализ и проектирование. На этих этапах реализуемость технических решений проверяется путем создания прототипов. Каждый виток спирали соответствует созданию фрагмента или версии ПО, на нем уточняются цели и характеристики проекта, определяется его качество и планируются работы следующего витка спирали. Таким образом углубляются и последовательно конкретизируются детали проекта и в результате выбирается обоснованный вариант, который доводится до реализации.

Разработка итерациями отражает объективно существующий спиральный цикл создания системы. Неполное завершение работ на каждом этапе позволяет переходить на следующий этап, не дожидаясь полного завершения работы на текущем. При итеративном способе разработки недостающую работу можно будет выполнить на следующей итерации. Главная же задача - как можно быстрее показать пользователям системы работоспособный продукт, тем самым активизируя процесс уточнения и дополнения требований.

Основная проблема спирального цикла - определение момента перехода на следующий этап. Для ее решения необходимо ввести временные ограничения на каждый из этапов жизненного цикла. Переход осуществляется в соответствии с планом, даже если не вся запланированная работа закончена. План составляется на основе статистических данных, полученных в предыдущих проектах, и личного опыта разработчиков.

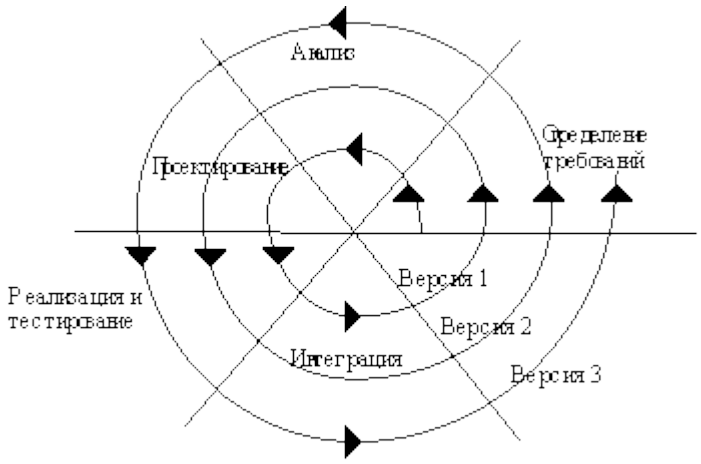

Рис 5.4. Спиральная модель ЖЦ

V-образная модель была создана с целью помочь работающей над проектом команде в планировании с обеспечением дальнейшей возможности тестирования системы. В этой модели особое значение придается действиям, направленным на верификацию и аттестацию продукта. Она демонстрирует, что тестирование продукта обсуждается, проектируется и планируется на ранних этапах жизненного цикла разработки. План испытания приемки заказчиком разрабатывается на этапе планирования, а компоновочного испытания системы - на фазах анализа, разработки проекта и т.д. Этот процесс разработки планов испытания обозначен пунктирной линией между прямоугольниками V-образной модели.

V-образная модель, показанная на рис. 5.5, была разработана как разновидность каскадной модели, а значит, унаследовала от нее такую же последовательную структуру. Каждая последующая фаза начинается по завершению получения результативных данных предыдущей фазы. Модель демонстрирует комплексный подход к определению фаз процесса разработки ПО. В ней подчеркнуты взаимосвязи, существующие между аналитическими фазами и фазами проектирования, которые предшествуют кодированию, после которого следуют фазы тестирования. Пунктирные линии означают, что эти фазы необходимо рассматривать параллельно.

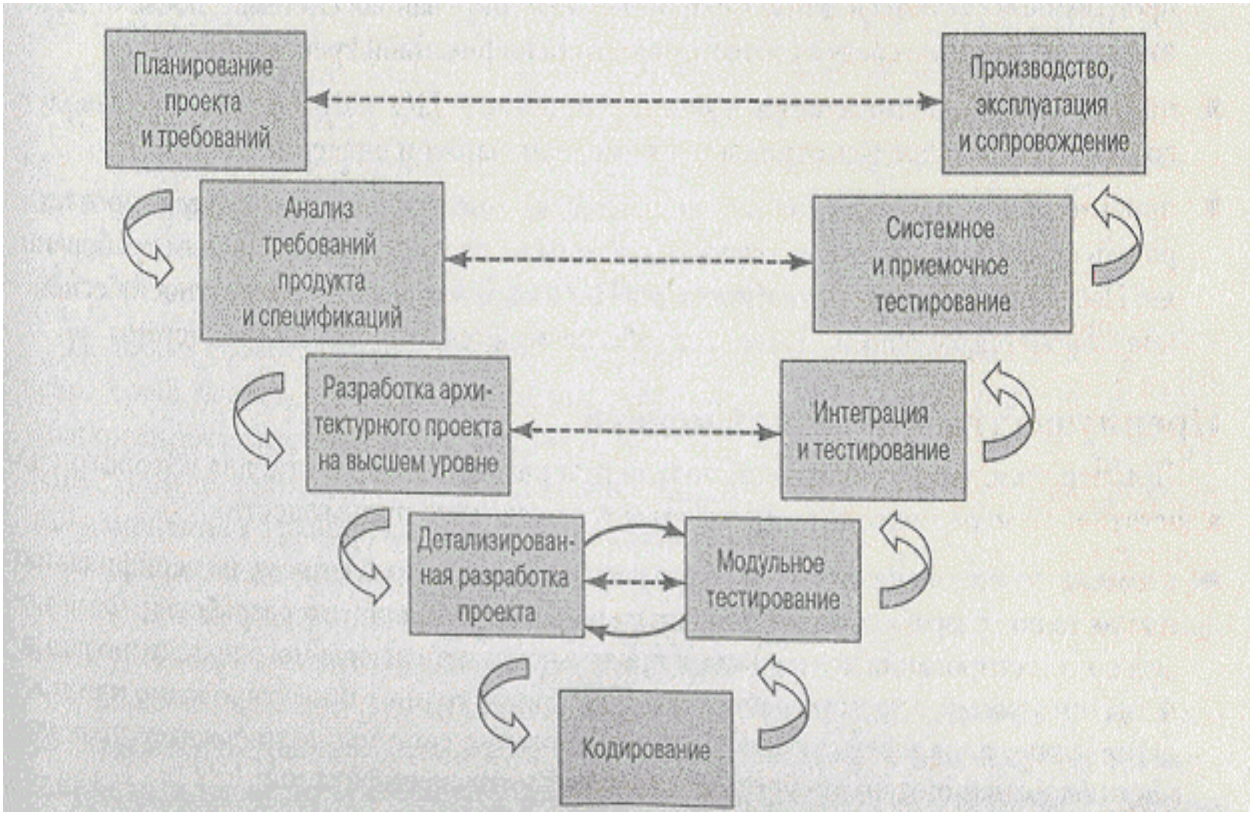

Рис 5.5. V-образная модель ЖЦ

Рассмотрим краткое описание каждой фазы V-образной модели, начиная от планирования проекта и требований вплоть до приемочных испытаний:

- планирование проекта и требований – определяются системные требования, а также то, каким образом будут распределены ресурсы организации с целью их соответствия поставленным требованиям. (в случае необходимости на этой фазе выполняется определение функций для аппаратного и программного обеспечения);
- анализ требований к продукту и его спецификации – анализ существующей на данный момент проблемы с ПО, завершается полной спецификацией ожидаемой внешней линии поведения создаваемой программной системы;
- архитектура или проектирование на высшем уровне – определяет, каким образом функции ПО должны применяться при реализации проекта;
- детализированная разработка проекта – определяет и документально обосновывает алгоритмы для каждого компонента, который был определен на фазе построения архитектуры. Эти алгоритмы в последствии будут преобразованы в код;

- разработка программного кода – выполняется преобразование алгоритмов, определенных на этапе детализированного проектирования, в готовое ПО;
- модульное тестирование – выполняется проверка каждого закодированного модуля на наличие ошибок;
- интеграция и тестирование – установка взаимосвязей между группами ранее поэлементно испытанных модулей с целью подтверждения того, что эти группы работают также хорошо, как и модули, испытанные независимо друг от друга на этапе поэлементного тестирования;
- системное и приемочное тестирование – выполняется проверка функционирования программной системы в целом (полностью интегрированная система), после помещения в ее аппаратную среду в соответствии со спецификацией требований к ПО;
- производство, эксплуатация и сопровождение – ПО запускается в производство. На этой фазе предусмотрены также модернизация и внесение поправок;
- приемочные испытания (на рис. не показаны) – позволяет пользователю протестировать функциональные возможности системы на соответствие исходным требованиям. После окончательного тестирования ПО и окружающее его аппаратное обеспечение становятся рабочими. После этого обеспечивается сопровождение системы.

Преимущества V-образной модели

При использовании V-образной модели при разработке проекта, для которого она в достаточной мере подходит, обеспечивается несколько преимуществ:

- в модели особое значение придается планированию, направленному на верификацию и аттестацию разрабатываемого продукта на ранних стадиях его разработки. Фаза модульного тестирования подтверждает правильность детализированного проектирования. Фазы интеграции и тестирования реализуют архитектурное проектирование или проектирование на высшем уровне. Фаза тестирования системы подтверждает правильность выполнения этапа требований к продукту и его спецификации;
- в модели предусмотрены аттестация и верификация всех внешних и внутренних полученных данных, а не только самого программного продукта;
- в V-образной модели определение требований выполняется перед разработкой проекта системы, а проектирование ПО - перед разработкой компонентов;

- модель определяет продукты, которые должны быть получены в результате процесса разработки, причем каждые полученные данные должны подвергаться тестированию;
- благодаря модели менеджеры проекта могут отслеживать ход процесса разработки, так как в данном случае вполне возможно воспользоваться временной шкалой, а завершение каждой фазы является контрольной точкой;
- модель проста в использовании (относительно проекта, для которого она является приемлемой).

Недостатки V-образной модели

При использовании V-образной модели в работе над проектом, для которого она не является в достаточной степени приемлемой, становятся очевидными ее недостатки:

- с ее помощью непросто справиться с параллельными событиями;
- в ней не учтены итерации между фазами;
- в модели не предусмотрено внесение требования динамических изменений на разных этапах жизненного цикла;
- тестирование требований в жизненном цикле происходит слишком поздно, вследствие чего невозможно внести изменения, не повлияв при этом на график выполнения проекта;
- в модель не входят действия, направленные на анализ рисков.

Графически модель зачастую изображается (как показано на рис. 5.5) без указания интегральных задач. Этот вопрос достаточно легко решается, он здесь упоминается только для того, чтобы напомнить читателю о том, что интегральные задачи имеют место при использовании всех моделей жизненного цикла.

С целью преодоления этих недостатков V-образную модель можно модифицировать, включив в нее итерационные циклы, предназначенные для разрешения изменений в требованиях за рамками фазы анализа.

Область применения V-образной модели

Подобно своей предшественнице, каскадной модели, V-образная модель лучше всего срабатывает тогда, когда вся информация о требованиях доступна заранее. Общераспространенная модификация V-образной модели, направленная на преодоление ее недостатков, включает в себя внесение итерационных циклов для разрешения изменения в требованиях за рамками фазы анализа.

Использование модели эффективно в том случае, когда доступными являются информация о методе реализации решения и технология, а персонал владеет необходимыми умениями и опытом в работе с данной технологией.

V-образная модель — это отличный выбор для систем, в которых требуется высокая надежность, таких как прикладные программы для наблюдения за пациентами в клиниках, а также встроенное ПО для устройств управления аварийными подушками безопасности в автомобилях.

5.2. Расширение и обновление ИС.

Эволюция информационных систем, связанная с характером развития технических средств обработки информации и достоинств информационных систем:

1-й этап (до конца 60-х годов) характеризуется проблемой обработки больших объемов данных в условиях ограниченных возможностей аппаратных средств.

2-й этап (до конца 70-х годов) связывается с распространением ЭВМ серии *1BM/360*. Проблема этого этапа - отставание программного обеспечения от уровня развития аппаратных средств. 1-й и 2-й этапы характеризуются довольно эффективной обработкой информации при выполнении рутинных операций с ориентацией на централизованное коллективное использование ресурсов вычислительных центров. Основным критерием оценки эффективности создаваемых информационных систем была разница между затраченными на разработку и сэкономленными в результате внедрения средствами. Основной проблемой на этом этапе была психологическая - плохое взаимодействие пользователей, для которых создавались информационные системы, и разработчиков из-за различия их взглядов и понимания решаемых проблем. Как следствие этой проблемы - создавались системы, которые пользователи плохо воспринимали и, несмотря на их достаточно большие возможности, не использовали в полной мере.

3-й этап (с начала 80-х годов) - компьютер становится инструментом непрофессионального пользователя, а информационные системы - средством поддержки принятия его решений. Проблемы - максимальное удовлетворение потребностей пользователя и создание соответствующего интерфейса работы в компьютерной среде. Изменился подход к созданию информационных систем - ориентация смещается в сторону индивидуального пользователя для поддержки принимаемых им решений. Пользователь заинтересован в проводимой разработке, налаживается контакт с разработчиком, возникает взаимопонимание обеих групп специалистов. На этом этапе используется как централизованная обработка данных, характерная для 1-го этапа, так и

децентрализованная, базирующаяся на решении локальных задач и работе с локальными базами данных на рабочем месте пользователя.

4-й этап (с начала 90-х годов) - создание современной технологии межорганизационных связей и информационных систем. Этот этап связан с понятием анализа стратегических преимуществ в бизнесе и основан на достижениях телекоммуникационной технологии распределенной обработки информации. Информационные системы имеют своей целью не просто увеличение эффективности обработки данных и помощь управленцу. Соответствующие информационные технологии должны помочь организации выстоять в конкурентной борьбе и получить преимущество. Проблемы этого этапа весьма многочисленны.

Наиболее существенными из них являются:

- выработка соглашений и установление стандартов, протоколов для компьютерной связи;
- организация доступа к стратегической информации;
- организация защиты и безопасности информации.
-

По принципу построения информационные технологии делятся на:

– функционально ориентированные технологии;
– объектно-ориентированные технологии.

При построении функционально ориентированных информационных технологий деятельность специалистов в рассматриваемой предметной области разбивается на множество иерархически подчиненных функций, выполняемых ими в процессе решения профессиональных задач. Для каждой функции разрабатывается технология ее реализации на рабочем месте пользователя, в рамках которой определяются исходные данные, процессы их преобразования в результатную информацию, а также выделяются информационные потоки, отражающие передачу данных между различными функциями.

Построение объектно-ориентированных информационных технологий заключается в проектировании системы в виде совокупности классов и объектов предметной области. При этом иерархический характер сложной системы отражается в виде иерархии классов, ее функционирование рассматривается как совокупность взаимодействующих во времени объектов, а конкретный процесс обработки информации формируется в виде последовательности взаимодействий. В качестве объектов могут выступать пользователи, программы, клиенты, документы, базы данных и т. д. Такой подход характерен тем, что используемые процедуры и данные заменяются понятием «объект», что позволяет динамически отражать поведение моделируемой предметной области в зависимости от возникающих событий.

По степени охвата задач управления выделяют следующие виды:
– информационные технологии обработки данных;
– информационные технологии управления;
– информационные технологии автоматизации офисной деятельности;
– информационные технологии поддержки принятия решений;
– информационные технологии экспертных систем.

Информационные технологии обработки данных предназначены для решения функциональных задач, по которым имеются необходимые входные данные и известны алгоритмы, а также стандартные процедуры их обработки. Эти технологии применяются в целях автоматизации некоторых рутинных, постоянно повторяющихся операций управленческой деятельности, что позволяет существенно повысить производительность труда персонала. Характерной особенностью этого класса технологий является их построение без пересмотра методологии и организации процессов управления

Целью информационной технологии управления является удовлетворение информационных потребностей сотрудников, имеющих дело с принятием решений. Эти технологии ориентированы на комплексное решение функциональных задач, формирование регулярной отчетности и работы в информационно-справочном режиме для подготовки управленческих решений. Они решают следующие задачи обработки данных:

оценка планируемого состояния объекта управления;
– оценка отклонений от планируемых состояний;
– выявление причин отклонений;
– анализ возможных решений и действий.

Информационные технологии автоматизации офисной деятельности направлены на организацию и поддержку коммуникационных процессов как внутри организации, так и с внешней средой на базе компьютерных сетей и других современных средств передачи и работы с информацией. В них реализуются типовые процедуры делопроизводства и контроля управления:

– обработка входящей и исходящей информации;
– сбор и последующее составление отчетности за определенные периоды времени в соответствии с различным критериями выбора;
– хранение поступившей информации и обеспечение быстрого доступа к информации и поиск необходимых данных.

Эти технологии предусматривают наличие интегрированных пакетов прикладных программ: текстовый процессор, табличный процессор, электронная почта, телеконференции, специализированные программы реализации электронного документооборота и т. д.

Информационные технологии поддержки принятия решений предусматривают широкое использование экономико-математических методов, моделей и пакетов прикладных программ для аналитической работы и формирования прогнозов, составления бизнес-планов и обоснованных выводов по изучаемым процессам и явлениям производственно-хозяйственной практики. Отличительными характеристиками этих технологий является ориентация на решение слабоформализованных задач, генерация возможных вариантов решений, их оценка, выбор и предоставление пользователю лучшего из них и анализ последствий принятого решения. Информационные технологии поддержки принятия решений могут использоваться на любом уровне управления и обеспечивают координацию лиц, принимающих решение, как на разных уровнях управления, так и на одном уровне.

Информационные технологии экспертных систем составляют основу автоматизации труда специалистов-аналитиков. Эти работники, кроме аналитических методов и моделей для исследования складывающихся в рыночных условиях ситуаций, могут использовать накопленный и сохраняемый в системе опыт оценки ситуаций, т. е. сведения, составляющие базу знаний в конкретной предметной области. Обработанные по определенным правилам такие сведения позволяют подготавливать обоснованные решения и вырабатывать стратегии управления и развития. Отличие информационных технологий экспертных систем от технологии поддержки принятия решения состоит в том, что они предлагают пользователю принять решение, превосходящее его возможности, и способны пояснять свои рассуждения в процессе получения решения.

5.3. Сопровождение, контроль эффективности и качества ИС.

CALS-технологии

Под этими технологиями понимается система непрерывного информационного сопровождения всего жизненного цикла производства продукции (процессов разработки, производства, сбыта, эксплуатации, сервисного обслуживания и утилизации производимой продукции)-от качества сырья до мониторинга рынка, включая аспекты производства.

До недавнего времени CALS-технологии были известны как технологии поддержки менеджмента сбыта продукции военного назначения.

Опыт высокотехнологичных фирм показывает, что применение. CALS-технологий дает сокращение времени проектирования при разработке нового изделия примерно на 50%, сокращение ошибок при передаче данных - на 98%, повышение показателей качества - на 80%. В конечном итоге это приводит к снижению себестоимости продукции и повышению ее конкурентоспособности.

Данная концепция возникла в 70-е годы при попытке создать единое информационное пространство для обмена данными между заказчиком, производителем и потребителем вооружений и военной техники в оборонном комплексе США. Дословно *CALS (Computer Aided Logistic Support)* - компьютерная поддержка поставок. Эта концепция базировалась на понятии жизненного цикла вооружений и военной техники и охватывала в основном их производство и эксплуатацию.

В настоящий момент эта концепция получила распространение в различных отраслях экономики и рассматривается более широко: *Continuous Acquisition and Life cycle Support* - непрерывная информационная поддержка всего жизненного цикла продукта, от маркетинга до утилизации.

Основная идея *CALS* состоит в совместном использовании информации заинтересованными сторонами на всех стадиях жизненного цикла продукта. Для обеспечения этого создаются единые информационные модели продукта, жизненного цикла продукта, бизнес-процессов на всех этапах жизненного цикла, производственной и эксплуатационной среды, стандартизируются способы доступа к информации, ее интерпретации, разрабатываются методы защиты информации и определяются юридические вопросы ее совместного использования. Это позволяет обеспечить эффективную информационную кооперацию всех участников жизненного цикла продукта, решать задачи анализа эффективности бизнес-процессов, повышения качества продукции, стандартизации, преобразования в электронную форму и обмена конструкторской документацией, электронных расчетов потребности в материалах; создания справочников по эксплуатации и т.п.

Информационная система организации необходима для предоставления нужной информации, в нужное время и в нужном месте. Вопрос оценки ее качества сводится к оценке качества порождаемого в ней информационного продукта с учетом затрат на его производство. В некотором смысле менеджеру безразлично, каким образом была получена требуемая информация, если она получена вовремя и затраты на ее получение находятся в пределах его представления о разумном их размере.

Поскольку информационная система организации, как правило, является ее частью, то кроме качества информационного продукта должен обсуждаться вопрос и о его качестве.

Информационный продукт, производящая его информационная система организации и применяемые в ней информационные технологии являются продукцией производственно-технического назначения.

Оценки общественные и личные:

1. Насколько удобно использовать - надежность, простота.

2. Насколько удобно эксплуатировать - понятность (учет требований пользователя, записанных в техническом задании; понимание назначения системы и ее функциональных элементов, понимание принятых ограничений).
3. Модифицируемость - возможность внесения изменений без значительных затрат времени и ресурсов.
4. Структурированность - разбиение на подсистемы и элементы.
5. Качество документации.
6. Точность - точность результатов расчета.
7. Завершенность - имеются все компоненты для выполнения заданных функций.

Очевидно, что оценка качества информационной системы- процесс неоднозначный и многокритериальный. Качественность информационной системы предполагает, что она будет обладать рядом свойств. Поэтому для практики полезнее определить эти свойства. Источники, размещенные в *Internet*, определяют следующий минимальный перечень требований к системе, претендующей на "звание" качественной информационной системы:

1. **Функциональная полнота системы:**

- выполнение международных стандартов управленческого учета - *MRP II, ERP, CSRP*;
- автоматизация в рамках системы решения задач:
  - планирования, бюджетирования, прогнозирования;
  - оперативного (управленческого) учета;
  - бухгалтерского учета;
  - статистического учета;
  - финансово-экономического анализа.
- формирование отчетов и ведение учета одновременно по российским и международным стандартам (IAS и CAAP);
- общими характеристиками функциональной полноты корпоративной информационной системы является *количество однократно учитываемых параметров деятельности предприятия*. Для КИС количество этих параметров должно быть примерно следующим:
  - количество учитываемых параметров 2000 - 10000 ;
  - количество таблиц баз данных 800 - 3000.

2. **Локализация информационной системы:**

- функциональная (учет особенностей российского законодательства и системы расчетов);
- лингвистическая (интерфейс, система помощи и документация на русском языке).

3. **Система должна обеспечивать надежную защиту информации.**

Для этого необходимы:

- парольная система разграничения доступа к данным и функциям;
- многоуровневая система защиты данных, включающая средства авторизации вводимой и корректируемой информации, регистрация времени ввода и, модификации данных, протокол удалений;
- программно-аппаратные средства шифровки данных, сертифицированные ФАПСИ.

4. **Реализация удаленного доступа и работы в распределенных сетях.**

5. **Наличие инструментальных средств адаптации и сопровождения системы:**

- изменение структуры и функций бизнес-процессов;
- изменение информационного пространства (изменение структуры, добавление или удаление БД, модификация полей таблиц, связей, индексов и т.п.);
- изменение интерфейсов ввода, просмотра и корректировки информации;
- изменение организационного и функционального наполнения рабочего места пользователя;
- генератор произвольных отчетов;
- генератор сложных хозяйственных операций;
- генератор форм (в том числе стандартизованных).

6. **Обеспечение обмена данными между ранее разработанными ИС и другими программными продуктами функционирующими на предприятии.**

7. **Возможность, консолидации информации:**

- на уровне предприятий - для объединения информации филиалов, дочерних компаний, предприятий, входящих в холдинг, и т.п.;

- на уровне отдельных задач;
- на уровне временных периодов - для выполнения анализа изменения.тех или иных показателей за период, превышающий отчетный.

8. **Наличие специальных средств анализа состояния системы в процессе эксплуатации:**

- анализ архитектуры баз данных;
- анализ, алгоритмов;
- анализ статистики количества обработанной информации (количество записей, документов, проводок; объем дисковой памяти);
- журнал выполненных операций;
- список работающих станций, внутрисистемная почта.

5.4. Мониторинг безопасности ИС.

Мониторинг состояния ИС проводится администраторами регулярно в соответствии с планом обслуживания ИС.

Мониторинг функционирования аппаратных компонентов

В соответствии с утвержденным регламентом должен систематически проводиться мониторинг работоспособности аппаратных компонентов ИС. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы ЛВС, активное сетевое оборудование) должны контролироваться постоянно в рамках работы дежурных администраторов.

Управление паролями пользователей

Пароль является одним из основных средств аутентификации в ИС Компании. Зарегистрировавшись на сервере под конкретным паролем, пользователь получает доступ к тем ресурсам, к которым ему предоставлены права доступа в соответствии с выполняемыми функциями. Узнав имя пользователя и его пароль, злоумышленник может выполнять действия и просматривать информационные ресурсы от имени легального пользователя. В данной ситуации возможны как финансовые потери от действий злоумышленника, так и потеря доверия со стороны клиентов и партнеров Компании.

Возможно использование двух схем выработки паролей:

1. Пароли генерируются для каждого пользователя с использованием специального ПО.
2. Каждый пользователь самостоятельно выбирает для себя пароль.

В первой схеме, с использованием специализированного ПО, гарантируется необходимая стойкость пароля (длина, уникальность, необходимая мощность алфавита, невозможность подбора методом полного перебора и т.д.). Но возникают трудности для пользователей с запоминанием сгенерированных паролей.

Кроме того, используя данную схему, необходимо решить ряд организационных вопросов:

- Процедуру выдачи паролей пользователям;
- Способ хранения носителя с выданным паролем (например, индивидуальный сейф в охраняемом помещении);
- Контроль использования носителя и его дальнейшее уничтожение после смены пароля.

Данную схему целесообразно применять при наличии отлаженных механизмов режимного делопроизводства.

Вторая схема лишена перечисленных недостатков, но при ее реализации не гарантирована необходимая стойкость пароля (по статистике около 80% пользователей используют очень простые, легко ассоциируемые с самим пользователем пароли).

Существуют общие правила работы с паролями, обязательные для использования в ИС Компании.

1. Идентификаторы пользователей и их пароли должны быть уникальными для каждого пользователя.
2. Пароли должны состоять как минимум из 7 символов.
3. Пароль должен быть трудноугадываемым. Пароль не должен совпадать с именем пользователя. Паролем не может быть слово на русском или иностранном языках. В пароле не должна в явном виде использоваться информация, ассоциируемая с владельцем пароля (имя, фамилия, дата рождения, номер автомобиля, имена близких родственников и т.п.).
4. Пароли должны держаться в секрете, то есть не должны сообщаться другим людям, не должны вставляться в тексты программ, и не должны записываться на бумаге либо на обратной стороне клавиатуры и т.п.
5. Пароли должны меняться каждые 90 дней (или через другой период, определенный ответственным лицом). Большинство систем могут заставить принудительно поменять пароль через определенное время и

предотвратить использование того же самого или легко угадываемого пароля. Для привилегированных пользователей необходима более частая смена паролей (через каждые 45 дней).

6. Пользователи и администраторы ИС обязаны изменять пароль каждый раз, когда есть подозрение о его компрометации.
7. Средства защиты должны быть сконфигурированы таким образом, что бы учетные записи пользователей блокировались после 3 неудачных попыток входа в систему. Все случаи неверно введенных паролей должны быть записаны в системный журнал, используемый для анализа попыток проникновения в систему.
8. При успешном входе в систему должны отображаться дата и время последнего входа в систему.
9. Сеансы пользователей с сервером должны блокироваться после 15-минутной неактивности пользователя (или по истечении другого указанного периода времени). Для возобновления сеанса должен снова требоваться ввод пароля.
10. Учетные записи пользователей должны блокироваться после определенного времени неиспользования.
11. Должно производиться периодическое тестирование специальными программными средствами (взломщиками паролей) процедуры выбора паролей для случайно выбранных пользователей. Целью тестирования является выявление легко угадываемых паролей.
12. Не следует включать пароли в сценарии для автоматического входа в системы (например, в макросы).
13. Рекомендуется использовать однонаправленные хэш-функции и алгоритмы шифрования для защиты пользовательских паролей, хранимых в системе.

Пользователи, в результате действий (ненадлежащим образом выбран пароль) которых произошло раскрытие критичной информации, несут ответственность в соответствии с правилами, установленными в Компании.

Контроль за выполнением настоящих рекомендаций возлагается на администратора безопасности.

Для усиления политики управления паролями и контроля надежности пользовательских паролей администратору безопасности необходимо:

- Установить программу, осуществляющую проверку пользовательских паролей на очевидность с целью выявления слабых паролей, которые легко угадать, или дешифровать с помощью специализированных программных средств (взломщиков паролей), или использовать встроенные системные средства;

- Периодически использовать взломщики паролей для выявления слабых паролей и принуждения пользователей к их смене.

Для выполнения своих функциональных обязанностей по управлению паролями и контролю надежности пользовательских паролей администратору безопасности должны быть предоставлены соответствующие полномочия, позволяющие осуществлять доступ к системным файлам, содержащим пользовательские пароли.

Мониторинг целостности и анализ защищенности

Мониторинг целостности и анализ защищенности ИС включает в себя следующее:

- проверка контрольных сумм и цифровых подписей файлов,
- контроль изменения параметров системного и прикладного ПО,
- проверка прав доступа, связей и размеров файлов и каталогов,
- регистрация фактов добавления и удаления файлов в контролируемых каталогах,
- обнаружение дубликатов идентификаторов пользователей и групп,
- контроль правильности системных конфигурационных файлов.

Активный аудит

Для предупреждения и своевременного выявления попыток несанкционированного входа в систему используются средства активного аудита, которые осуществляют:

- Фиксацию неудачных попыток входа в систему в системном журнале;
- Протоколирование работы сетевых сервисов;
- Выявление фактов сканирования диапазона сетевых портов;
- Выявление различных видов локальных и сетевых атак на ресурсы ИС;
- Оповещение администратора безопасности и другие действия по реагированию на несанкционированные действия в отношении ресурсов ИС со стороны пользователей ИС и внешних нарушителей.

Мониторинг производительности

Косвенной причиной уменьшения производительности системы может являться нарушение безопасности. Мониторинг производительности проводится регулярно в соответствии с планом.

Каждый компонент сети должен иметь контрольно-измерительные средства. Если они отсутствуют, обеспечить бесперебойную работу или даже выяснить причину снижения производительности невозможно.

Если приложение в сети работает недостаточно производительно, то в первую очередь необходимо выявить причину проблемы.

При определении причины недостаточной производительности первоначально нужно выяснить, является ли она постоянной или временной. Например, всегда ли приложение работает непроизводительно или только в период пиковой нагрузки. Если верно первое, то имеет место статическое снижение производительности, если второе – динамическое.

Для того чтобы собрать требуемую информацию, необходимо встретиться с пользователями и выяснить природу возникновения проблемы.

Как только определено, является ли падение производительности статическим или динамическим, можно начинать поиск возможных причин. Динамическое снижение производительности обычно указывает на недостаток ресурсов, к примеру, пропускной способности разделяемой сети или недостаточной производительности процессора хоста, и проблемы, с ними связанные, возникают, как правило, в разделяемых областях инфраструктуры: в сети или на серверах. Сетевые проблемы проявляются в сегментах сети или, что происходит заметно чаще, на промежуточных маршрутизаторах, коммутаторах или шлюзах. Серверные проблемы связаны с нехваткой таких ресурсов, как емкость памяти, мощность процессора или скорость обмена с диском. Динамическое падение производительности происходит в тех случаях, когда потребности в ресурсах превосходят возможности имеющихся ресурсов.

Правильное размещение в сети контрольно-измерительных средств позволит диагностировать и установить причину возникновения динамического снижения производительности, поскольку оно связано с очевидным недостатком ресурсов.

Статическое снижение производительности устранить сложнее, так как очевидных ограничений на ресурсы в этом случае нет. Данные проблемы вызваны в основном недостатками архитектуры. К примеру, сеть не имеет необходимой пропускной способности, клиенты и серверы обладают недостаточной памятью, мощности процессора не хватает, а скорость внутренней шины обмена с диском низка. Неправильное размещение приложений и чрезмерный объем кода графического интерфейса, элементов данных и исполняемых модулей также относятся к изъянам архитектуры.

Зачастую для определения источника статических или архитектурных недостатков необходим сложный анализ, поскольку установленные датчики не всегда правильно указывают причину низкой производительности. В частности, с одной стороны, мониторы производительности, отслеживающие сетевой трафик или загрузку процессора на сервере, не обнаруживают перегрузки, а с другой – приложение не отвечает требованиям пользователей к производительности. Приложение, например, может производить слишком большое число обменов по сети в рамках одной транзакции или чересчур много небольших транзакций, связанных с чтением/записью на диск.

Как только будет определено, в чем состоит проблема, необходимо решить, производить ли модернизацию оборудования или придется изменить архитектуру приложения.

Классификация причин снижения производительности приведена ниже.

Проблемы производительности:

- **Динамические**
    - Сеть

    1. Узкие места в маршрутизации
    2. Недостаточная временная пропускная способность

    - Сервер

    1. Процессор
    2. Диск
    3. Память

- **Статические**
    - Приложение

    1. Код графического интерфейса
    2. Избыточность элементов данных
    3. Неоптимальный исполняемый модуль

    - Клиент

    1. Память
    2. Диск
    3. Процессор
    4. Шина

    - Сервер

    1. Память
    2. Шина
    3. Процессор
    4. Диск

    - Сеть

1. Узкие места в маршрутизации
2. Недостаточная пропускная способность

Синхронизация системных часов

Синхронизация системных часов производится регулярно при помощи соответствующих сетевых программных средств (программных агентов) и является важным условием правильного функционирования системы аутентификации пользователей сети и обеспечения точности записей журналов аудита.

Антивирусные мероприятия

Целесообразно использовать антивирусные программные средства для защиты от вирусов рабочих станций, а также серверов:

- Антивирусные сканеры, тестирующие и восстанавливающие файлы и загрузочные секторы дисков, дезактивирующие резидентные части вирусов и тестирующие файлы и системные секторы на наличие неизвестных вирусов;
- Резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- Утилиты для обнаружения и анализа новых вирусов (дисассемблеры, редакторы ОП, трассировщики прерываний и т.п.).

План проведения антивирусных мероприятий состоит из трех основных частей:

1. Предотвращение – мероприятия и правила, позволяющие предотвратить заражение вирусами;
2. Обнаружение – мероприятия, позволяющие определить, что данный выполняемый файл, загрузочная запись или файл данных содержит вирус;
3. Удаление – удаление вируса из зараженной компьютерной системы может потребовать удаления вируса из зараженного файла, удаления файлов или переинсталляции ОС.

Вероятность заражения вирусами пропорциональна частоте появления новых файлов или приложений на компьютере. Изменения в конфигурации для работы в Интернете, для чтения электронной почты и загрузка файлов из внешних источников – все это увеличивает риск заражения вирусами.

Вирусы обычно появляются в системе из-за действий пользователя (например, установки приложения, получения файла по FTP, чтения

электронного письма и т.п.). Поэтому в плане проведения антивирусных мероприятий особое внимание обращено на ограничения по загрузке потенциально зараженных программ и файлов.

Чем выше критичность приложения, обрабатываемого на компьютере, или данных, хранящихся в нем, тем более строгие мероприятия необходимо проводить для предотвращения заражения вирусами.

Все серверы и АРМ пользователей в соответствии с данным критерием (критичность информации) разбиваются на три группы:

1. К группе низкого риска относятся СВТ, на которых обрабатывается и хранится информация, не являющаяся критичной. Кроме того, поток входящих данных минимален либо отсутствует;
2. К группе среднего риска относятся СВТ, на которых обрабатывается и хранится информация, не являющаяся критичной. Поток входящих и исходящих данных средней интенсивности;
3. К группе высокого риска относятся все СВТ, на которых обрабатывается и хранится информация, являющаяся критичной. Кроме того, к данной группе относятся СВТ, обрабатывающие некритичную информацию, но с высоким трафиком входящих и исходящих данных.

Результаты проведенной классификации СВТ оформляются документально и утверждаются руководителем ОИБ.

Низкий риск

Мероприятия по антивирусной защите СВТ с низким риском содержат шаги по доведению до пользователей их обязанностей по регулярной проверке АРМ на наличие вирусов.

Предотвращение

Пользователи должны знать о возможных путях заражения вирусами и о том, как использовать антивирусные средства.

Обнаружение

Антивирусные средства должны использоваться для еженедельной проверки на вирусы. Ведение журналов проверки СВТ на наличие вирусов не является необходимым.

Сотрудники должны информировать администратора ЛВС о любом обнаруженном вирусе, изменении конфигурации или необычном поведении

компьютера или программы. После получения информации об обнаружении вируса администратор должен информировать всех пользователей, имеющих доступ к программам или файлам данных, которые могли быть заражены вирусом, что, возможно, вирус заразил их системы. Пользователям должен быть сообщен порядок определения, заражена ли их система, и удаления вируса из системы. Пользователи должны сообщить о результатах проверки на вирусы и удаления вируса администратору.

Администратор обязан доложить о факте заражения вирусом своему непосредственному начальнику.

Удаление

Любая система, которая подозревается в заражении вирусом, должна быть немедленно отключена от сети. Система не должна подключаться к сети до тех пор, пока администратор не удостоверится в том, что вирус удален.

Средний риск

Мероприятия по антивирусной защите СВТ со средним риском предполагают проведение более частых проверок на вирусы, а также использование антивирусных средств для проверки серверов, связанных с данным СВТ, и электронной почты.

Предотвращение

Программы, инсталлированные на СВТ, должны устанавливаться только администратором (который проверяет их на вирусы и тестирует).

На файловые сервера должны быть установлены антивирусные программы для ограничения распространения вирусов в сети. Должна производиться ежедневная проверка всех программ и файлов данных на серверах на наличие вирусов. АРМы пользователей должны иметь резидентные антивирусные программы, сконфигурированные так, что все файлы проверяются на вирусы при загрузке на компьютер. Все приходящие электронные письма должны проверяться на вирусы. Запрещается запускать программы и открывать файлы с помощью приложений, уязвимых к макровирусам, до проведения проверки этих файлов на вирусы.

С сотрудниками компании должны проводиться периодические семинары, содержащие следующую информацию о риске заражения вирусами:

Антивирусные программы могут обнаружить только те вирусы, которые уже были кем-то обнаружены раньше. Постоянно разрабатываются новые, более изощренные вирусы. Антивирусные программы должны регулярно (еженедельно) обновляться для того, чтобы можно было обнаружить самые

новые вирусы. Важно сообщать администратору о любом необычном поведении компьютера или приложений. Важно сразу же отсоединить компьютер, который заражен или подозревается в заражении, от сети, чтобы уменьшить риск распространения вируса.

Обнаружение

Должны использоваться лицензионные антивирусные программы для ежедневных проверок на вирусы. Антивирусные программы (базы сигнатур) должны обновляться каждую неделю. Все программы или данные, импортируемые в компьютер (с дискет, электронной почты и т.д.), должны перед использованием проверяться на вирусы.

Должны вестись журналы проверки АРМ на наличие вирусов. Данные журналы должны просматриваться администратором.

Сотрудники должны информировать администратора об обнаруженных вирусах, изменениях в конфигурации или странном поведении компьютера или приложений.

При получении информации о заражении вирусом администратор должен информировать всех пользователей, имеющих доступ к программам и файлам данных, которые могли быть заражены вирусом, что вирус, возможно, заразил их системы. Пользователям должен быть сообщен порядок определения, заражена ли их система, и удаления вируса из системы. Пользователи должны сообщить о результатах проверки на вирусы и удаления вируса администратору.

Администратор обязан доложить о факте заражения вирусом своему непосредственному начальнику.

Удаление

Любая система, которая подозревается в заражении вирусом, должна быть немедленно отключена от сети. Система не должна подключаться к сети до тех пор, пока администратор не удостоверится в том, что вирус удален.

Высокий риск

Системы с высоким уровнем риска содержат данные и приложения, которые являются критическими для деятельности Компании. Заражение вирусами может вызвать значительные потери времени, данных и нанести ущерб репутации Компании. Из-за заражения может пострадать большое число компьютеров. Следует принять все возможные меры для предотвращения заражения вирусами.

Предотвращение

Установка ПО на серверы и АРМ пользователей производится непосредственно администраторами. К эксплуатации в ИС допускается только лицензионное ПО, приобретенное непосредственно у производителя либо его официального представителя. Перед установкой ПО должно пройти тестовые испытания на стенде. Конфигурация ПО на АРМ пользователей должна проверяться еженедельно на предмет выявления программ, самостоятельно установленных пользователями.

С целью ограничения риска заражения ПО должно устанавливаться только с разрешенных внутренних серверов либо с лицензионных носителей. Запрещено загружать ПО из Интернета.

На серверах должны быть установлены антивирусные средства для предотвращения заражения и распространения вирусов в сети. Должна производиться ежедневная проверка всех программ и файлов данных на серверах на наличие вирусов.

На АРМ пользователей должны устанавливаться резидентные антивирусные средства, сконфигурированные так, что все файлы проверяются на вирусы при загрузке на компьютер. Запрещается запускать программы и открывать файлы с помощью приложений, уязвимых к макровирусам, до проведения проверки этих файлов на вирусы.

Все приходящие письма и файлы, полученные из сети, должны проверяться на вирусы при получении. Рекомендуется использование антивирусных средств, установленных на межсетевых экранах. Данные средства способны выполнять "на лету" проверку всего входящего и исходящего трафика сегмента сети.

С сотрудниками компании должны проводиться периодические семинары, содержащие следующую информацию о риске заражения вирусами:

Антивирусные программы могут обнаружить только те вирусы, которые уже были кем-то обнаружены ранее. Постоянно разрабатываются новые, более изощренные вирусы. Антивирусные программы должны регулярно (ежемесячно) обновляться для того, чтобы можно было обнаружить самые новые вирусы. Важно сообщать администратору о любом необычном поведении компьютера или приложений. Важно сразу же отсоединить компьютер, который заражен или подозревается в заражении, от сети, чтобы уменьшить риск распространения вируса.

Невыполнение данных мероприятий должно вести к наказанию сотрудника согласно правилам, принятым в Компании.

Обнаружение

Должны использоваться лицензионные антивирусные программы для ежедневных проверок на вирусы. Антивирусные программы (базы сигнатур) должны обновляться каждую неделю. Все данные, импортируемые в

компьютер (с дискет, электронной почты и т.д.), должны перед использованием проверяться на вирусы.

Должны вестись журналы проверки АРМ пользователей на наличие вирусов. Данные журналы должны просматриваться и анализироваться администратором.

Проверка серверов должна производиться каждый день в обязательном порядке. Результаты проверок должны протоколироваться, автоматически собираться и анализироваться администраторами.

Сотрудники обязаны информировать администратора об обнаруженных вирусах, изменениях в конфигурации или странном поведении компьютера или приложений.

При получении информации о заражении вирусом администратор должен информировать всех пользователей, имеющих доступ к программам и файлам данных, которые могли быть заражены вирусом, что вирус, возможно, заразил их системы. Пользователям должен быть сообщен порядок определения, заражена ли их система, и удаления вируса из системы.

Администратор обязан доложить о факте заражения вирусом своему непосредственному начальнику.

Удаление

Любая система, которая подозревается в заражении вирусом, должна быть немедленно отключена от сети. Система не должна подключаться к сети до тех пор, пока администратор не удостоверится в удалении вируса. Для удаления вируса должны использоваться только лицензионные программы, приобретенные непосредственно у разработчика либо его официального представителя.

Если используемые антивирусные средства не могут удалить вирус либо предупреждают о некорректном восстановлении поврежденной информации, то необходимо обратиться по телефону либо электронной почте к фирме-изготовителю с целью получения обновленной версии программы-антивируса. Также возможен вариант вызова специалиста из фирмы, оказывающей экстренную помощь при заражении компьютерными вирусами.

В крайнем случае допускается уничтожение вируса путем форматирования носителя информации (предварительно загрузившись с "чистой" операционной системы), с дальнейшим восстановлением программного обеспечения и данных с резервных копий.

После восстановления СВТ должно быть повторно проверено на наличие вирусов.

Каждый случай заражения сервера или АРМ пользователя должен тщательным образом анализироваться. На основе выводов должны быть сформулированы предложения и внесены изменения в технологическую цепочку обработки критичной информации.

Пользователи ИС, в результате действий которых произошло искажение (уничтожение) критичной информации, подлежат наказанию в соответствии с правилами, принятыми в Компании.

Мониторинг внешних источников информации

Мониторинг внешних источников информации производится администратором безопасности регулярно в соответствии с планом и включает в себя получение информации об уязвимостях используемых ОС и МЭ, выпуске пакетов программных коррекций и других вопросах безопасности.

Аудит безопасности

Аудит безопасности производится администратором аудита регулярно, а также в ситуациях, требующих проведения расследования инцидента, связанного с нарушением информационной безопасности ИС.

Обзоры безопасности

Обзоры безопасности проводятся с целью проверки соответствия текущего состояния ИС тому уровню защищенности, который удовлетворяет требованиям политики безопасности. Выделяют три уровня защищенности: низкий, средний и высокий. Для каждого из этих уровней описывается состояние системы в терминах неизменности системной конфигурации и целостности системных файлов (таблиц), системных программ, СУБД, приложений, сетевых сервисов и системных устройств. Обзоры безопасности проводятся с целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующим специально составленному списку проверки (например, шаблоны значений параметров настройки ОС). Для проведения проверок и составления отчетов используются автоматизированные программные средства администратора безопасности, работающие либо в интерактивном, либо в фоновом режиме. Обзоры безопасности, как минимум, должны включать следующие пункты:

- Отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских системных окружений;
- Выявление троянских программ при помощи антивирусных средств и сетевых сканеров;

- Проверка содержимого конфигурационных файлов ОС на соответствие спискам проверки;
- Выявление изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
- Проверка прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- Проверка правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- Проверка корректности конфигурации системных устройств и активного сетевого оборудования (мостов, маршрутизаторов, концентраторов и межсетевых экранов).

Активное тестирование системы защиты

Активное тестирование – тестирование механизмов контроля доступа путем осуществления попыток проникновения в систему и других видов атак (с помощью автоматического инструментария или вручную).

Пассивное тестирование системы защиты

Пассивное тестирование механизмов контроля доступа, в отличие от активного, осуществляется путем анализа конфигурационных файлов ОС, а также МЭ и прочих СЗИ НСД. Информация об известных уязвимостях извлекается из документации и внешних источников информации. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний, т.е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

Контроль внесения изменений в системное программное обеспечение и установки программных коррекций

Внесение изменений производится с уведомлением каждого, кого касается предлагаемое изменение. Контроль внесения изменений осуществляется периодическими проверками состава и конфигурации СВТ и сравнения его с данными, указанными в паспорте на СВТ (ИС).

Планирование конфигурации подсистемы аудита безопасности

Планирование конфигурации подсистемы аудита безопасности включает в себя следующие шаги:

- Спланировать хранение журналов аудита:

    1. Определить для каждой контролируемой системы классы событий, которые будут регистрироваться.
    2. Определить, какие события к какому классу относятся.
    3. Определить, какое количество информации аудита необходимо генерировать для каждой контролируемой системы. Найти компромисс между требованиями обеспечения безопасности и количеством доступного для аудита дискового пространства.
    4. Определить, какие компьютеры будут выполнять роль серверов аудита и какие будут клиентами для этих серверов.
    5. Определить имена и расположение файловых систем для аудита.
    6. Спланировать использование файловых систем на серверах аудита.

- Определить, какие действия и для каких пользователей будут отслеживаться:

    1. Определить, для каких классов событий желательно осуществлять аудит.
    2. Определить, какие пользователи должны быть подвергнуты более тщательному наблюдению.
    3. Определить, какое минимальное количество дискового пространства должно оставаться на диске, прежде чем посылать предупреждение администратору аудита.
    4. Определить конфигурацию подсистемы аудита безопасности.
    5. Определить стратегию аудита - стратегия аудита определяет различные детали, связанные с аудитом, например, следует ли включать в записи аудита их порядковые номера или данные о группе пользователя, а также следует ли регистрировать информацию об окружении и аргументах командной строки вызываемых программ.
    6. Определить стратегию в случае переполнения журнала аудита - необходимо решить следует ли, в случае переполнения журнала аудита, запрещать выполнение подконтрольных действий или позволить системе продолжать функционирование и просто регистрировать число потерянных записей аудита.

Анализ журналов аудита

Анализ больших объемов информации, содержащейся в журналах системного аудита, осуществляется с использованием специализированного программного инструментария.

В качестве исходных данных для анализа используется информация из следующих источников:

- Журналов аудита ОС;
- Журналов аудита СУБД;
- Журналов аудита приложений;
- Журналов аудита сетевых устройств.

Внешний аудит безопасности

В отличие от внутреннего аудита, внешний аудит безопасности производится независимыми экспертами, не имеющими отношения к администрированию системы.

Внешний аудит безопасности входит в состав комплекса работ по аудиту ИС наряду с вопросами анализа надежности, производительности, разрешения проблемных ситуаций и т. д. Целями проведения аудита безопасности являются:

- Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- Оценка текущего уровня защищенности ИС;
- Локализация узких мест в системе защиты ИС;
- Выработка рекомендаций и требований по обеспечению безопасности ИС.

Использование криптографических методов защиты информации от НСД

Для обеспечения конфиденциальности и целостности критичной информации при передаче ее по каналам связи, проходящим вне контролируемой зоны, а также при хранении информации на магнитных носителях, необходимо использовать криптографические методы защиты информации. Программные и/или аппаратные средства криптографической защиты информации выбираются исходя из необходимости обеспечить определенный уровень защиты в соответствии с требованиями политики безопасности. В целом, должно быть предусмотрено:

- Использование систем шифрования с открытыми и закрытыми ключами для обеспечения конфиденциальности электронных документов;

- Использование средств электронной подписи для подтверждения авторства и контроля целостности электронных документов.

5.5. Перспективы и основные направления развития ИС и средств их проектирования.

Информационная технология является наиболее важной составляющей процесса использования информационных ресурсов общества. К настоящему времени она прошла несколько эволюционных этапов, смена которых определялась главным образом развитием научно-технического прогресса, появлением новых технических средств переработки информации. В современном обществе основным техническим средством технологии переработки информации служит персональный компьютер, который существенно повлиял как на концепцию построения и использования технологических процессов, так и на качество результатной информации. Внедрение персонального компьютера в информационную сферу и применение телекоммуникационных средств связи определили новый этап развития информационной технологии и, как следствие, изменение ее названия за счет присоединения одного из синонимов: "новая", "компьютерная" или "современная".

Прилагательное "новая" подчеркивает новаторский, а не эволюционный характер этой технологии. Ее внедрение является новаторским актом в том смысле, что она существенно изменяет содержание различных видов деятельности в организациях. В понятие новой информационной технологии включены также коммуникационные технологии, которые обеспечивают передачу информации разными средствами, а именно — телефон, телеграф, телекоммуникации, факс и др. В табл. 5.1 приведены основные характерные черты новых информационных технологии.

Основные черты новых информационных технологии.

Таблица 5.1

Система	Элементы системы	Главная цель системы
Фирма	Люди, оборудование, материалы, здания и др.	Производство товаров
Компьютер	Электронные и электромеханические	Обработка данных
Телекоммуникационная система	Компьютеры, модемы, кабели, сетевое программное обеспечение и др.	Передача информации

Информационная система	Компьютеры, компьютерные сети, люди, информационное и программное обеспечение	Производство профессиональной информации

Основные тенденции развития информационных систем и технологий:

- Применение объектных технологий .
- Интеграция неоднородных информационных ресурсов.
- Распределенные системы обработки информации.
- Поддержка метаданных.
- Управление потоками данных.
- Семантическая поддержка информационных ресурсов.
- Глобализация информационных систем.
- Соблюдение принципов корпоративности при разработке и эксплуатации.
- Развитие стандартов информационных технологий.
- Автоматизированная разработка информационных систем и т.д.
- Виртуализация ресурсов информационных систем.

Список литературы

1. Международные стандарты, поддерживающие жизненный цикл программных средств. М., МП "Экономика", 1996
2. Зиндер Е.З. Бизнес-реинжиниринг и технологии системного проектирования. Учебное пособие. М., Центр Информационных Технологий, 1996