|  |
| --- |
| Правительство Российской Федерации  Федеральное государственное автономное образовательное учреждение  высшего профессионального образования  «Национальный исследовательский университет  «Высшая школа экономики»  Факультет информационных технологий и вычислительной техники  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Компьютерные мультисреды\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Специализация)  \_\_\_\_\_\_\_\_\_[Информационно-коммуникационные технологии](http://omop.su/article/11/882315.html)\_\_\_\_\_  (кафедра) ДИПЛОМНАЯ РАБОТА «Разработка процессной и технической архитектуры комплекса предоставления IT-услуг в рамках технического ВУЗа»  Выполнил  Студент группы № С-95  Денисов Андрей Павлович  Научный руководитель:  Азаров Владимир Николаевич, д.т.н., профессор  Консультант:  Линецкий Борис Львович |

Москва 2013

|  |
| --- |
|  |

**1.Аннотация**

Данный проект ставит своей целью создание базового набора IT-сервисов для обеспечения деятельности технического ВУЗа, а так же разработка процессной и технической архитектуры комплекса предоставления IT-услуг в рамках технического ВУЗа. В ходе разработки осуществлен анализ современных подходов к организации комплекса предоставления IT-услуг.

**2.Содержание**

1.Аннотация 2

2.Содержание 3

3.Введение 4

4.Обзорно-аналитическая часть 5

4.1.Анализ современных подходов 5

4.2 Анализ библиотек 5

4.2.1. ITIL 5

4.2.2.Cobit 8

4.2.3. CMMI 9

4.2.4. ASL 11

4.2.5. MSM 12

4.2.6. ISPL 15

4.2.7. FITS 16

4.3. Выбор международного подхода 17

5.Технологическая часть 18

6.Разработка 19

6.1.Разработка базового набора IT-сервисов 19

6.2.Разработка процессной архитектуры 25

6.3.Разработка технической архитектуры 49

7.Экспиреминтальная часть 51

8.Охрана труда 53

8.1.Анализ рисков по защите информации 55

9.Вывод 59

10.Список используемой литературы 60

**3.Введение**

За последние десятилетия IT технологии произвели огромное влияние на многие бизнес – процессы. При появлении персональных компьютеров, частных сетей, интернет технологии клиент – сервер позволило организациям намного быстрее вывести на рынок свои услуги и продукты. Учитывая рамки традиционных иерархических организаций, зачастую трудно отреагировать на условия быстроменяющихся рынков, что привело к появлению новых, более гибких организаций с меньшей сложностью иерархичности. В организациях происходил переход от вертикальных функций к горизонтальным, которые работают в рамках всей организации, а право принятия решения в большей степени переходило на более низкие уровни. На такой основе развивались процессы управления IT – услугами. Как следствие, появилось большое количество подходов к организации предоставления IT- услуг. В работе будет проведен анализ современных подходов к организации комплекса предоставления IT-услуг. Выбран оптимальный подход для разработки процессной и технической архитектуры комплекса предоставления IT-услуг в рамках технического ВУЗа. А так же разработан базовый набор IT-сервисов для обеспечения деятельности технического ВУЗа. Данная тема очень актуальна на сегодняшний день, т.к. построен кампус «МИЭМ НИУ ВШЭ Строгино». Для которого требуется разработать и внедрить базовый набор IT-сервисов, а так же процессную и техническую архитектуру комплекса предоставления IT-услуг.

**4. Обзорно-аналитическая часть**

**4.1. Анализ современных подходов к организации комплекса предоставления IT-услуг**

IT Service Management – подход к организации комплекса предоставления IT – услуг, ориентированный на предоставление определенных услуг и сфокусированный на потребителе.

Сущность ITSM в том, чтобы IT отдел не был вспомогательным звеном для основного бизнеса компании, отвечающий за работу серверов, приложений и сетей. IT отдел должен быть полноправным участником бизнеса, он должен выступать как поставщик сервисов, таким образом отношения между бизнес-подразделениями и IT отделом складываются как потребитель и поставщик. Бизнес-подразделение определяет требования к необходимым сервисам, их качеству, а IT отдел поддерживает инфраструктуру компании на таком уровне, чтобы обеспечивать запрошенный сервис с определенным качеством.

Для реализации ITSM важной частью является разработка формализованных процессов. Для всех процессов назначается последовательность выполнения работ, а так же необходимое время и ресурсы. Помимо того, если процесс строго определен и документирован, можно вычислить его производительность, что позволяет совершенствовать процесс и корректировать его до того, как произойдет сбой в реализации сервиса.

Существует много методов и подходов к организации работы всей информационной системы и других сопровождающих служб, представляющие собой инструмент для управления сервисами и выполнение нормативных требований. Самой известной и сильной является библиотека ITIL. Так же существуют: Cobit - метод контроля и аудита, CMMI - модель зрелости, MSM - один из методов разработанных компанией Microsoft, как и многие другие.

**4.2. Анализ библиотек комплекса предоставления IT-услуг**

**4.2.1. ITIL**

ITIL(IT Infrastructure Library – это библиотека инфраструктуры различных информационных технологий). ITIL является самым распространенным подходом к управлению IT как поставщиком услуг. В нем описаны процессы, которые нужны для повышения качества сервисов компании, предоставляемых заказчикам и пользователям. ITIL описывает лучшие из средств организации работы компаний и подразделений (применяемых на практике), которые предоставляют услуги в области IT. Библиотека представляет собой набор лучших практик взятых из опыта предприятий частного сектора, а так же общественных и некоторых государственных организаций.

Процессный подход, который использован в ITIL полностью соответствует стандартам из серии ISO 9000 (ГОСТ Р ИСО 9000). Этот подход фокусирует внимание компании на достижении ранее поставленных целей, на ресурсах, затраченных на достижение целей, а также анализе эффективности ключевых показателей (KPI). Процессный подход очень популярен, т.к. не имеет равных себе по обеспечению измеримости и управляемости деятельности компании.

На данный момент на основе ITIL создан британский стандарт BSI 15 000, который с небольшими изменениями стал международным стандартом под названием ISO 20000. Основываясь на базе рекомендаций ITIL, разработан ряд программ по автоматизации служб технической поддержки IT.

ITIL является обобщением лучшего международного опыта в сфере организации и управления информационными технологиями. На сегодняшний день этот стандарт используется предприятиями и организациями по всему миру.

ITIL помогает в большей степени повысить эффективность обслуживания, повышает уровень удовлетворенности клиентов оказанным им сервисом, снизить стоимость услуг.

Вывод: ITIL является одним из самых известных и распространенных подходов к управлению IT. Направлен на повышение качества услуг, снижение их стоимости, на повышение удовлетворенности клиентов сервисом. ITIL ориентирован на крупные организации, которые готовы к масштабным затратам, к реорганизации процессов с целью получения некоторой выгоды за счет их использования.

Формальные стандарты для ITSM были впервые опубликованы Британским Институтом Стандартов и названы BS15000. Далее их приняли в ISO (International Standards Organisation), и дали обозначение ISO20000.

Стандарт ISO/IEC 20000 - основной стандарт в области управления IT-услугами (ITSM), считается обобщением мирового опыта при организации управления IT сервисами и может применяться в любой организации, не зависимо от ее отрасли и размеров.

Он содержит определение ключевых процессов и управление ими при предоставлении IT-услуг, в полной мере отвечающих требованиям потребителей и реализации бизнес-задач организации.

Стандарт основывается на лучших практиках в этой сфере, включая ITIL. ISO/IEC 20000 устанавливает необходимый уровень для оказания услуг и дает методологию для достижения поставленных задач и требований при помощи управляемого процесса. Стандарт состоит из двух частей:

1. ISO 20000-1:2005 «Information technology — Service management. Part 1: Specification» состоит из подробного описания требований к системе менеджмента информационных сервисов и ответственности за инициирование, выполнение и качественную поддержку в организациях.

2. ISO 20000-2:2005 «Information technology — Service management. Part 2: Code of Practice» - это практические рекомендации процессов и требований к ним, описанные в первой части стандарта. Является очень полезным руководством для организаций и аудиторов, которые собираются пройти сертификацию.

В стандарте выдвинуты требования к степени ответственности руководителей компании, которые предоставляют сервисы IT, а также к организации управления документацией, достаточной компетенции, полной осведомлённости и тщательной подготовке персонала.

Для обеспечения интегрированного подхода при оказании высококачественных и эффективных информационных сервисов, стандарт ISO 20000:2005 предлагает переход к сервисной модели информационных технологий, реализуемый путём разработки и внедрения в организацию формальной системы управления ИТ сервисами (СУИС). СУИС помогает повысить уровень капитализации предприятия, может способствовать его признанию на мировом уровне. С окончанием внедрения СУИС предприятие готово к сертификации. При сертификации по стандарту ISO 20000 проверяется политика руководства и цели компании, оценочная система рисков сервисов ИТ, используемые процедуры и полное соответствие требованиям стандарта.

Во-первых ISO 20000:2005 предоставляет средства для оценки организации ИТ и измерения эффективности их деятельности . Во-вторых данный стандарт направлен на практическую реализацию задач, связанных с выбором внешнего поставщика ИТ сервисов (тендером). Независимая сертификация, при помощи этого стандарта, позволяет организациям наглядно продемонстрировать своим клиентам соответствие качества услуг лучшим мировым практикам.

Стандарт ISO/IEC 20000, определяющий требования к системе управления ИТ-услугами состоит из следующих частей:

-взаимосвязанные и задокументированные процессы системы управления ИТ-услугами (процессы СУИТУ),

-сотрудники ИТ-подразделений, реализующие данные процессы управления, а также представители из состава руководства организации;

-системы и средства автоматизации, используемые сотрудниками ИТ-подразделений при реализации процессов управления ИТ услугами.

Вывод: ISO/IEC 20000 является основным стандартом в сфере управления ИТ-услугами. Он основан на самых удачных практиках в этой области, включая ITIL. При соблюдении условий стандарта организация может наглядно показать своим клиентам полное соответствие качеству предоставляемых сервисов.

**4.2.2. Cobit**

Методы управления, контроля и аудита данных информационных систем была разработана в 1992 году Международной ассоциацией аудита и контроля за информационными системами (ISACA). Она предоставляет менеджерам, аудиторам и пользователям IT набор утверждённых метрик, процессов и лучших практик с целью помощи в извлечении максимальной пользы от использования информационных технологий и для разработки соответствующего руководства и контроля IT в организации.

Для достижения целей, информация должна соответствовать некоторым критериям, которые в Cobit называют бизнес-требованиями к информации. Можно выделить следующие бизнес-требования и критерии к информации: рациональность, целостность, конфиденциальность, эффективность, доступность, соответствие нормам и надёжность информации. Механизмы управления включают процедуры и регламенты, организационные структуры, политики.

Посредством использования CobiT руководители IT отделов формулируют задачи бизнеса в чёткие и внятные планы развития IT. Основным преимуществом Cobit является его отчётливые практические рекомендации и инструменты, на основе которых можно создать систему управления IT корпорации.

Вывод: CobiT описывает бизнес-ориентированный подход к реализации информационной среды: информационные технологии рассматриваются как инструмент бизнеса, а стандарт определяет принципы строения и организации работы IT департамента, используя информацию аудита, полученной службой технической поддержки. Не редко внедряется как дополнение к ITIL.

**4.2.3.CMMI**

CMMI (Capability Maturity Model Integration)— набор моделей улучшения процессов на предприятиях разнообразных размеров и видов деятельности.

CMMI содержит набор практик, при реализации которых можно реализовать цели, которые необходимы для полной реализации определенных сфер деятельности. CMMI является дальнейшим развитием методологии CMM, разрабатывающаяся со второй половины 1980-х годов в Software Engineering Institute (SEI) в университете Карнеги-Меллона (Carnegie Mellon University).

Набор моделей CMMI содержит 3 модели: CMMI for Development (CMMI-DEV), CMMI for Services (CMMI-SVC) и CMMI for Acquisition (CMMI-ACQ). Самой известной считается модель CMMI for Development, которая ориентирована на организации, занимающиеся разработкой программного обеспечения, аппаратного обеспечения и комплексных систем.

CMMI определяет 22 области процессов (process areas). Для каждой из данных областей существует ряд целей (goals), которые необходимо достигнуть при внедрении CMMI в этой процессной области. Некоторые цели уникальны — их называют специальными (specific). Общие (generic) цели применяются к нескольким процессным областям. Они достигаются при помощи выполнения практик. Как и цели, практики можно разделить на специальные и общие. Грамотное использование данной модели позволяет предприятию оценивать эффективность бизнес-процессов, устанавливать приоритетные направления их усовершенствования, также внедрять данные усовершенствования.

Вывод: CMII набор методологий для оценки и совершенствования процессов в организациях различных размеров. Цель CMII - рост зрелости процессов до высочайшего уровня.

ISO/IEC 38500

В настоящее время в сфере управления информационными технологиями сложилась такая ситуация, когда неточная и неполная информация может помешать осуществлению некоторых условий конкурентоспособности или подвергнуть организацию, использующую эту информацию, риску несоблюдения законов. Чтобы решить данного рода проблему был разработан и опубликован стандарт ISO/IEC 38500, где представлены очень подробные инструкции и разъяснения по управлению ИТ.

С помощью стандарта ISO/IEC 38500 учреждение может модернизировать рабочий процесс эффективного управления ИТ. В главной мере стандарт предназначен высшему руководству организаций, для полного понимания и качественного выполнения их обязательств в отношении ИТ (правовых, этических и нормативных) .

Главная цель стандарта состоит в дальнейшем продвижении применения ИТ разными организациями и учреждениями. Для управления ИТ используется ISO/IEC 38500:2008 организациями любых видов и размеров, начиная от небольших коммерческих и некоммерческих предприятий и организаций вплоть до крупных госучреждений.

Абсолютное большинство организаций использует информационные технологии в качестве основного средства для бизнеса. Все бизнес-планы, составляемые на будущее не обходятся без разработок в ИТ. Любая неточность в информации может помешать осуществлению всех условий конкурентоспособности и подвергнуть организацию некоторому риску несоблюдения законов. стандарт ISO/IEC 38500 был разработан и опубликован для решения данных проблем , в нем представлены подробные разъяснения и инструкции по управлению ИТ.

Данный стандарт способствует проведению политики быстрого развития деятельности организации в соответствии со всеми обязательствами (законодательством, общим правом, нормативными актами и контрактными соглашениями) относительно допустимого использования ИТ.

С помощью применения данного стандарта создаётся инфраструктура эффективного управления ИТ и, тем самым, оказывается реальная помощь в реализации юридических, нормативно-правовых и моральных обязательств в сфере использования ИТ, соответствующим также и стандартам ITIL.

Структура стандарта ISO/IEC 38500 включает в себя определения, принципы и модели управления. В тексте этого стандарта описаны шесть самых эффективных принципов управления ИТ, в которых указаны основные аспекты принятия решений:

- ответственность;

- человеческое поведение;

- стратегия;

- реализация;

-приобретение;

- соответствие.

Вывод: Данный стандарт позволяет руководству объективно оценить инфраструктуру информационных технологий в своей организации, направить и проконтролировать использование информационных технологий. Для получения в итоге чёткой и продуктивной системы управления информационными технологиями.

**4.2.4. ASL**

ASL (Application Services Library) - библиотека сервис-приложений; Библиотека ASL создана специалистами компании PinkRoccade. В библиотеке собран опыт эксплуатации приложений в общей библиотеке. Они исходили из следующей гипотезы, создавая ее,. Если говорить о приложениях, то на протяжении почти всего времени существования информационных технологий в фокусе внимания был преимущественно собственно процесс разработки. На сегодняшний день работоспособность приложений становится критичной для бизнеса , фокус смещается к эксплуатации приложений. Поддержание работоспособности, надежность эксплуатации приложений становятся важнейшими факторами их жизненного цикла. На них приходятся от 50% до 70% затрат на протяжении всего жизненного цикла.

Управление приложениями на протяжении жизненного цикла остается проблемной областью, практически не привлекающей к себе внимания теоретиков в области программирования. Это происходит из-за недостаточно точного определения различий между двумя типами действий по отношению к программному обеспечению: enhancement (модернизация или усовершенствование) и maintenance (поддержка и эксплуатация).

ASL дает следующие определения данным понятиям.

Модернизация — это результат действий, которые были выполнены по запросу и относятся к функциональным или нефункциональным требованиям, не специфицированных изначально, в оригинале системы.

Эксплуатация — это координированные действия, обеспечивающие непрерывность функционирования существующей системы в соответствии с согласованными правилами и процедурами.

Структура ASL состоит из шести групп процессов, условно разделенных на три уровня:

-Процессы управления

-Эксплуатационные процессы

-Стратегические процессы

Эксплуатационные процессы и процессы управления рассматриваются в рамках ограничения по времени, тогда как стратегические процессы рассматриваются в перспективе на несколько лет вперед.

Используя представленную в ASL методологию, существует возможность реализации процесса эксплуатации рациональным образом на протяжении всего жизненного цикла приложений.

Вывод: Основная задача библиотеки ASL - поддержание работоспособности приложений и надежности их эксплуатации. ASL представляет собой методы создания структуры управления прикладным программным обеспечением.

**4.2.5 MSM**

В MSM включены наилучшие практические методы управления системами, базирующиеся на технологии компании Microsoft. Основой выступает подход Microsoft Operations Framework (MOF). Этот подход дает подробные рекомендации по планированию, эксплуатации и быстрому развитию оперативных процессов, которые поддерживают критические важные решения. Основой составления MOF послужила библиотека ITIL. Microsoft дополняет методологические рекомендации ITIL своими собственными наработками, которые затрагивают вопросы использования продуктов и технологий данной корпорации. MSM ставит во главу не технические детали реализации информационной системы, а процессы, составляющие ее логическую схему, что позволяет добиться универсальности содержащихся в ее решениях рецептов. Однако, даже при современном уровне, процессы автоматизации остаются лишь инструментами в руках людей, использующих их. MSM рассматривает IT-кадры предприятия как еще одну важную составляющую в системе управления. Третья составляющая цепочки управления — задействованные в IT-инфраструктуре компании технологии. Для объединения этих трех факторов в эффективную структуру управления, MSM предлагает прибегать к помощи комплекса специально разработанного для этого программного обеспечения.

MSM использует понятия моделей и сценариев.

Моделью называют набор технологий и практических примеров наилучшего использования их в реальных условиях. Всего их три в MSM.

Модель процессов описывает процессы управления и поддержки информационной системы. Представив информационные системы в формализованном виде, модель позволяет легко и довольно доступно описывать насколько угодно сложную схему управления информационной инфраструктурой. Она определяет структурную архитектуру комплекса мероприятий по обслуживанию информационных систем, приводит к ускорению жизненного цикла IT-решений, налаживает систему обратной связи и содержит советы по внедрению управления рисками в ежедневную административную рутину.

Модель коллектива касается вопросов организации коллектива IT-сотрудников, распределения внутри них основных задач и ролей, а также увелечения эффективности работы технических отделов организации. Она содержит самые удачные примеры создания структуры организации в командах администраторов, отмечает ключевые задачи для каждого из отделов внутри подразделения, показывает пути увеличения коллективов в связи с ростом предприятия.

Модель рисков включает описания и примеры использования практически проверенных техник управления рисками. Она детально описывает такие эффективные стратегии, как непрекращающийся поиск новых рисков, управление ими на основе ролей и функций, публичный анализ найденных рисков, использование графиков, основанных на рисках и формализация их процесса.

В отличие от моделей сценарии представляют собой примеры для решений в области управления информационной инфраструктурой, связанные с четко обозначенными программными продуктами Майкрософт. MSM версии 1.0 включает в себя распространение обновлений (позволяет быстро, эффективно и управляемо внедрить выпущенные Microsoft обновления программных продуктов, Service packs и hot fixes, используя SMS);постоянное наблюдение и управление службами (автоматизирует мониторинг доступности Active Directory, Exchange 2000 и SQL Server 2000 на Windows 2000 Server);оценка функционирования (дает возможность пользователям идентифицировать точки главных проблем и разработать план, адресуемый к ним);установка Office XP (позволяет быстро, эффективно и управляемо внедрять Office XP).

MSM рассматривает три увязанных в логическую последовательность этапа трансформации информационной системы, ставящих своей общей целью достижение высоких показателей экономичности, безопасности и эффективности инфраструктуры. Первый шаг реализуется за счет внедрения решений, направленных на упрощение IT-архитектуры и снижение издержек на ее администрирование и обслуживание (консолидации серверов). Следующим шагом является достижение полной безопасности в условиях использования общественных каналов связи и ведения хозяйственной деятельности через сеть. Здесь на помощь приходят решения из набора организации наиболее безопасного доступа ко всем информационным системам. Итак, после того как были достигнуты достаточная экономичность, внутренняя стандартизация и внешняя безопасность, приходит очередь обеспечия максимальной эффективности коллективной работы отдельных работников и целых подразделений предприятия. Именно об этом заходит речь в принятии решений, касающихся инфраструктуры систем взаимодействия.

Вывод: Основой MSM являются технологии и средства комании Microsoft. Использовать который имеет смысл только в компаниях использующих решения Microsoft.

**4.2.6. ISPL**

ISPL - это библиотека накопленного опыта для управления процессами приобретения.

Процесс приобретения называют процесс получения системы (услуги) или их комбинации. Управление приобретением содержит в себе определенные подходы приобретения, планирование поставки системы, управление процессом выбора предложений, критерии решений о лучших предложениях и поставщике, контроль расходов и сроков, управление рисками, мониторинг контрактов.

Сервисы состоят из процессов, которые выполняет одним человек(организация) для другого человека или организации. ISPL рассматривает 2 типа сервисов:

- постоянно действующие сервисы, целью которых является выполнение процессов, определяемых уровнем сервиса. Примером могут служить процессы ITIL: управление сетью, управление конфигурациями, управление изменениями и функция технической поддержки.

- проекты, цель которых изменение процессов или систем в предприятии. Например, такие как модификация и развитие системы, реконструкция бизнес-процесса и установка технической поддержки,

ISPL предлагает набор инструментария, книг и услуг, помогающих заказчику или поставщику организовать управление приобретения сервисов и систем для государственных и частных организаций.

Выгоды в использовании ISPL для заказчиков:

- ясность изложения требований,

- усовершенствование управления системными рисками,

- руководство для выбора необходимого подхода к приобретению в различных сложных ситуациях,

- достаточное понимание предложений поставщиков,

- легкость оценки предложений поставщиков,

- легкость контроля дополнительно появляющихся пожеланий,

- хорошая информированность для контроля затрат,

- независимость от поставщика,

- независимость от используемого специфического метода приобретения,

- улучшение процесса принятия решений относительно выбора наиболее достойного поставщика,

- улучшение управления контрактами.

Выгоды от использования ISPL для поставщиков:

- хорошее понимание нужд заказчиков,

- понимание требуемых систем и услуг,

- повышение уровня управления рисками, которые связаны с услугами,

- определение подходящего подхода к доставке услуг,

- легкость получения поддержки от заказчика при выработке ключевых решений,

- легкость сдачи системы, путем лучшего определения требований и планирование поставки,

- лучшая информированность для контроля затрат,

- улучшение управления контрактами.

Вывод: ISPL помогает поставщику и клиенту достигать необходимых уровней качества, используя малое количество денег и времени, лучшие методы менеджмента, планирования и управления. ISPL основывается на отношениях между поставщиком и клиентом. Что существенно помогает поставщику и заказчику осуществлять контроль затрат и сроки, улучшать взаимопонимание и управлять рисками.

**4.2.7. FITS**

FITS -собрание лучших практик, которые основаны на библиотеке ITIL, но переделанной под нужду школ, охватывающих всевозможный спектр технической поддержки. Руководство собиралось по опыту провайдеров со всех концов Британии.

Использование FITS может помочь:

- Уменьшить затраты;

- Повысить уверенность и надежность: каждый месяц, приблизительно 55 процентов учителей борются с принтерами и более чем у 40 процента есть проблемы с их компьютерами классной комнаты.

FITS улучшает надежность, помогая штату технической поддержки предотвратить проблемы прежде, чем они появятся.

- Штат технической поддержки может быть превентивный, и должен препятствовать появлению проблем.

- Позволяет учителям сосредоточиться на преподавании и обучении. Освобождает их от необходимости тратить время на решение различных технических проблем.

- Предоставяет возможность лучшего использования ICT

-Улучшает инспекционные результаты

- Улучшает школьные показатели в целом.

Вывод: FITS является набором инструментов разработанных для помощи техническому штату школы, в управлении и поддержки ICT в структурированной и эффективной форме.

**4.3. Выбор международного подхода**

Рассмотрев основные подходы к организации предоставления IT – услуг, проведя детальный анализ каждого из подходов, можно сделать вывод, что для создания комплекса предоставления IT – услуг наиболее подходящим является метод ITSM.

ITSM является наиболее авторитетным собранием лучших практик. Учитывая не большой размер IT отделов, можно достичь полезных результатов в улучшении качества предоставляемых сервисов и сокращению затрат на них.

Остальные методы не подходят по разным причинам:

MSM направлен на продукцию Microsoft, что не удобно в нашем случае.

FITS сильно упрощенный вариант, который используется в школах, и данный метод не подходит в конкретном случае.

ISPL не подходит т.к. в первую очередь касается процессов приобретения, а не процессов управления ИТ отделом в целом.

CobIT же зачастую является логическим продолжением методологии ITSM

ISO/IEC 20000 и ISO/IEC 38500 являются стандартами качества, а не методами организации ИТ инфраструктуры.

CMII направлен на совершенствование процессов, а не на разработку, что не позволяет использовать его в данном проекте.

**5. Технологическая часть**

**5.1. Выбор технологических и технических решений для реализации IT – сервисов, необходимых для обеспечения деятельности технического ВУЗа**

Для реализации IT – сервисов, необходимо:

- Создать инженерные системы и СКС. СКС – это основа инфраструктуры института, предоставляющая возможность свести в единую систему сетевые сервисы: телефонные и локально вычислительные сети, системы безопасности и видеонаблюдения и т.д. Произвести монтаж кабельных трасс, разводка и подключение электрических сетей, установка розеток, оборудование серверной комнаты, установка систем бесперебойного питания, создание систем кондиционирования и вентиляции.

- Создать сетевую инфраструктуру. Произвести монтаж сетевого оборудования, беспроводных сетей Wi-Fi.

- Установить автоматическую телефонную станцию (АТС). Установить и настроить АТС, запрограммировать логику работы, подключение услуг IP – телефонии.

- Установить серверное оборудование. Произвести установку и подключить серверное оборудование, системы резервного копирования, системы хранения данных.

- Установить систему виртуализации серверов. Виртуализация серверов позволяет одновременно функционировать несколько виртуальных машин на одном физическом сервере, что существенно сокращает затраты на оборудование, программное обеспечение, электроэнергию, обслуживание, повышает гибкость и надежность IT – инфраструктуры.

- Внедрить основные сетевые службы на основе протокола TCP/IP. Произвести установку служб DHCP и DNS.

- Внедрить сервера печати. Для обеспечения управления всеми принтерами института. Служат для распределения нагрузки, хранения и управления очередями печати.

- Внедрить СУБД (система управления базами данных). Для обеспечения хранения, доступа и управления базами данных приложений.

- Внедрить сервер управления и защиты интернет трафика. Для обеспечения защиты корпоративной сети от интернет-атак, контроля и управления доступа пользователей в интернет.

- Внедрить сервер резервного копирования. Для обеспечения всей электронной информации института.

- Внедрить сервера антивирусной защиты. Для обеспечения развертывания, управления и обновления антивирусного программного обеспечения.

- Установить рабочие места. Произвести установку и настройку рабочих станций, ноутбуков, телефонов и прочего оборудования.

- Установить периферийную технику. Произвести установку и настройку принтеров, ксероксов, сканеров, многофункциональных устройств и т.д. Настроить сетевые параметры устройств. Установить средства мониторинга и управления периферийным оборудованием.

**6. Разработка**

**6.1. Разработка базового набора IT-сервисов для обеспечения деятельности технического ВУЗа**

Данный набор базовых IT – сервисов для обеспечения деятельности технического вуза в общем своем виде базируется на классической сервисно–ресурсной модели, которая описана в IITIL v3. В главе №3 «Service Design principles» описано, как должны формироваться IT – сервисы и из чего они должны состоять.

Один из принципов Всеобщего менеджмента качества (Total Quality Management – TQM) , которые положены в основу новой версии серии стандартов ISO 9000 - процессно-ориентированный подход к управлению организацией. Согласно этому принципу, необходимый результат достигается быстрее, когда деятельностью и соответствующими ресурсами управляют как всем процессом.

Международные стандарты ISO серии 9000 версии 2005 года – стандарты, направленные на применение «процессного подхода» при разработке, улучшении и внедрении результативности системы менеджмента качества с целью увеличения удовлетворенности потребителя за счет выполнения его требований. Чтобы результативно существовать, организации необходимо определять и управлять многими взаимосвязанными процессами.

Процессно-ориентированный подход при управлении организацией, в данном случае высшего учебного заведения (ВУЗ), включает описание и определение всех основных и вспомогательных процессов вуза, а также построение взаимосвязей между этими процессами и дальнейшего управления ими, используя непрерывное улучшение по методике РDСА (рис. 1), мониторинг удовлетворенность потребителя и внутренний аудит процессов.

Процесс - это набор взаимодействующих и взаимосвязанных между собой типов деятельности, преобразующие входы в выходы. Процессы организации типично осуществляются и планируются в управляемых условиях для добавления значимости продукции.

Входы процесса – это ресурсы, которые преобразуются в ходе процесса в выходы процесса. Входами к процессу чаще всего являются выходы других процессов.

Выходы процесса – это конечные результаты (продукт, услуга) процесса.

Желаемый результат (т.е. цель) достигается эффективнее, когда данной деятельностью и соответствующими ресурсами управляют как и процессом. В процессах описана не вся деятельность организации, а только та ее часть, которая влияет на получение продукции. Границы процесса должны быть четко определены (по функциям и ответственности руководителей).

Можно выделить основные и вспомогательные процессы.

Основные процессы лежат на пути следования продукции: сначала в виде маркетинговой информации, проекта, затем в виде материального объекта (детали, товара, программного продукта, услуги и т. д.).

Для обеспечения нормального функционирования основных процессов выделяют вспомогательные процессы .

Каждой организации жизненно необходимо постоянно совершенствовать свою деятельность, для сохранения имеющиеся и достижения более новых преимуществ перед организациями-конкурентами. Один из методов непрерывного совершенствования - управление деятельностью организации согласно знаменитому циклу Деминга «РDСА» состоит из планирования, выполнения, проверки, действий.PDCA является методологией, которая представляет простой алгоритм действий руководителя по управлению процессом и достижению его целей. Цикл управления начинается с планирования.

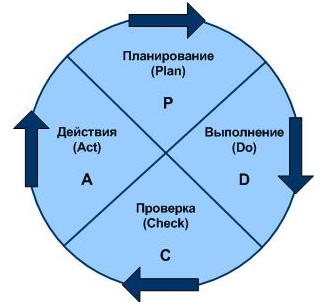


Рис. 1 – Цикл Деминга PDCA

Планированием (Plan) называют установление целей и процессов, которые необходимы для достижения целей, планирование выделения и распределения необходимых ресурсов, планирования работ по достижению целей процесса и удовлетворенность потребителя.

Выполнением (Do) принято считать осуществление плановых работ.

Проверкой (Check) называется сбор информации и контроль результата, который получился при выполнении процесса, установление причин отклонений, а так же выявление и анализ отклонений.

Действия (управление, корректировка) (Act) – это принятие мер для устранения причин отклонений от планированного результата, изменения в распределении и планировании ресурсов. После окончания этапа «Действия» цикл начинается заново.

При прохождении цикла PDCA, организация (в отличие от организации со стандартным методом управления) имеет продукцию более высокого качества и, как следствие, более высокие требованиями к технологии ее изготовления.

Цикл PDCA применим к процессу в целом, а так же к отдельным видам деятельности, входящих в состав процесса.

В ходе разработки решения по базовому набору IT – сервисов для обеспечения деятельности технического вуза было выделено 2 типа сервисов:

1. Образовательные сервисы – сервисы, которые содержат описание и детали всех IT – услуг, необходимых техническому вузу для обеспечения образовательной деятельности. Данные IT - сервисы будут использоваться студентами, абитуриентами, преподавателям, аспирантам и др.

2. Управленческие сервисы – сервисы, которые содержат описание и детали всех IT – услуг, необходимых техническому вузу для обеспечения управленческой деятельности. Данные IT – сервисы будут использоваться сотрудниками административно – управленческого аппарата для решения задач управления вузом.

Для разработки базового набора IT сервисов для обеспечения деятельности технического вуза, был проведен анализ структуры технического ВУЗа. На основе полученных данных была создана (рис.2) модель процессов жизненного цикла деятельности ВУЗа



Рис.2 – Модель процессов жизненного цикла деятельности ВУЗа

На входе модели мы имеем «контингент на обучение». Это абитуриенты, поступившие в высшее учебное заведение. Пройдя процесс обучения, они преобразуются в выходные данные «дипломированные специалисты, бакалавры, магистры».

Модель направлена на постоянное улучшения качества учебного процесса. Контроль учебного процесса имеет обратную связь, что позволяет не только поддерживать процесс обучения на должном уровне, но и постоянно его улучшать.

Для осуществления своей деятельности процессы жизненного цикла включают в себя различные IT-сервисы. Рассмотрим взаимосвязи процессов и IT-сервисов.

Учебный процесс использует следующие IT-сервисы:

* Электронную библиотеку;
* Систему LMS;
* Сервис печати и копирования;
* Web-сайты;
* Сервис web-конференций (вебинары);
* Файловое хранилище;
* Медицинский сервис;

Процесс информационно-технологического обеспечения включает в себя:

* Управление рабочими местами
* Управление телефонией
* Управление печатью и копированием
* Управление системами хранения и резервирования данных
* Управление системой электронной почты
* Управление корпоративными системами документооборота
* Управление корпоративными порталами и web – сайтами
* Системное и сетевое администрирование
* Управление информационной безопасностью

Отдел кадров использует следующие IT-сервисы:

* Сервис печати и копирования
* Сервис телефонии
* Систему документооборота
* Электронную почту
* Файловое хранилище

Процесс разработки учебной и учебно-методической документации использует следующие IT-сервисы:

* Интернет издательство
* Файловое хранилище
* Сервис печати и копирования
* Электронная-библиотека

В результате мы получили набор IT-сервисов, который необходим для обеспечения деятельности ВУЗа:

* Управление рабочими местами
* Управление телефонией
* Управление печатью и копированием
* Управление системами хранения и резервирования данных
* Управление системой электронной почты
* Управление корпоративными системами документооборота
* Управление корпоративными порталами и web – сайтами
* Системное и сетевое администрирование
* Управление информационной безопасностью
* Система LMS
* Файловое хранилище
* Медицинский сервис
* Интернет издательство
* Электронно-библиотечная система
* Сервис web-конференций (вебинары)

**6.2. Разработка процессной архитектуры комплекса предоставления IT-услуг на базе ITSM**

Процесс изображается в виде блока (Рисунок 2). Входная стрелка, примыкающая к блоку слева, обозначает входы процесса. С ее помощью описывают ресурсы , которые перерабатывается в рамках процесса. Соответственно, выходная стрелка, примыкающая к блоку справа, изображает выходы процесса. С помощью этой стрелки обозначается продукция, производимая в рамках процесса.

Входы и выходы процесса могут быть как нематериальными, так и материальными (например, информационными) объектами. Примерами входов и выходов являются: материалы, компоненты, комплектующие изделия, информация и т.п.

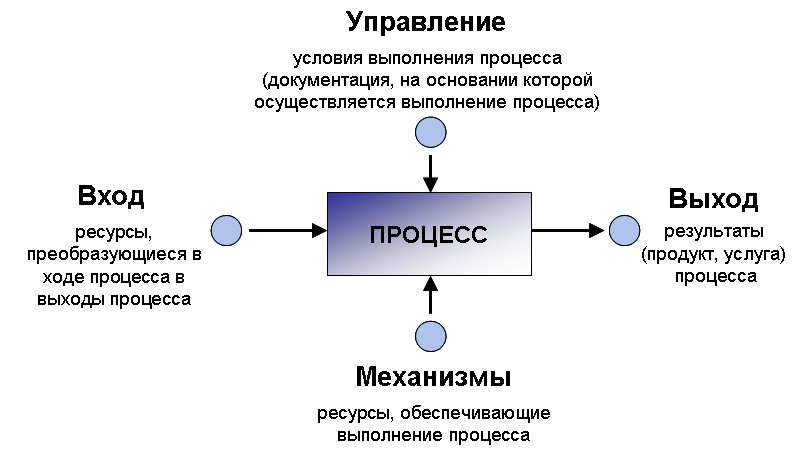


Рис. 3 – схема процесса

Далее опишем базовый набор IT-сервисов с помощью процессного подхода.

1.Управление рабочими местами персонала института

|  |  |
| --- | --- |
| Название IT-сервиса | Управление рабочими местами персонала института |
| Описание IT-сервиса | Выполнение работ по обеспечению и поддержке работоспособности оборудования и ПО рабочего места |
| Измеряемые параметры | Количество рабочих мест.  Количество обращений по категориям(запрос на обслуживание, инцидент) |
| Состав IT-сервиса | Service Desk.  Поддержка операционных систем и базового программного обеспечения.  Управление данными на рабочих местах.  Управление обновлениями программного обеспечения.  Управление антивирусной защитой. |

Рис.4 – Процесс управления рабочими местами

Данный IT-сервис обеспечивает:

-Выполнение работ по установке и настройке операционных систем и базового программного обеспечения

-Консультирование пользователей по работе базового программного обеспечения

-Решение инцидентов в работе операционных систем и программного обеспечения

-Сборка, модернизация и мелкий ремонт настольных и мобильных персональных компьютеров

-Подключение персональных компьютеров и ноутбуков к сетям передачи данных

-Установка, подключение и мелкий ремонт телефонных аппаратов

-Восстановление данных из резервной копии

-Выполнение обновлений программного обеспечения

-Установка антивирусного программного обеспечения на рабочие станции

-Обновление антивирусных баз

-Лечение от вирусов

1. Управление телефонией

|  |  |
| --- | --- |
| Название IT-сервиса | Управление телефонией |
| Описание IT-сервиса | Обеспечение работоспособности и поддержка оборудования телефонии и сетей |
| Измеряемые параметры | Количество площадок.  Количество телефонного и факсимильного оборудования. |
| Состав IT-сервиса | Управление телефонной и факсимильной связью.  Управление мобильной связью. |



Рис.5 – Процесс управления телефонией

Данный IT-сервис обеспечивает:

|  |
| --- |
| -Монтаж и демонтаж оборудования телефонной и факсимильной связи  -Настройка оборудования телефонной и факсимильной связи  -Подключение оборудования телефонной и факсимильной связи к инженерным сетям  -Коммутация входящих/исходящих линий  -Профилактическое обслуживание оборудования телефонной и факсимильной связи  -Решение инцидентов в работе оборудования телефонной и факсимильной связи  -Учет устройств мобильной связи  -Решение инцидентов в работе устройств мобильной связи   1. Управление печатью и копированием |

|  |  |
| --- | --- |
| Название IT-сервиса | Управление печатью и копированием |
| Описание IT-сервиса | Обеспечение работы оргтехники |
| Измеряемые параметры | Количество площадок    Количество устройств по типам |
| Состав IT-сервиса | Управление устройствами копирования и печати.  Управление расходными материалами.    Управление системой сетевой печати.    Управление сетевой печатью.  Управление персональной печатью .  Управление устройствами сканирования |



Рис.6 – Процесс управления печатью и копированием.

Данный IT-сервис обеспечивает:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| -Развертывание систем сетевой печати  -Устранение мелких неполадок в работе оргтехники  -Ремонт малой оргтехники    -Закупка, учет и замена расходных материалов  -Решение инцидентов в работе систем сетевой печати и оргтехники  -Подключение устройств печати к рабочей станции и настройка  -Консультирование по вопросам работы с оргтехникой  -Настройка устройств сканирования  -Решение инцидентов с устройствами сканирования  -Консультирование по работе с устройствами сканирования  4.Управление системами хранения и резервирования данных.   |  |  | | --- | --- | | Название IT-сервиса | Управление системами хранения и резервирования данных. | | Описание IT-сервиса | Обеспечение работоспособности систем хранения данных и систем резервного копирования, а также выполнение процедур резервного копирования | | Измеряемые параметры | Количество систем хранения данных и резервирования  Объем копируемой информации | | Состав IT-сервиса | Управление оборудованием хранения данных    Управление системой резервного копирования и восстановления данных    Резервное копирование и восстановление данных |     Рис.7 – Процесс хранения и резервирования данных.  Данный IT-сервис обеспечивает:  -Монтаж и демонтаж систем хранения данных  -Настройка оборудования систем хранения данных  -Профилактическое обслуживание систем хранения данных  -Ремонт и модернизация оборудования систем хранения данных  -Решение инцидентов в работе оборудования хранения данных  -Настройка систем резервного копирования и восстановления данных  -Настройка процедур резервного копирования по расписанию  -Резервное копирование данных  -Восстановление данных из резервной копии  -Решение инцидентов в работе систем резервного копирования и восстановления данных  -Мониторинг доступности оборудования систем хранения данных и резервного копирования   1. Управление системой электронной почты  |  |  | | --- | --- | | Название IT-сервиса | Управление системой электронной почты | | Описание IT-сервиса | Управление электронной почтой | | Измеряемые параметры | Количество серверов почты | | Состав IT-сервиса | Управление электронной почтой |   Рис.8 – Процесс управления электронной почтой  Данный IT-сервис обеспечивает:  -Развертывание и базовая настройка сервера электронной почты  -Создание почтовых ящиков  -Решение инцидентов в работе системы электронной почты  -Консультирование по работе с электронной почтой   1. Управление корпоративными системами документооборота  |  |  | | --- | --- | | Название IT-сервиса | Управление корпоративными системами документооборота | | Описание IT-сервиса | Обеспечение работоспособности и сопровождение систем документооборота | | Измеряемые параметры | Количество серверов системы  Количество баз данных системы  Количество пользователей системы | | Состав IT-сервиса | Поддержка серверов системы  Управление серверными операционными системами    Управление серверным ПО системы    Сопровождение систем управления базами данных    Поддержка клиентского ПО системы  Дополнения и изменения в функционале системы |     Рис.9 – Процесс управления корпоративными системами документооборота  Данный IT-сервис обеспечивает:  -Поддержка серверов системы  -Управление серверными операционными системами  -Управление серверным ПО системы  -Сопровождение систем управления базами данных  -Поддержка клиентского ПО системы  -Дополнения и изменения в функционале системы  -Настройка серверов  -Профилактическое обслуживание серверов системы  -Ремонт серверов системы  -Решение инцидентов в работе серверов системы  -Развертывание и базовая настройка серверных операционных систем  -Обновление серверных операционных систем  -Решение инцидентов в работе серверных операционных систем  -Развертывание и базовая настройка серверного программного обеспечения системы документооборота  -Обновление серверной части системы  -Мониторинг работоспособности серверной части системы документооборота  -Решение инцидентов в работе серверной части системы  -Развертывание и базовая настройка программного обеспечения системы управления базами данных  -Управление базами данных (создание, удаление, настройка)  -Управление доступом к базе данных   1. Управление корпоративными порталами и web - сайтами  |  |  | | --- | --- | | Название IT-сервиса | Управление корпоративными порталами и web - сайтами | | Описание IT-сервиса | Сопровождение и развитие корпоративных порталов и web-сайтов | | Измеряемые параметры | Количество порталов и web-сайтов | | Состав IT-сервиса | Управление корпоративными порталами  Управление корпоративными web-сайтами |     Рис.10 – Процесс управления корпоративными порталами и web-сайтами  Данный IT-сервис обеспечивает:  -Развертывание и базовая настройка программного обеспечения web-сервера, портала  -Настройка web-сервера, портала  -Решение инцидентов в работе программного обеспечения web-сервера, портала  -Обновление программного обеспечения web-сервера, портала  -Управление доступом к web-сайту, порталу  -Управление контентом (добавление, удаление, модификация)   1. Системное и сетевое администрирование.  |  |  | | --- | --- | | Название IT-сервиса | Системное и сетевое администрирование | | Описание IT-сервиса | Комплексное администрирование информационных систем и локальной вычислительной сети | | Измеряемые параметры | Количество площадок  Количество пользователей  Количество виртуальных серверов  Количество сетевых устройств  Количество устройств телефонной и факсимильной связи  Количество устройств хранения данных  Количество серверных ОС по платформам o MS Windows  o UNIX, LINUX, BSD и т. п.  Количество баз данных | | Состав IT-сервиса | Управление серверными операционными системами  Управление базовыми сетевыми службами  Управление службой единого каталога  Управление системой централизованного обновления  Управление системой электронной почты  Управление системой терминального доступа  Управление системой мониторинга инфраструктуры  Сопровождение системы управления инфраструктурой  Сопровождение систем управления базами данных  Управление средой виртуализации  Управление корпоративными порталами  Управление оборудованием хранения данных  Управление системой резервного копирования и восстановления данных  Резервное копирование и восстановление данных  Управление общими файловыми ресурсами |     Рис. 11 – Процесс системного и сетевого администрирования.  Данный IT-сервис обеспечивает:  -Настройка серверов  -Ремонт серверов  -Мониторинг доступности серверов  -Решение инцидентов в работе серверов  -Плановая диагностика серверного оборудования  -Профилактическое обслуживание серверного оборудования  -Развертывание и базовая настройка серверных операционных систем  -Обновление серверных операционных систем  -Профилактическое обслуживание серверных операционных систем  -Решение инцидентов в работе серверных операционных систем  -Мониторинг работоспособности серверных операционных систем  -Развертывание и настройка службы единого каталога  -Создание групп, учетных записей и других элементов  -Управление политиками и правилами службы единого каталога  -Решение инцидентов в работе службы единого каталога  -Развертывание и настройка базовых сетевых служб  -Развертывание и базовая настройка системы централизованного обновления  -Создание пакетов обновлений  -Развертывание и базовая настройка сервера электронной почты  -Создание почтовых ящиков  -Консультирование по работе с электронной почтой  -Решение инцидентов в работе системы электронной почты  -Развертывание и базовая настройка сервера терминального доступа  -Управление доступом к системе терминального доступа  -Решение инцидентов в работе системы терминального доступа  -Развертывание и базовая настройка системы управления инфраструктурой  -Управление объектами инфраструктуры (добавление, модификация, удаление)  -Развертывание и базовая настройка системы мониторинга инфраструктуры  -Управление объектами мониторинга (добавление, модификация, удаление)  -Развертывание и базовая настройка программного обеспечения системы управления базами данных  -Управление базами данных (создание, удаление, настройка)  -Резервное копирование и восстановление баз данных  -Решение инцидентов в работе программного обеспечения системы управления базами данных  -Монтаж и демонтаж систем хранения данных  -Профилактическое обслуживание оборудования систем хранения данных  -Подключение систем хранения данных к инженерным сетям  -Управление резервным фондом расходных материалов систем хранения  -Настройка системы резервного копирования и восстановления данных  -Настройка расписаний резервного копирования  -Восстановление данных из резервной копии  -Создание и поддержка файловых ресурсов  -Управление доступом к файловым ресурсам  9.Управление информационной безопасностью.   |  |  | | --- | --- | | Название IT-сервиса | Управление информационной безопасностью | | Описание IT-сервиса | Управление аппаратными и программными комплексами информационной безопасности | | Измеряемые параметры | Количество пользователей  Количество серверов  Количество сетевого оборудования  Количество рабочих мест | | Состав IT-сервиса | Антивирусная защита серверов  Антивирусная защита рабочих станций  Защита электронной почты от спама  Управление учетными записями службы единого каталога  Защита сетевого оборудования  Защита программного обеспечения  Контроль доступа в сеть Интернет |     Рис.12 – Процесс управления информационной безопасностью.  Данный IT-сервис обеспечивает:  -Развертывание централизованной системы антивирусной защиты  -Установка антивирусного программного обеспечения на серверы и рабочие станции  -Настройка процедур автоматического обновления антивирусных баз  -Лечение от вирусов  -Развертывание системы защиты от спама на почтовом сервере  -Настройка фильтров системы защиты от спама  -Решение инцидентов, связанных с защитой от спама  -Создание, изменение, удаление, блокировка учетных записей службы единого каталога  -Развертывание и настройка аппаратных и программных комплексов сетевой безопасности  -Отслеживание и устранение уязвимостей сетевого оборудования  -Управление доступом к сетевому оборудованию и VPN каналам  -Отслеживание и устранение уязвимостей программного обеспечения серверов и рабочих станций  -Настройка системы контроля доступа в Интернет  -Управление доступом в сеть Интернет  -Решение инцидентов безопасности, связанных с доступом в Интернет  10.Управление системой LMS   |  |  | | --- | --- | | Название IT-сервиса | LMS (Learning Management System) – система управления обучением | | Описание IT-сервиса | Система для управления учебным процессом | | Измеряемые параметры | Количество пользователей  Количество необходимых дисциплин | | Состав IT-сервиса | Управление системой LMS  Взаимодействие преподавателей и студентов  Удаленное обучение студентов |     Рис.13 – Процесс управления системой LMS.  Данный IT-сервис обеспечивает:  -Повышение уровня и качества методической, дидактической, информационной поддержки организации учебного процесса для студентов, преподавателей и административных работников факультетов.  -Вовлечение студентов в учебный процесс  -Создание активного взаимодействия между преподавателем и студентом  -Обучение студентов в удаленном режиме  11. Файловое хранилище   |  |  | | --- | --- | | Название IT-сервиса | Файловое хранилище | | Описание IT-сервиса | Система хранения учебных материалов | | Измеряемые параметры | Количество пользователей  Объем данных | | Состав IT-сервиса | Управление файловым хранилищем  Хранение данных студентов |     Рис.14. – Процесс управления файловым хранилищем.  Данный IT-сервис обеспечивает:  -Хранение файлов  -Обмен файлами  12.Медицинский сервис   |  |  | | --- | --- | | Название IT-сервиса | Медицинский сервис | | Описание IT-сервиса | Система медицинского обслуживания | | Измеряемые параметры | Количество пользователей | | Состав IT-сервиса | Профилактика заболеваний  Стационарное обслуживание |     Рис.15 – Процесс управления медицинским сервисом.  Данный IT-сервис обеспечивает:  -Электронную медицинскую карту для каждого студента  -Стационарное обслуживание  -Оповещение о плановых медицинских обследованиях  13.Интернет издательство   |  |  | | --- | --- | | Название IT-сервиса | Интернет издательство | | Описание IT-сервиса | Подготовка, выпуск и распространение продукции в электронном виде в Интернете | | Состав IT-сервиса | Создание электронной книги или видео |     Рис.16. Процесс управления интернет издательством.  Данный IT-сервис обеспечивает:  -Создание обучающей продукции в электронном виде  -Создание интернет сайтов  -Создание мобильных приложений  14.Электронно-библиотечная система   |  |  | | --- | --- | | Название IT-сервиса | Электронная библиотека | | Описание IT-сервиса | Упорядоченная коллекция разнородных электронных документов | | Измеряемые параметры | Количество пользователей  Количество электронных документов | | Состав IT-сервиса | Управление электронной библиотекой  Удаленное обучение студентов |     Рис.17. – Процесс управления электронно-библиотечной системой.  Данный IT-сервис обеспечивает:  -Доступ к электронным документам разного рода  -Экономию средств  15.Веб-конференция, вебинар   |  |  | | --- | --- | | Название IT-сервиса | Веб-конференция, вебинар | | Описание IT-сервиса | проведение онлайн-встреч или презентаций через [Интернет](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) в режиме [реального времени](http://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D0%B2%D1%80%D0%B5%D0%BC%D1%8F) | | Измеряемые параметры | Количество пользователей | | Состав IT-сервиса | Управление вебинарами  Удаленное обучение студентов |     Рис.18 – Процесс управления вебинарами.  Данный IT-сервис обеспечивает:  -Удаленное обучение студентов в режиме реального времени  -Организацию голосований и опросов |

* 1. **Разработка технической архитектуры комплекса предоставления IT-услуг**

При разработке технической архитектуры комплекса предоставления IT-услуг была применена технология «Power over Ethernet(POE)». Технология позволяет передавать по «витой паре» помимо данных еще и электрическую энергию. Таким образом к беспроводным точкам доступа, IP-камерам и прочему оборудованию не проводится отдельный электрический кабель, что позволяет сохранить интерьер и сэкономить средства.

Для разработки технической архитектуры комплекса предоставления IT-услуг(рис19) требуется:

- Создать инженерные системы и СКС. СКС – это основа инфраструктуры института, предоставляющая возможность свести в единую систему сетевые сервисы: телефонные и локально вычислительные сети, системы безопасности и видеонаблюдения и т.д. Произвести монтаж кабельных трасс, разводка и подключение электрических сетей, установка розеток, оборудование серверной комнаты, установка систем бесперебойного питания, создание систем кондиционирования и вентиляции.

- Создать сетевую инфраструктуру. Произвести монтаж сетевого оборудования, беспроводных сетей Wi-Fi.

- Установить автоматическую телефонную станцию (АТС). Установить и настроить АТС, запрограммировать логику работы, подключение услуг IP – телефонии.

- Установить серверное оборудование. Произвести установку и подключить серверное оборудование, системы резервного копирования, системы хранения данных.

- Установить систему виртуализации серверов. Виртуализация серверов позволяет одновременно функционировать несколько виртуальных машин на одном физическом сервере, что существенно сокращает затраты на оборудование, программное обеспечение, электроэнергию, обслуживание, повышает гибкость и надежность IT – инфраструктуры.

- Внедрить основные сетевые службы на основе протокола TCP/IP. Произвести установку служб DHCP и DNS.

- Внедрить сервера печати. Для обеспечения управления всеми принтерами института. Служат для распределения нагрузки, хранения и управления очередями печати.

- Внедрить СУБД (система управления базами данных). Для обеспечения хранения, доступа и управления базами данных приложений.

- Внедрить сервер управления и защиты интернет трафика. Для обеспечения защиты корпоративной сети от интернет-атак, контроля и управления доступа пользователей в интернет.

- Внедрить сервер резервного копирования. Для обеспечения всей электронной информации института.

- Внедрить сервера антивирусной защиты. Для обеспечения развертывания, управления и обновления антивирусного программного обеспечения.

- Установить рабочие места. Произвести установку и настройку рабочих станций, ноутбуков, телефонов и прочего оборудования.

- Установить периферийную технику. Произвести установку и настройку принтеров, ксероксов, сканеров, многофункциональных устройств и т.д. Настроить сетевые параметры устройств. Установить средства мониторинга и управления периферийным оборудованием.



Рис. 19 – Техническая архитектура комплекса предоставления IT-услуг.

**7.Экспирементальная часть**

Процессная и техническая архитектура комплекса предоставления IT-услуг для подготовки проектной документации и обеспечения деятельности МИЭМ НИУ ВШЭ была применена на практике. Разработки попали в техническое задание на проектирование учебного комплекса:

1.Центральный коммутатор с функцией маршрутизации: Cisco Catalyst WS-C6509-V-E, а также опции к нему:

1.Управляющий модуль («супервизор»): VS-S720-10G-3CXL, 2 шт.

2.16-портовый 10 Гбит Ethernet-модуль: WS-X6716-10G-3CXL, 3 шт.

3.Оптические модули 10 Гбит: X2-10GB-LRМ, 48 шт.

4.Блок питания на 6 кВт: WS-CAC-6000W, 2 шт.

5.Силовой кабель: CAB-AC-2500W-EU, 4 шт.

2.Коммутатор с 24-мя портами 1000BaseT (скорость передачи – 1 Гбит/с у каждого порта) и исходящим портом со скоростью передачи 10 Гбит/с: коммутатор Cisco Catalyst 2960S-24TD-L, приемопередатчик Cisco SFP-10G-LRM (или Cisco SFP-10G-LR при длине ВОК более 300 метров).

3.Коммутатор с 48-ю портами 1000BaseT (скорость передачи – 1 Гбит/с у каждого порта) и исходящим портом со скоростью передачи 10 Гбит/с: коммутатор Cisco Catalyst 2960S-48TD-L, приемопередатчик Cisco SFP-10G-LRM (или Cisco SFP-10G-LR при длине ВОК более 300 метров).

4.Коммутатор с 24-мя портами 1000BaseT (скорость передачи – 1 Гбит/с у каждого порта) и исходящим портом со скоростью передачи 10 Гбит/с с поддержкой технологии PoE: коммутатор Cisco Catalyst 2960S-24PD-L, приемопередатчик Cisco SFP-10G-LRM (или Cisco SFP-10G-LR при длине ВОК более 300 метров).

5.Коммутатор с 48-ю портами 1000BaseT (скорость передачи – 1 Гбит/с у каждого порта) и исходящим портом со скоростью передачи 10 Гбит/с с поддержкой технологии PoE: коммутатор Cisco Catalyst 2960S-48FPD-L, приемопередатчик Cisco SFP-10G-LRM (или Cisco SFP-10G-LR при длине ВОК более 300 метров).

6.Беспроводная точка доступа (БТД), поддерживающая стандарты IEEE 802.11b, IEEE 802.11g и IEEE 802.11n: Cisco Aironet 1140 Series, AIR-LAP1142N-x-K9.

7.Сетевые (протокол IP) переключатели электропитания BayTech.

8.Сервер VoIP (элемент АТС): два центральных процессора Intel Xeon X5660, 48 гигабайт ОЗУ, плата аппаратного преобразования кодеков G.723.1 и G.729 Digium TCE400B, плата для

подключения 4-х потоков E1 c эхоподавлением Digium TE420B и плата на 24 аналоговых FXO линий Digium AEX2400.

9.Телефонный аппарат VoIP с питанием по PoE: Linksys SPA941 или Cisco IP Phone 7911G.

10.Телефонный аппарат VoIP с питанием по PoE и поддержкой видеосвязи: Linksys SPA962.

11.Беспроводной телефонный аппарат VoIP Wi-Fi: Linksys WIP330 или AddPac AP-WP100.

12.ЖК-панель: Sharp PN-E421.

13.Настенный компьютер: ViewSonic VOT132.

**8.Охрана труда**

Осознавая первоочередную важность сохранения жизни и здоровья пользователей любой системы и первоочередной приоритет требований безопасности перед всеми остальными, рассмотрим, какой потенциальный вред пользователю может нанести подобная система.

Все виды опасностей на производстве можно разделить на следующие виды:

1. Механические, такие как удары, падения, поражения высоким давлением, а также иные физические, такие как свет, ионизирующее излучение, звук, электрический ток и тому подобные;

2. Биологические, такие как вирусы, бактерии, грибки, паразиты и так далее;

3. Химические, такие как кислоты, основания, тяжёлые металлы и другие;

4. Заболевания опорно-двигательного аппарата;

5. Психологические, такие как моббинг , эмоциональное выгорание, негативное воздействие среды, принуждающей к нездоровой активности (такой как неумеренное употребление спиртных напитков, курение и так далее) как необходимому условию карьерного роста и интеграции в коллектив.

Важно отметить, что со временем меняются не только непосредственно опасные факторы, как результат научно-технического прогресса, но и представления о них, как официальные, так и неофициальные. Рассмотрим, например, такой вредный фактор как моббинг. Согласно данным аналитической системы Google Trends, слово mobbing является популярным поисковым запросом уже с 2004 года, и, судя по тенденции, было таковым раньше, но только в 2008 начался рост его упоминаний в новостях . Найти же нормативные документы, упоминающие моббинг как официально принимаемый во внимание вредный фактор не удалось вообще.

Рассматривая потенциальный вред от разрабатываемой системы, отметим, что все её компоненты являются исключительно программными средствами, а потому физический вред нанести в той же мере, в которой те аппаратные средства, на которых система выполняется. Однако ни в коем случае нельзя оставлять за пределами рассмотрения потенциальный психологический вред. Так, известно наличие в сети Интернет сайтов, таких как 4chan, длительное пребывание на которых, по мнению многих аналитиков, может приводить к деформации личности.

К счастью, можно сразу сказать, что система позиционирования транспорта не предполагает взаимодействие между её пользователями, а сама по себе, хоть и использует алгоритмы машинного обучения, не является в достаточной мере интеллектуальной, чтобы наносить психический вред самостоятельно.

Таким образом, имеет смысл рассматривать вред, который может нанести система через ЭВМ. Здесь также можно отметить значительное устаревание имеющихся нормативные документов. Так, основной нормативный документ, описывающий санитарные требования к рабочему месту оператора ЭВМ —САНПИН 2.2.2/2.4.1340-03 уделяет большое внимание вопросу рентгеновского излучения ЭЛТ-мониторов, несмотря на то, что те из них, которые могли сохранить работоспособность до 2013 года, гарантированно относятся к поколению, в котором вся необходимая защита встроена в корпус трубки. С другой стороны, такому явлению, как чтению с экрана, уделено недопустимо мало внимания. Такая характеристика как контрастность вообще не рассматривается, считаются только знаки, как будто они все равноценны. При том, что многие люди действительно не осведомлены о том, что контрастность текста измерять нужно, и делать это в чёрно-белом варианте, в связи с чем недопустим, например, светло-зелёный текст на розовом фоне, хотя эти цвета очень легко различить.

Не уделяется там и внимание такому фактору, давно изучаемому специалистами по интерфейсам, но не специалистами по охране труда, как шрифты. А ведь замечено, что неправильно подобранный шрифт может существенно уменьшить время, которое человек может провести за чтением текста, не устав.

Ещё одним фактором является мерцание и быстрая смена картинки. На это тоже нет никаких нормативов, в связи с чем, зная, что серверная часть разрабатываемой системы будет выводить на экран много текста с большой скоростью, авторам работы остаётся лишь порекомендовать пользователям, во избежание раздражения и покраснения глаз, не злоупотреблять использованием консольного интерфейса сервера, отдавая предпочтение графическому клиенту. Нормировать этот параметр не представляется возможным за отсутствием необходимых норм.

Таким образом, несомненно, можно выделить много потенциально негативных факторов в работе с любым программным продуктом, но те требования, которые были предъявлены 10 лет назад и продолжают предъявляться до сих пор, не соответствуют реальным потребностям повышения юзабилити, не могут быть выполнены и не выполняются в современных условиях, при том, что новые опасные факторы не нормируются или нормируются с большим опозданием.

**8.1. Анализ рисков по защите информации**

Информация в организации можно разделить на критичную и чувствительную*.* Критичность информации - значит, что информация может быть доступна там и тогда, когда она потребуется. Критичность информации напрямую связана с критичностью процессов доступа к информации.

Критичность информации может быть следующих видов:

* существенная: информация или интенсивность обработки информации, утрата которой нанесет серьезный или даже непоправимый вред организации;
* важная*:* информация или интенсивность обработки информации, утрата которой нанесет средний, но поправимый вред организации;
* нормальная*:* информация или интенсивность обработки информации, утрата которой нанесет минимальный вред.

Чувствительность информации может быть следующих видов:

* высоко-чувствительная*:* информация высшей чувствительности, утрата которой приведет к значительному вреду для организации.
* чувствительная*:* информация, утрата которой приведет к существенному вреду для организации. Например персональная данные или информация о пользователях.
* внутренняя*:* информация, утрата которой нанесет некоторый ущерб организации. Например телефонные книги.
* открытая*:* информация, свободного доступа.

# Анализ рисков по защите информации:

-Подделка идентификатора пользователя

Объектом риска является существенная информация. Коэффициент ущерба высокий. Возможны потери производительности, затруднения деятельности, финансовые потери. Источником риска являются хакеры. Мотивация умышленная.

**-**Доступ к сети неавторизованных пользователей

Объектом риска является существенная информация. Коэффициент ущерба высокий. Возможны потери производительности, затруднения деятельности, финансовые потери. Источником риска являются хакеры. Мотивация умышленная.

**-**Вредоносное программное обеспечение

Объектом риска является существенная информация. Коэффициент ущерба высокий. Возможны потери производительности, затруднения деятельности, финансовые потери. Источником риска являются вирусы. Мотивация отсутствует.

**-**Ошибки пользователей

Объектом риска является существенная информация. Коэффициент ущерба высокий. Возможны потери производительности, затруднения деятельности, финансовые потери. Источником риска является персонал. Мотивация неумышленная (халатность, небрежность).

**-**Анализ трафика

Объектом риска является существенная информация. Коэффициент ущерба высокий. Возможны потери конфиденциальности. Источником риска являются хакеры. Мотивация умышленная.

-Перехват

Объектом риска является существенная информация. Коэффициент ущерба высокий. Возможны потери конфиденциальности. Источником риска являются хакеры. Мотивация умышленная.

**-**Повреждения в линиях связи

Объектом риска является сеть, рабочий процесс. Коэффициент ущерба средний. Возможны снижения производительности. Источником риска является персонал. Мотивация неумышленная (халатность).

**-**Техническая неисправность компонентов сети

Объектом риска является сеть, рабочий процесс. Коэффициент ущерба высокий. Возможны снижения производительности. Источником риска является системный администратор. Мотивация отсутствует.

**-** Ошибка технического обслуживания

Объектом риска является рабочий процесс. Коэффициент ущерба высокий. Возможны снижения производительности. Источником риска является системный администратор. Мотивация неумышленная (халатность).

-Авария программного обеспечения

Объектом риска является рабочий процесс. Коэффициент ущерба средний. Возможны снижения производительности. Источник риска отсутствует. Мотивация отсутствует

**-**Нелегальный импорт/экспорт программного обеспечения

Объектом риска является рабочий процесс. Коэффициент ущерба высокий. Возможны снижения производительности. Источником риска является системный администратор. Мотивация неумышленная (халатность).

-Ошибочная маршрутизация сообщений

Объектом риска является существенная информация. Коэффициент ущерба высокий. Возможны снижения производительности. Источником риска является системный администратор. Мотивация неумышленная (халатность).

-Ошибки при передаче

Объектом риска является существенная информация. Коэффициент ущерба высокий. Возможны снижения производительности. Источником риска является системный администратор. Мотивация неумышленная (халатность).

-Преднамеренное повреждение

Объектом риска является рабочий процесс. Коэффициент ущерба средний. Возможны снижения производительности. Источником риска является персонал. Мотивация умышленная.

Вывод: Единого способа, который будет гарантировать 100% сохранности данных не существует. Однако создание комплексной концепции безопасности, учитывающей специфику задач конкретной организации, сведет риск потери ценной информации к минимуму.

**9.Вывод**

В рамках данной работы были рассмотрены современные подходы к организации комплекса предоставления IT-услуг, библиотеки, описывающие лучшие из применяемых на практике способы организации работы подразделений и компаний.

В качестве практической части был разработан базовый набор IT-сервисов для обеспечения деятельности технического ВУЗа, а так же разработана процессная и техническая архитектура комплекса предоставления IT-услуг.

Стоит отметить, что в свободном доступе нет аналогов разработанного комплекса предоставления IT-услуг. Разработанный комплекс может быть применен для любого технического ВУЗа.

**10.Список используемой литературы**

# 1. Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов. Москва: РИА "Стандарты и качество", 2004. — 398 с

2. Роб Ингланд. Лайвбук; Введение в реальный ITSM, 2010 – 132 с.

3.COBIT 4.1. Российское издание. Аудит и контроль информационных систем, ISBN 978-5-9901321-1-5; 2008 г

4**.** [Л. Н. Коршунова, Н. А. Проданова](http://www.ozon.ru/context/detail/id/3299562/#tab_person)**.** Оценка и анализ рисков

Издательство [Феникс](http://www.ozon.ru/context/detail/id/4636582/); 2007 г. - 96 с.

5.ГОСТ 12.0.003-86 Опасные и вредные производственные факторы. Классификация

6.Сибаров Ю.Г. и др. Охрана труда на ВЦ. М. 1989.

7.ГОСТ 12.1.030-81 Электробезопасность. Защитные заземления, зануления.

8.САНПиН 1340-03 Гигиенические требования к персональным ЭВМ и организация работы

9.ГОСТ CCБТ 12.1.045-84 Электростатические поля. Допустимые условия на рабочем месте

10.ГОСТ CCБТ 12.1.124-84 Средства защиты от статического электричества

11. ФЗ РФ №181 1999г. «Об основах охраны труда в РФ»