Эксплуатация и сопровождение ИС. Управление рисками и инцидентами. Управление безопасностью. Резервное копирование и восстановление информации.

Лекция 5

ЭКСПЛУАТАЦИЯ И СОПРОВОЖДЕНИЕ ИС

Эксплуатация включает работы по внедрению компонентов ПО в эксплуатацию, в том числе:

конфигурирование БД и рабочих мест пользователей,

обеспечение эксплуатационной документацией,

проведение обучения персонала,

непосредственно эксплуатацию,

локализацию проблем и устранение причин их возникновения,

модификацию ПО в рамках установленного регламента,

подготовку предложений по совершенствованию, развитию и модернизации системы.

Ожидаемые результаты должны рассматриваться с учётом вероятной отсрочки в улучшении проектных и эксплуатационных характеристик.

Техническое обслуживание и модернизация.

Если собственно техническое обслуживание (очистка от пыли, смазка вентиляторов, подтяжка креплений, контроль состояния аккумуляторов, изменение физической топологии сети и т. п.) может осуществляться *службой технической поддержки*,

то грамотное формулирование заявок на изменение аппаратной конфигурации, организация закупки дополнительных лицензий или обновленной версии программного обеспечения – *задача администратора*.

Важным вопросом сопровождения ИС является мониторинг работы сетевого и иного вычислительного оборудования. *Задачу оперативного управления ИС* выполняет *администратор системы*.

Принято обращать внимание на критически важные инциденты. Затем рекомендуется осуществлять контроль сроков исполнения, оптимизировать контролируемы параметры и др.

УПРАВЛЕНИЕ РИСКАМИ И ИНЦИДЕНТАМИ

Определение рисков - сложная задача.

Успешное выявление и ликвидация рисков зависит от умения их распознавать.

Выделяю восемь наиболее опасных рисков:

1) недостаточное внимание к проекту со стороны руководства заказчика (компании) и недостаточное в нём участие;
2) неконкретная постановка задачи или непонимание сторонами конечных целей проекта;
3) изменения, вносимые заказчиком в процессе реализации проекта;
4) недостаточная квалификация работников;
5) отсутствия мотивации сотрудников заказчика, противодействие персонала;
6) срыв сроков;
7) технические проблемы;
8) недостаточное или нестабильное финансирование.

Недостаточное или нестабильное финансирование является одним из типовых рисков, независящих как от разработчиков проектов, так и специалистов, эксплуатирующих ИС.

Предлагается определять “точку невозврата”, то есть ситуацию, при которой теряется весь бюджет. Оценивая риск прекращения финансирования, важно определить его появление на соответствующих этапах.

Риски относящиеся к эксплуатации ИС, управление которой осуществляют администраторы ИС:

- *недостаточное внимание руководства организации, эксплуатирующей ИС, к главным вопросам эксплуатации и администрирования ИС;*
- *непонимание им важности данной работы, влекущее за собой некорректные указания по данным вопросам;*
- *недостаточную квалификацию администраторов и пользователей ИС;*
- *технические и финансовые проблемы.*

К рискам администрирования ИС относят:

- *сокращение установленных в соответствующих планах (графиках) сроков выполнения работ;*
- *увеличение стоимости сопровождения, эксплуатации и администрирования ИС из-за системных и иных ошибок, недостаточного уровня поддержки со стороны руководства и администраторов ИС;*
- *сложность эксплуатации системы;*
- *несоблюдение условий безопасности ИС и хранящихся в ней данных;*
- *сбои;*
- *увольнение администраторов и специалистов, осуществляющих эксплуатацию и поддержку ИС и др.*

Риски надо постоянно анализировать и актуализировать как в ходе проектирования, так и в ходе эксплуатации ИС.

Существует мнение, что если вероятность наступления какого-либо события превышает 50%, то следует быть готовым, что оно действительно произойдёт, а если она составляет 90%, то это уже серьёзная угроза.

Чем выше степень неопределённости условий планирования и эксплуатации ИС, тем выше степень необходимости количественного анализа рисков.

Количественную оценку большинства организационно-управленческих рисков для ИТ-проектов (ИС) оценить трудно, так же как и его экономическую эффективность, так как они обычно носят характер качественного улучшения и выполняются в условиях относительно низкой неопределённости. *При этом обычно все наиболее важные риски случаются до начала выполнения проекта.*

Качественную оценку рисков в виде низкий, средний, высокий, некоторые специалисты считают возможным перевести **в качественно-количественные показатели**.

При этом они определяют *высокую вероятность появления риска в 70% и выше (или 3 балла), среднюю – от 40 до 70% (2 балла) и низкую – менее 40% (1 балл)*.

Другой критерий предполагает, что если *воздействие приведёт к потере менее 1% бюджета или затянет сроки исполнения проекта менее чем на 5% отведённого времени, то его можно считать низким. Соответственно при 1–5% бюджета и 5–10% дополнительного времени – средним. Если бюджет превышен больше чем на 5%, а сроки – более чем на 10%, то высоким.*

Проведение внешней экспертизы по оценке рисков **способствует сокращению серьёзных системных ошибок** с далеко идущими последствиями, но может привести, как утверждают некоторые специалисты, **к погрешности расчётов**.

Для определения рисков некоторые специалисты **рекомендуют составлять таблицу с полями или столбцами, позволяющими получать ответы на следующие вопросы:**

что может случиться;

какова вероятность что это случится;

на каком этапе проекта это может произойти;

сколь сильно это может повлиять на результаты проекта;

что необходимо делать, чтобы это не случилось;

что делать, если это все-таки произойдёт?

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

Важным компонентом администрирования системы является обеспечение информационной безопасности: составление плана доступа пользователей к ресурсам (в соответствии с принятой в компании политикой информационной безопасности) и контроль его исполнения.

К функциям обеспечения безопасности относятся также отслеживание появления различных уязвимостей в используемых операционных системах, организация получения и установки “заплаток” (patches).

Функционально безопасность ИС можно разделить на технологическую, логическую и физическую безопасности.

- Для обеспечения ***технологической безопасности*** в информационных системах используют “зеркальные” серверы, двойные жёсткие диски, надёжные системы бесперебойного питания и др.
- ***Логическая безопасность*** заключается в использовании программных средств борьбы с компьютерными вирусами, защиты от несанкционированного доступа, идентификации и кодирования информации.
- ***Физическая безопасность*** включает персонал, меры и преграды, препятствующие проникновению несанкционированных лиц на недоступные для них объекты.

Аспектом общей надёжности ИС является её **безопасность (security)**, то есть **способность системы защитить данные от несанкционированного доступа**.

В распределённой системе это сделать сложнее, чем в централизованной.

В сетях *сообщения передаются по линиям связи*, часто проходящим через общедоступные помещения, в которых могут быть установлены *средства прослушивания линий*.

Другим уязвимым местом могут быть *оставленные без присмотра персональные компьютеры*.

Кроме того, всегда *имеется потенциальная угроза взлома защиты сети от неавторизованных пользователей*, если сеть имеет выходы в глобальные сети общего пользования.

Безопасность характеризует степень защищённости сети от несанкционированного использования её ресурсов:

1) Сети передачи данных,
2) Вычислительных ресурсов,
3) Информации (доступ, изменение).

Другой характеристикой надёжности является отказоустойчивость (fault tolerance).

В сетях под отказоустойчивостью понимают способность системы скрыть от пользователя отказ отдельных её элементов.

Например, если копии таблицы базы данных хранятся одновременно на нескольких файловых серверах, то пользователи могут просто не заметить отказ одного из них.

В отказоустойчивой системе отказ одного из её элементов приводит к некоторому снижению качества её работы (деградации), а не к полному останову.

Так, при отказе одного из файловых серверов в предыдущем примере увеличивается только время доступа к базе данных из-за уменьшения степени распараллеливания запросов, но в целом система будет продолжать выполнять свои функции.

В большинстве случаев **для защиты информации, ограничения несанкционированного доступа к ней**, в здания, помещения и к другим объектам приходится одновременно использовать программные и технические средства, системы и устройства.

Для защиты информации в информационных компьютерных сетях используют специальные программные, технические и программно-технические средства.

С целью защиты сетей и контроля доступа в них используют:

- *фильтры пакетов, запрещающие установление соединений, пересекающих границы защищаемой сети;*
- *фильтрующие маршрутизаторы, реализующие алгоритмы анализа адресов отправления и назначения пакетов в сети;*
- *шлюзы прикладных программ, проверяющие права доступа к программам.*

Необходимо поддерживать два фундаментальных принципа: **проверку полномочий (санкционирование)** и **проверку подлинности (аутентификация)**.

Проверка полномочий основана на том, что для каждого пользователя или процесса информационной системы устанавливаться набор санкционированных действий, которые он может выполнять по отношению к определенным объектам.

- *Проверка полномочий сама по себе недостаточна для обеспечения даже минимального уровня безопасности. Если, например, процесс «2» сможет успешно выдать себя за процесс «1», то он сможет выполнять действия и операции, доступные только процессу «1». Поэтому необходимы дополнительные меры.*

Проверка подлинности означает достоверное подтверждение того, что пользователь или процесс, пытающийся выполнить санкционированные действия, действительно является тем, за кого он себя выдает.

В безопасной среде должна поддерживаться проверка подлинности, способная обеспечить надёжную верификацию идентификаторов, предъявляемых пользователями или процессами.

Проверка подлинности стала ещё более важной в условиях массового распространения распределённых вычислений.

Сочетание средств проверки полномочий и проверки подлинности является мощным оружием в борьбе за безопасность информационных систем.

Однако *модель безопасности, основанная на базовых механизмах проверки полномочий и подлинности, не решает проблем, связанных с хищениями пользовательских идентификаторов и паролей или злонамеренными действиями пользователей*, обладающих полномочиями, например, администраторов ИС.

Если в системе хранится информация, относящаяся к разным классам безопасности (*от полностью открытой до совершенно секретной*), но все пользователи системы имеют разрешение на доступ к самой секретной информации, то в такой системе, вероятно, можно использовать мощные механизмы проверки полномочий и проверки подлинности. Такая **модель называется работой на высшем уровне секретности (running at system high).**

Однако **она окажется неудовлетворительной, если в учреждении необходимо организовать среду с многоуровневой безопасностью**.

Многоуровневая безопасность означает,

***во-первых**, что в системе хранится информация, относящаяся к разным классам безопасности, и,*

***во-вторых**, – часть пользователей не имеет доступа к информации, относящейся к высшему классу безопасности.*

Субъект имеет доступ к объекту, если уровень его допуска такой же или ниже, чем класс объекта.

При этом пользователь, имеющий низший уровень допуска, должен иметь возможность выполнять свою работу в системе, содержащей в базе данных совершенно секретные данные, но не должен иметь доступа к ним.

Информация и данные подвергаются классификации, а каждый субъект получает определённый уровень допуска к соответствующим классам данных (объектов).

Классы и уровни допуска совместно называются классами или уровнями доступа.

В военных и государственных ведомствах применяют следующую иерархию классов (сверху вниз):

- *совершенно секретно;*
- *секретно;*
- *конфиденциально;*
- *без грифа секретности.*

В частных компаниях возможны уровни иерархии (сверху вниз):

- *секретно;*
- *для ограниченного распространения;*
- *конфиденциально;*
- *для служебного пользования;*
- *для неограниченного распространения.*

Многоэкземплярность – общепринятая модель реализации баз данных с многоуровневой безопасностью.

Она заключается в том, что в рамках одного отношения может существовать множество кортежей (записей) с одним и тем же значением первичного ключа, например, данные с различными классами доступа могут быть реализованы в виде нескольких бах данных.

Защита носителей информации

Одной из важных проблем информационной безопасности является организация защиты электронных данных, хранящихся на различных носителях.

Защита данных от несанкционированного доступа предполагает:

1. *Обеспечение парольного входа в систему*: регистрация пользователей, назначение и изменение паролей.

2. *Обеспечение защиты конкретных данных*: определение прав доступа групп пользователей и отдельных пользователей, определение допустимых операций над данными для отдельных пользователей, выбор/создание программно-технологических средств защиты данных; шифрование информации с целью защиты данных от несанкционированного использования.

3. *Тестирование средств защиты данных*.

4. *Фиксация попыток несанкционированного доступа к информации*.

5. *Исследование возникающих случаев нарушения защиты данных и проведение мероприятий по их предотвращению*.

Обеспечение сохранности информации производится путём применения специальных мер организации хранения, восстановления (регенерации) информации, специальных устройств резервирования.

Качество обеспечения сохранности информации зависит от её целостности (точности, полноты) и готовности к постоянному использованию.

Важное значение для информации имеют методы её хранения и сохранения. Специалисты предлагают **несколько методик обеспечения сохранности электронных данных вообще и в Интернете в частности**:

- *постоянная миграция материала к наиболее современным аппаратурно-программным средствам* (т.е. непрерывная перезапись ресурса);
- *сохранение исходного формата и средств раскрытия содержания материала*;
- *копирование (архивирование);*
- *защита от несанкционированного использования, замены, искажения и удаления*;
- *защита от компьютерных вирусов и неполадок в электрических и компьютерных сетях*.

К сфере защиты данных относятся также сохранность данных и восстановление их после сбоя системы.

РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

Функционально безопасность ИС можно разделить на технологическую, логическую и физическую безопасности.

Для обеспечения ***технологической безопасности*** в информационных системах используют “зеркальные” серверы, двойные жёсткие диски, надёжные системы бесперебойного питания и др.

Логическая безопасность заключается в использовании программных средств борьбы с компьютерными вирусами, защиты от несанкционированного доступа, идентификации и кодирования информации.

Физическая безопасность включает персонал, меры и преграды, препятствующие проникновению несанкционированных лиц на недоступные для них объекты.

Важной особенностью систем хранения данных является ***непрерывная их защита*** (Continuous Data Protection, CDP).

Для защиты данных, хранящихся на файл-сервере, применяют **резервное копирование, ленточный автозагрузчик** и др.

Открытые файлы не копируются на ленту.

Операция резервного копирования создаёт дополнительную нагрузку на сервер.

В этом случае резервное копирование можно осуществлять в нерабочее время (ночью, в выходные и праздничные дни и др.), то есть в специально выделяемый для этого период времени – *окно резервного копирования*.

С целью обеспечения достоверности и постоянной работоспособности ИС **периодически вручную или автоматически осуществляется копирование ИС**.

Основными причинами, побуждающими выполнение процедур копирования, являются различные структурные изменения в ИС:

- *создание или удаление табличного пространства;*
- *добавление или переименование (перемещение) файла данных в существующем табличном пространстве;*
- *добавление, переименование (перемещение) или удаление журнала повторения и др.*

При этом резервное копирование может осуществляться непосредственно перед изменениями и после них.

Выделяют два основных вида резервного копирования:

1. ***Непротиворечивое (холодное) резервное копирование***, когда копии создаются, в случае закрытой для пользователей ИС. Копия ИС, созданной в автономном режиме, содержит: все файлы данных, журналы повторов и управляющие файлы. После остановки ИС, все её файлы копируются на один из “backup” дисков. По окончании копирования осуществляется перезагрузка ИС.
2. ***Резервное (горячее) копирование*** в оперативном режиме, к примеру, когда ИС всё время находиться в оперативном режиме и доступна пользователям.

Первоначальный режим архивирования ИС устанавливают во время её создания. После создания ИС решают, необходимо ли изменить первоначальный режим архивирования.

Автоматическое архивирование журнала в любой момент можно выключить. В этом случае придётся вручную периодически архивировать заполняемые группы журнала.

Для обеспечения бесперебойной работы часто **применяют архивирование ИС из журнала транзакций**, а в случае отказа системы при следующем старте операции над данными восстанавливают по журналу транзакций (например, производят их откат до определенного момента времени).

Применяют также **методы горячего резервирования**, когда работают два сервера: основной, обрабатывающий запросы пользователей, и резервный, который продолжает работу основного сервера в случае его отказа. Состояние хранилищ данных на основном и резервном серверах согласовано и поддерживается ИС автоматически.

Работа серверов в режиме горячего резервирования не избавляет от необходимости хранения резервных копий данных, это может быть и не очевидно для аналитиков и не предусмотрено ими.

Некоторые бизнес-процессы по своей природе требуют от информационной системы работы в режиме 24x7, и любой простой стоит очень дорого. В этих случаях работают две или три параллельные системы, и при отказе одного из серверов резервные серверы немедленно принимают управление на себя.

Эффективным, но дорогостоящим способом реализации таких задач являются **предоставляемые ИС технологии симметричной репликации**.

Еще один вариант – архивирование журналов транзакций на резервном узле на специальное устройство и немедленный докат по этому журналу резервного узла в случае отказа основного.

В простых ситуациях, *когда информационная система используется в основном для операций чтения данных, а сами данные меняются редко, резервное копирование может вообще не требоваться, если данные одной такой системы могут быть легко восстановлены из данных других работающих систем.*

Достаточно **обеспечить наличие образа ИС** (архив всех файлов, а также управляющих файлов – снимок ИС на определенный момент времени; проще всего такой снимок получить, остановив ИС и сделав резервную копию всех указанных файлов).

Разные ИС предлагают разные механизмы реализации подобной бесперебойной работы, администраторам приходится самостоятельно принимать верное решение.