

perimetrix

МЕТОДИКА ВНЕДРЕНИЯ

СИСТЕМЫ УПРАВЛЕНИЯ КЛАССИФИЦИРОВАННЫМИ
ДАННЫМИ ОГРАНИЧЕННОГО ДОСТУПА
PERIMETRIX SAFESPACE

Оглавление

ДОРОЖНАЯ КАРТА	4
МОДЕЛЬ УПРАВЛЕНИЯ	5
Модель управления электронными данными ограниченного доступа	
Цели и задачи	
Типовой состав «Модели управления данными»	
РЕГЛАМЕНТЫ	8
Регламент по работе с электронными данными ограниченного доступа	
Типовой состав Регламента	
ПРОЕКТНАЯ КОМАНДА	9
Роль проектной команды Заказчика	
Подходы к формированию проектной команды	
Роль руководителя Проекта со стороны Заказчика	
РИСКИ ПРОЕКТА	12
Цели и задачи проекта	
Участие бизнеса и управление ожиданиями	
Уровень ответственности руководителя проекта со стороны Заказчика	
БИЗНЕС-КОНСАЛТИНГ	14

Аннотация

Любой бизнес, независимо от размера и сложности, работает в рамках определённой *модели*. Бизнес-модель, в свою очередь, опирается на *инструменты*, дающие возможность её реализовать и ставящие бизнес в более выгодное положение, чем у компаний-конкурентов. Вместе они представляют собой симбиоз, и рассматривать их по отдельности не имеет смысла.

Созданием или внедрением цифровых инструментов компании занимаются не самостоятельно, а привлекая специалистов из ИТ-отрасли. В случае внедрения готовых решений — консультантов компании-вендора или ее партнеров.

Как любая сфера деятельности, данная отрасль работает по своим правилам и имеет специфику. Учитывая особенности проектной работы, бизнес может получить гораздо лучший результат опираясь или принимая в расчет эти правила, чем если будет их игнорировать.

Система Perimetrix SafeSpace — это тоже цифровой инструмент, предназначенный для классификации электронных данных ограниченного доступа

и управления ими. Последнее осуществляется с помощью применения ограничительных политик хранения, обработки и передачи данных, настраиваемых в соответствии с требованиями организации.

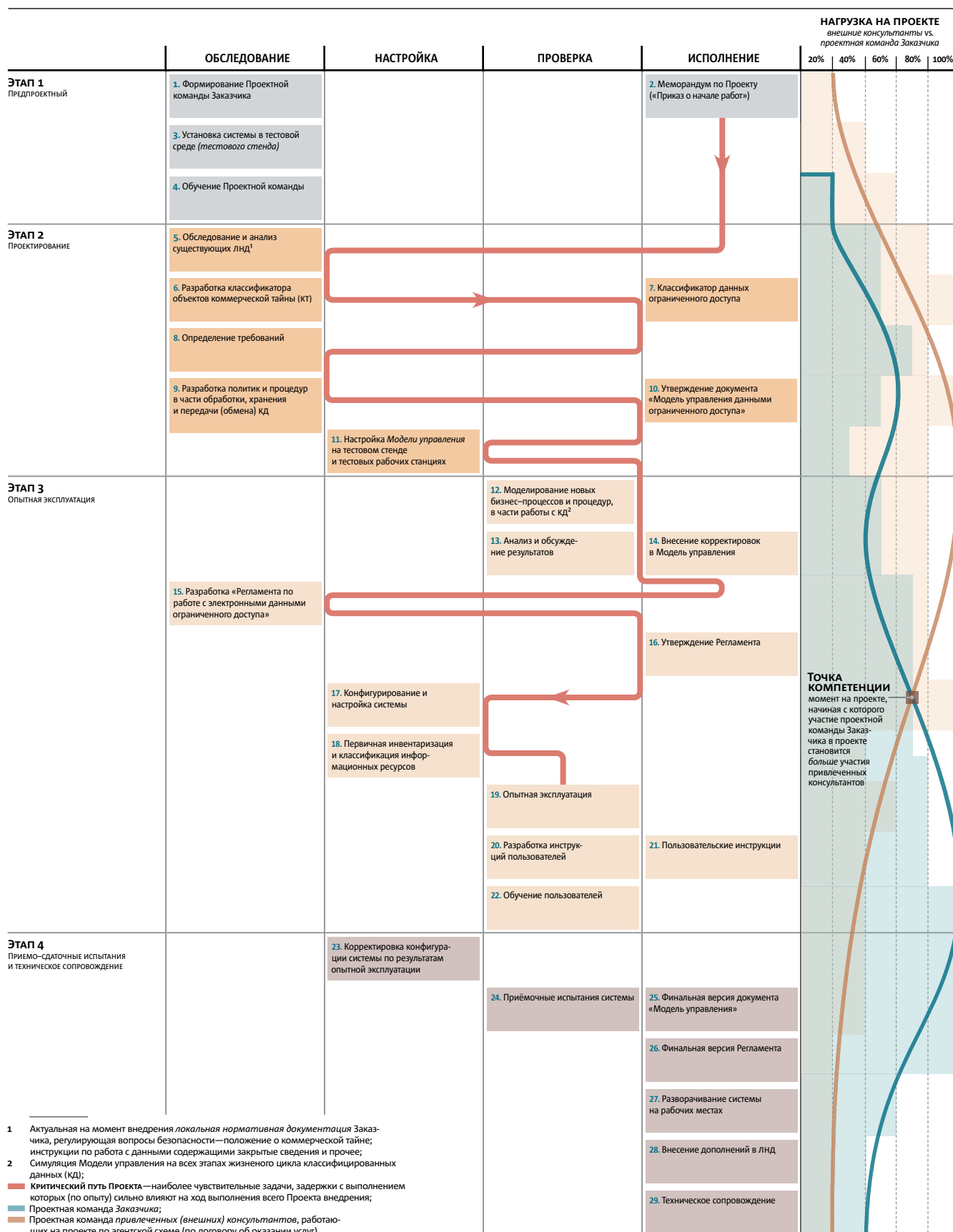
Perimetrix — это готовое решение, но его использование требует некоторого количества подготовительных процедур, мероприятий и документов, необходимых для настройки системы под нужды Заказчика. Все это в совокупности составляет методику внедрения Perimetrix, которая излагается в данном документе.

В этом документе обобщаются основные принципы внедрения Perimetrix, опробованные на реальных проектах, у клиентов с разной отраслевой принадлежностью, а так же даются рекомендации организационного и методического характера для наиболее эффективной организации работ.

Предполагается, что изложенные подходы и правила будут интерпретированы как некоторые универсальные рекомендации и окажутся востребованы в прикладном плане как клиентами, так и партнерами нашей компании.

Дорожная карта

Типовой состав и очередность работ по внедрению



Модель управления

Модель управления электронными данными ограниченного доступа

Система управления классифицированными данными Perimetrix SafeSpace включает в себя заранее спроектированные и опробованные решения и программные компоненты, чей набор и возможная конфигурация определены возможностями программного продукта.

Настройки Perimetrix представляет собой процесс с заранее известным набором параметров, значения которых необходимо выяснить в самом начале, на этапе предпроектного обследования и формализовать

Модель (фр. *modèle* от лат. *modulus* «мера, аналог, образец») — есть абстрактное представление реальности в какой-либо форме, предназначенное для представления определённых аспектов этой реальности и позволяющее получить ответы на изучаемые вопросы.

в виде документа, называемого «Модель управления электронными данными ограниченного доступа».

Модель управления — это *руководящий документ*, ключевой артефакт внедрения системы Perimetrix.

Первое для чего он предназначен, это переложить будущие настройки программного продукта в терминах корпоративной цифровой среды и существующей локальной нормативной документации Заказчика.



Этот документ описывает жизненный цикл электронных данных ограниченного доступа в терминах системы Perimetrix. Основная цель при его разработке — снижение неопределенности проекта внедрения и в конечном счете получение бизнесом именно того результата, на который он изначально рассчитывает получить от использования продуктов Perimetrix.

Большое значение здесь имеет и само знание о наличии неопределенности, и ее локализация в отдельных частях проекта. В этом контексте можно утверждать, что Модель управления данными, будучи проработанной с требуемым уровнем детализации, сводит эту неопределенность к минимуму, уменьшая тем самым риски проекта.

И здесь мы говорим в первую очередь об организационной стороне вопроса — начиная от необходимости получить ясный набор требований к Системе до решения вопросов, связанных с поиском специалистов нужной квалификации в проектную команду на стороне Заказчика.

Модель управления данными — ключевой инструмент проектирования будущей системы. Если ошибка будет обнаружена в момент его подготовки, цена этого будет несопоставимо ниже, чем если бы проблема выяснилась уже на этапе реализации. Говоря более образно, проектируя, мы позволяем умереть плохим идеям, а не готовому продукту.

Здесь первоочередную роль играют представители бизнеса — владельцы данных. Если же аспектом участия бизнеса в проектировании пренебречь, то вместо проработанной проектной документации Заказчик рискует получить фрагментарный набор функциональных требований, по странной традиции иногда именуемый «техническим заданием».

Цели и задачи

«Модель управления данными» призвана обеспечить решение следующих задач:

Модель управления данными ограниченного доступа отвечает на три вопроса: *что, кто и как*. Что защищаем; кто может получить доступ к тому, что защищаем; и как этот доступ может быть реализован — в смысле регламентированных вариантов обработки, передачи и хранения данных. Он описывает детальную модель «доступа» пользователей, приложений (процессов), устройств и к классифицированным информационным объектам, находящихся под управлением системы. В идеале этот документ должен служить дополнением к «Положению о коммерческой тайне» Заказчика и другим локальным нормативным актам, определяющим политики обращения электронных данных, содержащих закрытые сведения.

ОПРЕДЕЛЕНИЕ СОСТАВА объектов защиты, существующих ограничительных политик доступа и описание существующих процессов обработки защищаемых данных;

КЛАССИФИКАЦИЯ ОБЪЕКТОВ защиты в соответствии с требованиями Заказчика и нотациями Perimetrix;

РАЗРАБОТКА ПОЛИТИК доступа к классифицированным объектам защиты и политик хранения, обработки и передачи классифицированных электронных данных ограниченного доступа;

ОПИСАНИЕ рабочих процессов по созданию, сохранению, обработке и передаче классифицированных электронных данных, включающее:

1. список рабочих станций, на которых возможна обработка классифицированной информации заданной категории;
2. список пользователей (учетных записей), имеющих доступ к обработке такой информации;
3. список допустимых для обработки приложений;
4. список допустимых для хранения файловых форматов;
5. определение допустимых мест хранения информации, в том числе сетевых папок, СУБД и прочих сетевых ресурсов;
6. список разрешенных к использованию периферийных устройств;
7. список разрешенных для печати принтеров;
8. схемы бизнес-процессов обработки данных с учетом разрешенных мест хранения и используемых приложений;
9. процедуры раскрытия защищаемых сведений третьим лицам.

Типовой состав «Модели управления электронными данными ограниченного доступа»

Ниже представлено примерное наполнение «Модели управления» по разделам.

Раздел 1: «Сведения о проекте». Определяет цели и задачи проекта; описывает какая информация относится к конфиденциальным данным ограниченного доступа; дает верхнеуровневое определение актуальных угроз информационной безопасности классифицированных данных.

Раздел 2: «Исходные сведения о защищаемых данных». Классифицирует типы документов ограниченного доступа по функциональному признаку (например, корпоративный документооборот, планово-экономический отдел, управление персоналом и т.д.) и корреспондирующим информацион-

ным системам (систем бухгалтерского учета, базам данных и проч.); далее для каждого из классифицированного типа документов делается описание процесса обработки – этапов жизненного цикла документа – сбора, использования, передачи, хранения и уничтожения.

Раздел 3: «Оргструктура обработки конфиденциальных данных». Задаёт перечень структурных подразделений и наименование сведений ограниченного доступа, обрабатываемых с их участием.

Раздел 4: «Общие принципы построения системы».

Раздел 5: «Объекты защиты». Содержит реестр всех информационных систем, задействованных в обработке классифицированных данных, с указанием соответствующего кода объектов защиты, определенных ранее в «Исходных сведениях».

Раздел 6: «Классификационные измерения и уровни». Вводит понятие классификации данных (см. вставку ниже), классификационных измерения и уровней, исходя из целей и задач проекта, политик информационной безопасности и регламентов Заказчика.

Раздел 7: «Допустимые места хранения и каналы передачи». Формирует реестр

классифицированных данных в нотации — *наименование/допустимые места хранения/допустимый канал передачи*.

Раздел 8: «Допустимые программные средства для работы с защищаемыми данными».

Раздел 9: «Полномочия и роли сотрудников». Вводит понятие категории пользователей системы и приводится детальное описание сценариев работы с классифицированными данными для каждой категории пользователей.

Раздел 10: «Политики управления и обработки данных». Дополнение к уже существующим внутренним нормативным документам Заказчика, в котором закрепляются административно-технические правила хранения и обработки данных, реализуемые посредством внедряемой системы Perimetrix.

Раздел 11: «Описание процесса обработки защищаемых данных». Функциональная схема реализации будущей системы с описанием последовательности процесса обработки для каждой категории классифицированных данных, для каждой корреспондирующей информационной системы, входящей в функционально-технический объем проекта.

КЛАССИФИКАЦИЯ ДАННЫХ В PERIMETRIX

Доктрина безопасности Perimetrix строится на DATA CENTRIC SECURITY MODEL (DCSM), *информационно-центричной модели безопасности*. Эта модель была описана¹ в 2007 г. и заключается в том, что классификация данных должна коррелировать с их *значимостью* для бизнеса. В практическом смысле это означает, что уровень защиты данных должен соответствовать их бизнес-ценности.

Такой подход позволяет наладить корректную связь между технической компетентностью ИБ-специалистов и осведомленностью владельцев данных о роли информации в достижении целей бизнеса.

Он не заменяет, а дополняет традиционную, «гlossкую» классификацию — в разрезе «коммерческая тайна», «конфиденциальная информация», «персональные данные» и прочее. Вся информация ограниченного доступа классифицируется так, чтобы обеспечить требуемую *гранулярность* назначения полномочий субъектам управления. Например — по уровню секретности (*чувствительности*) и смысловой принадлежности данных (*владельцу*).

1. "Elevating the Discussion on Security Management — The Data Centric Paradigm" by IBM RESEARCH, IBM SECURITY & PRIVACY SERVICES, ZURICH FINANCIAL SERVICES; "Enterprise Security: A data-centric approach to securing the enterprise" by AARON WOODY

Последнее позволяет классифицировать объекты в *бизнес-контексте* и управлять атрибутами контроля доступа к данным со стороны пользователей, приложений или ИТ-устройств, с помощью которых реализуется и поддерживается корреспондирующий бизнес-процесс.



ПРИМЕР 1: Многоуровневая классификация
Пример трехуровневой классификации данных в разрезе чувствительность, функциональность и география.

Дополнительная информация: <https://www.perimetrix.com/>

Регламенты

РЕГЛАМЕНТ ПО РАБОТЕ С ЭЛЕКТРОННЫМИ ДАННЫМИ ОГРАНИЧЕННОГО ДОСТУПА

Этот документ, так же как и «*Модель управления*», является руководящим. Он разрабатывается на третьем этапе проекта, параллельно с настройкой тестовой конфигурации системы.

Он содержит описание правил, политик, ограничений и инструкций в части обработки, хранения и передачи электронных данных ограниченного доступа, содержащие защищаемые сведения Заказчика, и находящиеся под контролем системы управления электронными данными ограниченного доступа на базе специального программного обеспечения Perimetrix SafeSpace.

Его назначение — детальное описание сценариев взаимодействия пользователей с продуктом, в зависимости от установленной классификации и разработанных политик безопасности.

В нем, в частности, подробно описывается порядок действий, выполняемых в ходе рабочих процессов, связанных с обработкой хранением и передачей электронных данных, находящихся под контролем системы Perimetrix.

Он содержит описание правил (политик и ограничений) и инструкций в части обработки, хранения и передачи электронных

данных ограниченного доступа, составляющих защищаемые сведения Заказчика.

Отправной точкой для разработки Регламента являются результаты проектирования, полученные на 2-м этапе а так же локальные нормативные документы Заказчика — «Положение о коммерческой тайне», «классификатор данных, содержащих закрытые сведения» и другая локальная нормативная документация, регламентирующая вопросы информационной безопасности Заказчика.

Типовой состав Регламента

Разработанный и утвержденный Регламент должен содержать как минимум следующие сведения (**этап 3**):

- *защищаемые сведения*, состав и классификация данных ограниченного пользования;
- *права и обязанности пользователей* системы;
- *общие требования* по работе пользователей;
- *режимы работы пользователей* с информацией ограниченного доступа;
- *настраиваемые политики работы* с файлами, содержащими закрытые сведения;
- *порядок по работе пользователей* с классифицированными данными — детальные инструкции по обращению с информацией ограниченного доступа на всех этапах жизненного цикла (*чтение, запись, хранение, перемещение и так далее*), специфичных для данной установки системы и существующих бизнес-процессов Заказчика.

«РЕГЛАМЕНТ ПО РАБОТЕ ПОЛЬЗОВАТЕЛЕЙ» является итоговой декомпозицией проектирования системы, с уровня утвержденных в «Модели управления» политик безопасности — через рабочие процессы хранения, обработки и транспортировки данных — до уровня пользователей, приложений и технических средств, участвующих в обработке информации, содержащей закрытые сведения.

Проектная команда

Роль проектной команды заказчика

Проектная команда — это в первую очередь группа профессионалов, способных перевести запросы бизнеса на язык функционально-технических требований к системе Perimetrix. Такая команда специалистов рассматривается как единый механизм, имеющий в своем составе нужный набор компетенций и понимающий текущие запросы бизнеса.

Однако, если бы сложность продукта, а точнее сказать, ИТ-системы, лежащей в основе продукта, равнялась сумме всех ее частей, то потребность в серьезной работе была бы не столь высока.

Но сложность системы определяется взаимосвязями между ее частями. И для того, чтобы определить эти взаимосвязи вместо того, чтобы дать им сложиться хаотично, и нужна проектная команда со стороны Заказчика.

Ее задача — найти наилучший способ организации системы, как с учетом доступных технических возможностей коробочного решения и ограничений, так и с учетом того, как соединяются бизнес-требования Заказчика с конкретным пользовательским опытом.

Другим важным фактором, определяющим важность внутренней проектной команды, является достижение предела возможностей внедряемого продукта в рамках текущих форматов организации проектов и способов привлечения внешних специалистов.

Самый распространенный формат — агентский — постепенно теряет возможность эффективно решать возникающие сейчас у бизнеса задачи. Уровень профессиональных компетенций, требуемый от всех участников современного проекта, намного превышает навыки и опыт, которыми обладает типичный менеджер проекта, привлекаемый со стороны. Как результат, и бизнес, и участники проектной команды вынуждены взаимодей-



ствовать, упрощая обсуждаемые вопросы.

Ни точное определение целей, ни доскональное проектирование в виде проработанной модели защиты не способны устранить фундаментальный источник неопределенности, а именно — действия людей, участвующих в проекте и развертывающих систему на местах.

От принимаемых ими решений зависит в конечном счете успех или неуспех проекта. Поэтому формирование проектной команды — один из ключевых факторов, определяющих успех или неуспех проекта внедрения.

Все вышесказанное дает понять, насколько ответственная задача стоит перед проектной командой Заказчика. Это относится и к техническим решениям, и к решениям на уровне взаимодействия с пользователем и к бизнес-сценариям.

Иногда ситуацию спасает наличие необходимой компетенции со стороны компании, предоставляющей услуги по внедрению — будь то сам вендор, или компания-партнер. Но в конечном счете, чтобы проект не был лотереей, бизнес сам должен обладать пониманием критериев и подходом для выбора подходящих специалистов.

В идеале на стороне бизнеса должны быть люди, понимающие задачи, которые ставятся перед проектом, и одновременно разбирающиеся в ИТ-индустрии. В противном случае он становится заложником целей компании-поставщика, переплачивая за человека-часы внешних консультантов.

Любой работающий ИТ-продукт эволюционирует вместе с бизнесом. Когда бизнес создан и работает, то из-за изменений внешней среды он требует постоянного обновления. Такие обновления могут носить эволюционный характер, когда идет постепенное развитие инструментов и бизнес-процессов, но сама бизнес-модель не меняется.

Если же обстоятельства таковы, что для продолжения деятельности недостаточно простой адаптации, могут потребоваться серьезные изменения как в самой бизнес-мо-

дели, так и в инструментах, ее поддерживающих.

И в первом и во втором случае проектная команда со стороны Заказчика играет в этом процессе ведущую роль, сонастраивая цифровые продукты Perimetrix и меняющиеся потребности бизнеса.

Подходы к формированию проектной команды

Любой, кто хотя бы однажды занимался организацией проекта, понимает, что для получения нужного результата недостаточно просто привлечь правильных специалистов. Необходимо задать правила и построить работу таким образом, чтобы у каждого участника проектной команды был мотив и возможность реализовать свой профессиональный потенциал. Как только людей становится больше одного, встает вопрос взаимодействия в команде и того, по каким принципам строится работа в целом

Выбор специалистов в команду должен определяться объективными потребностями, вытекающими из целей и типа проекта, а также технологическими особенностями внедряемой системы

Важную роль играет персональная слаженность членов проектной команды. Только дилетанты выстраивают проектную работу с точки зрения чистых ролей без учета специфики каждого участника, забывая, что люди в одном случае могут тратить свои силы на борьбу друг с другом, а в другом — на достижение общих целей, что одновременно позволяют им достичь их собственных

Последним по очередности, но не по значению фактором, является уровень доверия к членам проектной команды со стороны бизнеса, без которого бизнес будет вынужден ограничивать их свободу действий формальными процедурами. Только имея достаточно полномочий, участники проектной команды смогут реализовать свои возможности.

Роль руководителя проекта со стороны заказчика

На проекте должен быть *один человек*, имеющий полномочия принимать окончательное решение. Речь, конечно же, не идет о безответственном самоуправстве, когда отвергается здравый смысл и игнорируются изначальные цели.

Но в ситуации, при которой у участников проекта не получается договориться, необходим тот, кто возьмет на себя ответственность.

Отсутствие сильного лидера проекта — не менее опасный источник рисков, чем и остальные (см. *подробнее в следующем разделе «Риски проекта»*).

Как и в любой работе, по ходу проекта внедрения регулярно возникает большое количество разной степени важности вопросов. Некоторые из них технические, другие связаны с уточнением требований к продукту, третьи — организационные.

Но в любом случае, если каждый из них не решается своевременно, то вместе с этим нарастает и внутренний «долг» проекта. Например, если вовремя не зафиксировать

функциональные требования к системе и продолжить работу, то в какой-то момент может выясниться невозможность совместить все функции, т.к. они не согласуются друг с другом. По итогу цена такой ситуации для бизнеса может быть значительно выше, чем просто стоимость еще нескольких месяцев работы над проектом.

Может показаться, что в роли такого лидера должен выступать представитель бизнеса. Проблема с этим подходом состоит в том, что часто полномочия у такого человека есть, особенно в силу формата отношения заказчик–исполнитель, но готовности нести ответственность за свои решения — нет.

Кроме того, большая часть вопросов связана с технической стороной проекта, поэтому их невозможно разрешить, не обладая профессиональными знаниями, опираясь только на административные инструменты.

Поэтому в роли лидера, наделенного ответственностью и полномочиями для решения вопросов, должен быть специалист, обладающий достаточными компетенциями, чтобы работать на стыке всех аспектов проекта.



Риски проекта

В этом разделе мы постарались обобщить наиболее часто встречающиеся неопределенности и связанные с ними риски внедрения. Данный перечень безусловно не является исчерпывающим и ситуации у Заказчика бывают разные. Поэтому мы приводим только те риски, которые по нашему опыту типичны и наиболее значимы в плане возможного негативного влияния на ход выполнения работ.

Цели и задачи проекта

По-настоящему ключевым источником неопределенности при внедрении является отсутствие четких целей проекта. Исторически сложилось так, что на многих проектах внедрения готовых ИТ-систем бизнес рассматривает технологии как универсальный способ решения своих задач, как своеобразную таблетку от всех болезней. В том числе и организационных. Система Perimetrix — это мощный ИТ-инструмент.

Но инструмент остается инструментом, которым еще нужно суметь воспользоваться. Нет смысла ожидать, что разработчики смогут реализовать бизнес-логику, если Заказчик не способен ее сформулировать. В свою очередь у бизнеса больше шансов получить требуемый результат, если цели открыто обозначаются в начале проекта. Поэтому эти цели должны быть определены в самом начале работ — в нотации, максимально точно отражающей ожидания бизнеса и однозначно интерпретируемой всеми участниками проекта.

Безусловно систему Perimetrix, как и любой цифровой продукт, можно внедрять основываясь только на формальных представлениях о бизнесе, но выполнять она будет функции, также отвечающие формальным, а не действительным целям, т. е. будет малоэффективной. Поэтому при проектировании будущего продукта на базе Perimetrix SafeSpace ключевая задача состоит не только в том, чтобы на основе предоставленных требований найти наиболее подходящее

решение задачи защиты данных конфиденциального характера, а в том, чтобы в принципе разобраться, каковы действительные требования по работе с данными, содержащими закрытые сведения, и оценить эффективность соответствия внедряемого решения этим самым требованиям.

УЧАСТИЕ БИЗНЕСА И УПРАВЛЕНИЕ ОЖИДАНИЯМИ

Комплексный продукт, к которым относится система Perimetrix, подобен растению, которое необходимо вырастить в той среде, где оно будет в дальнейшем жить. Бизнес работает в симбиозе с цифровыми инструментами, опираясь на них, чтобы иметь возможность реализовать определенную модель своей деятельности. Поэтому работа по внедрению системы должна подразумевать постепенную адаптацию и подстройку друг под друга процессов компании и промежуточных настроек продукта.

Совсем иначе обстоят дела в случае, когда бизнес рассчитывает получить «все и сразу». Лишая проектную команду возможности проверять на практике промежуточные гипотезы о том, насколько работоспособны проектные решения в реальной среде, бизнес накапливает в проекте неопределенность.

Дело в том, что первоначальные требования к проекту строятся на предположениях о том, как работает компания. Они могут исходить как от руководства, так и от рядовых сотрудников. Но и те и другие никогда не видят всей картины в целом, потому что любые представления — это лишь упрощенная модель реальности. И даже если предположить, что изначальная модель верна, то за время, пока идет работа над проектом, какие-то аспекты первоначальной постановки задачи могут поменяться.

Подобный подход также чреват тем, что бизнес, откладывая свое знакомство с будущим продуктом, завышает свои ожидания и рассматривает его как панацею от всех проблем. Именно поэтому часто по ходу проекта, еще до его завершения, появляется большое

количество дополнительных пожеланий и требований к функциональности. Что, конечно же, только усугубляет нарастающее несоответствие между реальными потребностями и итоговым результатом проекта.

Лучшей иллюстрацией того, какой эффект оказывает непонимание бизнесом своей ответственности за результаты проекта, является ситуация, когда практически готовая система презентуется руководителям бизнеса.

В реальной жизни часто бывает ситуация, когда топ-менеджер считает себя вправе дать оценку и высказать пожелания о том, как почти готовый продукт нужно доработать, и это при том, что ни разу не уделил внимания проекту в процессе работы над ним.

Очевидно, что на момент демонстрации проект прошел весь путь от формирования концепции продукта, проектирования, дизайна до разработки и тестирования. Количество взаимосвязанных и взаимоувязанных деталей в сложной системе, которой является такой продукт, огромно. Любая попытка внести хоть сколько-нибудь значимые изменения приводят к необходимости пересмотра большинства принятых решений и как следствие прохождению всего цикла проектных стадий.

Бизнес традиционно считает, что ответственность лежит на исполнителях, не заметивших «очевидные ошибки», на которые ему приходится указывать. Исполнители в свою очередь апеллируют к тому, что обсуждаемые замечания не были описаны в изначальных требованиях.

Бизнесу, чтобы избежать такого развития событий, стоит признать, что на нем в равной степени лежит ответственность за результаты проекта, и поменять формат своего участия в работе. Руководители должны быть вовлечены в принятие принципиальных решений на протяжении всего хода проекта, так, чтобы неопределенность в проекте не накапливалась скрыто и к моменту его завершения все замечания были учтены в наиболее подходящие для этого моменты. При таком подходе работающая система будет плодом совмест-

Участие владельцев данных в принятии принципиальных решений по проекту — залог адекватного отражения требований Заказчика в реализации системы. Чем раньше бизнес начнет знакомиться с промежуточными результатами внедрения — тем меньше риски возникновения отложенных требований к системе или части реализуемого функционала

ной деятельности сторон и не потребуется дополнительное время на его доведение.

УРОВЕНЬ ОТВЕТСТВЕННОСТИ РУКОВОДИТЕЛЯ ПРОЕКТА СО СТОРОНЫ ЗАКАЗЧИКА

Каждый из участников проекта рассматривает проект и принимает решения исходя из той картины, которая открывается его мысленному взору из той точки и той роли, в которой он находится. А значит, среди них должны быть специалисты, кто может охватить систему единым взглядом. Это касается всех аспектов проекта, особенно если рассматривать систему Perimetrix как составляющую часть бизнес-модели компании.

Если человек с нужным уровнем ответственности появится в проекте только в конце, то это будет означать, что в течение всего проекта работа строилась на неподтвержденных гипотезах, и, когда начнется их проверка, многие решения будут пересмотрены, а вместе с ними и результаты всей работы

Еще один важный аспект, касающийся уровня ответственности руководителя проекта — это подготовка и согласование внутри компании проектных решений. Практика показывает, что при недостаточном уровне ответственности принятие ключевых решений затягивается. Затягивание решения проектных вопросов — чаще всего не вопрос злого умысла.

Как правило это связано с тем, что в согласовании требований участвует несколько подразделений компании. Поскольку у каждого из них есть свои собственные цели, то вряд ли они смогут уступить друг другу и, кроме того, не отложить решение на неопределенное время.

Здесь нужен тот, кто видит картину целиком, представляет себе конечный продукт и сфокусирован на его запуске в эксплуатацию. При этом этот человек должен обладать административными навыками и достаточным уровнем ответственности, чтобы координировать и в случае необходимости ускорять принятие управленческих решений внутри Заказчика.

Бизнес-консалтинг

В современном мире лидерами становятся компании, ставящие на первое место связь между бизнес-моделью и цифровыми инструментами. Для того, чтобы такая стратегия была выигрышной, недостаточно работать в привычной манере, рассматривая ИТ в качестве вспомогательной инфраструктуры наряду с офисом и связью, значение которой ограничивается лишь тем, что существующие процессы начинают идти быстрее.

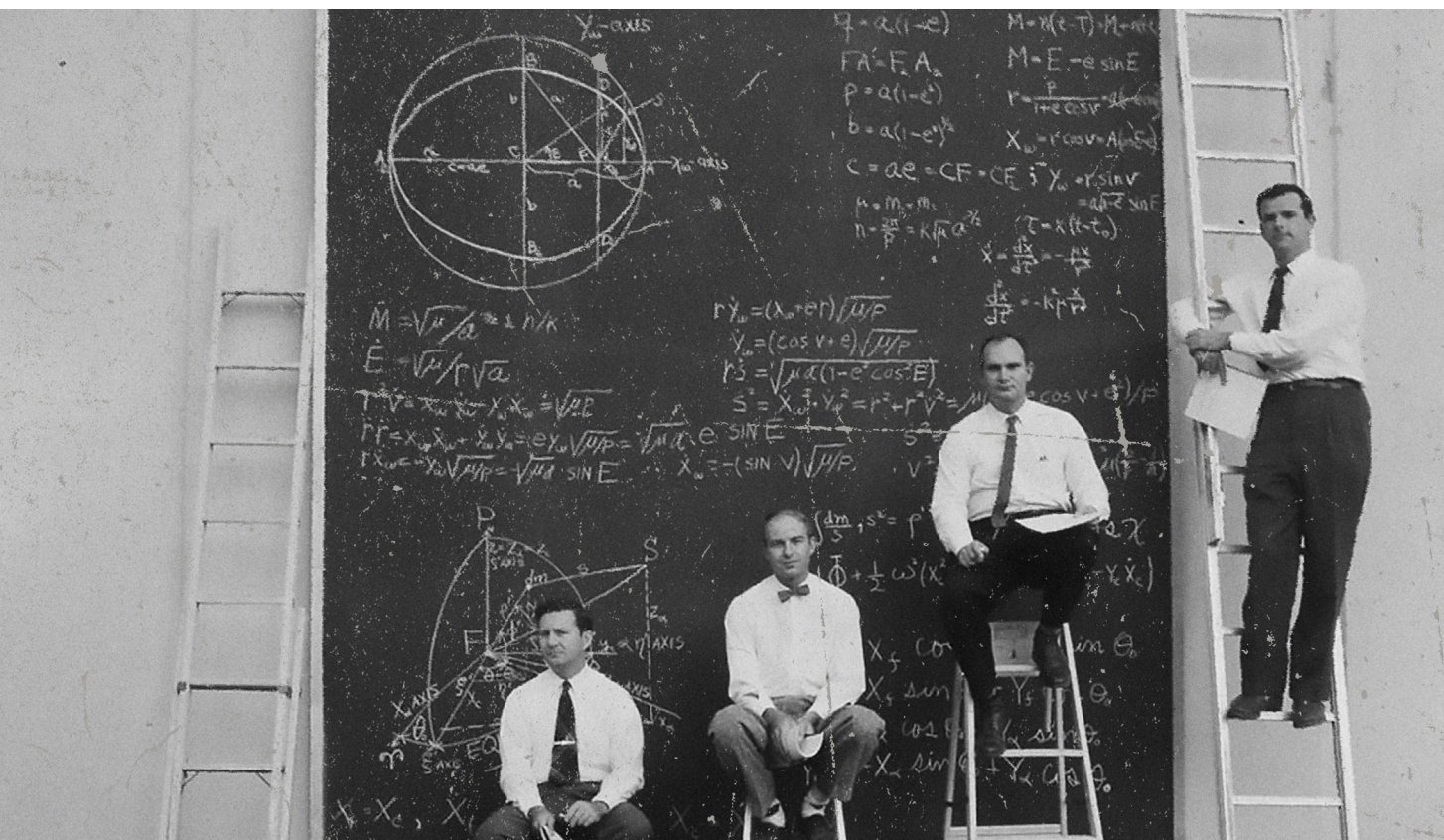
Цифровые системы — сама суть сегодняшнего бизнеса, основа, скелет, вокруг которого выстраивается бизнес-модель. Это не модные слова, а реальность, в которой мы живём.

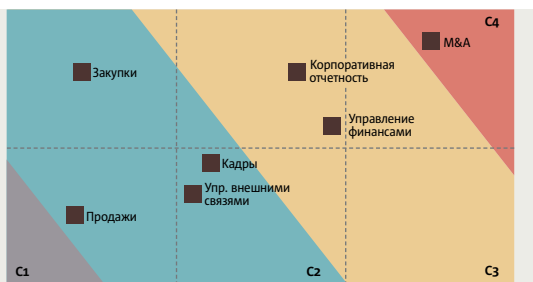
Внешняя среда любой компании все время меняется, то и сама компания должна непрерывно адаптироваться. А значит, любой действующий бизнес находится в постоянном процессе обновления своей инфраструктуры, в том числе и цифровой

Для создания работающих цифровых продуктов, вплетённых в бизнес-модель, требуется ясность относительно этой модели. Кроме того, современные цифровые системы — это вовсе не автоматизация существующих процессов, делающая всё чуть «эффективнее», а основные инструменты, в некотором роде скелет, на котором строится весь бизнес.

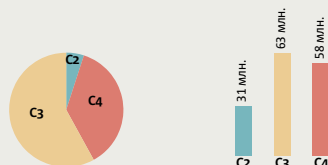
И здесь могут возникнуть вопросы на стыке бизнеса и цифровых технологий — например, какова эффективность внедряемых мер защиты в разрезе долгосрочной стратегии развития компании. Или насколько существующий портфель ИТ-продуктов в области защиты информации соответствует этим самым задачам бизнеса, текущей и прогнозной ситуации на рынках сбыта или конкурентному окружению.

Эти и другие вопросы закрываются в рамках отдельного вида работ, условно





ПРИМЕР 2: КЛАССИФИКАЦИЯ БИЗНЕС-ПРОЦЕССОВ И ДАННЫХ. Классификация данных у одного из операторов мобильной связи (Телеком), по уровням C1–C4, в зависимости от ценности бизнес-процессов, с которыми эти данные связаны. По *горизонтали* – оценочный ущерб в абсолютном выражении от компрометации данных, по *вертикали* – вероятность наступления такого события при существующих у Заказчика организационно-технических мерах безопасности.



ПРИМЕР 3: УДЕЛЬНОЕ РАСПРЕДЕЛЕНИЕ ПО УРОВНЯМ КОНФИДЕНЦИАЛЬНОСТИ. Тот же проект. Разкурс категорирования информационных активов и бизнес-процессов с ними связанных по уровням конфиденциальности. *Слева* — удельное распределение активов по категориям; *справа* — удельная стоимость возможного ущерба от компрометации данных (стоимость активов «под риском»).

именуемого «бизнес-консалтинг». Он может включать в себя, например, следующие задачи:

- Разработка *критериев* оценки эффективности внедрения системы управления классифицированной информацией;
- Разработка *методики* технико-экономического обоснования внедрения системы, которая может включать в себя следующие работы:
 1. определение стоимости информационных активов под риском и потенциального ущерба от их компрометации (AVR, assets value at risk);
 2. расчет стоимости владения системой (TCO, total cost of ownership);
 3. расчет периода окупаемости системы (ROI, return on investment);
 4. рекомендации по разработке методики оценки эффективности внедрения системы управления данными, содержащими закрытыми сведениями. ■

Указанный перечень далеко не полный и приведен здесь исключительно в *иллюстративных* целях. Такие работы не включаются в объем стандартного внедрения и выходят за рамки настоящего документа. Однако они могут быть предоставлены по запросу партнерами компании Perimetrix, имеющими опыт в проведении такого рода работ и обладающих соответствующими компетенциями.

CLASSIFIED

5

perimetrix © 2021 Perimetrix LLC

A Russian company founded in 2007, whose products have been trusted for more than 10 years to protect the confidential data of organizations such as AvtoVAZ, Gazprom Energoholding, the Federation Council of the Federal Assembly of the Russian Federation, TVEL and others. The company has a network of partners in Russia and abroad. The company's headquarters are located in Moscow.



®

© COPYRIGHT. ALL RIGHTS RESERVED

ALL RIGHTS RESERVED. NO PART OF THIS PUBLICATION MAY BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, INCLUDING PHOTOCOPYING, RECORDING, OR OTHER ELECTRONIC OR MECHANICAL METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF THE PUBLISHER, EXCEPT IN THE CASE OF BRIEF QUOTATIONS EMBODIED IN CRITICAL REVIEWS AND CERTAIN OTHER NONCOMMERCIAL USES PERMITTED BY COPYRIGHT LAW.

