31 октября 2024

Как провести ИТ-аудит и сколько это стоит

В зависимости от типа ИТ-аудита и масштаба задач можно снизить операционные затраты до 50%, избежать финансовых потерь от утечек информации и найти новые точки оптимизации ИТ-бюджета. Инструкцию, как это сделать, дает наш эксперт Владимир Бобров. Аудит — комплексная аналитическая работа, целью которой может быть обследование и оценка:

- всего ИТ-ландшафта компании;
- конкретных информационных систем;
- конкретных сервисов.

Это не просто подтверждение актуальности лицензий на ПО, а комплексный анализ всех взаимосвязей между ИТ-системами, поиск несостыковок и вариантов оптимизации.

Зачем и кому нужен ИТ-аудит

Обычно компании сталкиваются с довольно типичными проблемами ИТ-инфраструктуры. Чаще всего **причиной для проведения ИТ-аудита**

1. Непрозрачность ИТ-процессов

Бизнес-заказчик не понимает фактический уровень сервиса и эффективность работы, которые влияют на ИТ-бюджет. Например, бизнесу известен ФОТ,

выделяемый на ИТ, но детализация расходов отсутствует. Аудит выявит, на какие сервисы распределены расходы на поддержку пользователей, лицензии ПО, обслуживание оборудования, и актуализирует информацию по другим статьям бюджета.

Анализ позволит актуализировать матрицу функциональных обязанностей, чтобы оптимизировать трудозатраты. Для этого случая подойдут аудит организационной структуры и бюджетов ИТ и анализ экономической эффективности.

2. Нужно повысить уровень качества, надежности и безопасности ИТ-инфраструктуры

По результатам исследования Positive Technologies, во всех проанализированных компаниях были обнаружены угрозы в инфраструктуре, в 24% — на периметре сети. Согласно данным Group-IB, объем продаваемых в даркнете доступов к корпоративным сетям компаний увеличивается с каждым годом и в 2020 году наблюдался пик утечек: рост продаж доступов в скомпрометированные сети составил 162%.

Аудит и анализ защищенности информационных систем компании помогает обнаружить потенциально опасные места и аномалии, выработать рекомендации, как закрыть уязвимости.

3. Оценка экономической и технологической эффективности ИТ

ИТ-аудит позволяет узнать, какие стандарты приняты в отрасли, соответствует ли подход компании лучшим мировым практикам, что можно улучшить, чтобы поддержать развитие бизнеса. Например, компания планирует вырасти по объему производства продукции, и ей нужно понять, как правильно выстроить логистику: привлечь партнеров или создать собственное

подразделение. Здесь нужен аудит на соответствие лучшим практикам рынка.

4. Нужно улучшить бизнес-процессы

В организации много подразделений и в каждом есть собственные бизнес-процессы по взаимодействию с ИТ: заказ оборудования, организация рабочих мест, запуск новых информационных систем или проведение изменений в текущих. Если процессы похожи в каждом подразделении, но нет общих правил, в этом случае поможет аудит на соответствие методологии управления ИТ-услугами ITSM. Подобный аудит помогает выявить и устранить ситуации в случае, когда бизнес-заказчик и руководитель проекта внедряют новую информационную систему, о которой не знает архитектор ИТ-инфраструктуры.

ИТ-аудит бывает разным

ИТ-аудит можно разделить на **несколько типов** в зависимости от целей.

1. Аудит инфраструктуры с точки зрения лучших практик рынка

Этот формат отвечает на вопрос, соответствует ли ИТ-инфраструктура стандартам отрасли или рекомендациям вендора. Этот тип аудита позволит сравнить текущий уровень развития инфраструктуры и ПО компании с конкурентами и лидерами рынка с учетом требований бизнеса и стратегии компании. Для оценки стоимости аудита необходимо понимать масштаб работ и какие системы предстоит обследовать.

Длительность аудита зависит от сложности инфраструктуры и количества систем, например обследование CRM-системы занимает дни, ERP — недели. Экспресс-аудит базовой инфраструктуры на уровне оборудования, операционной системы и базовых сервисов (таких как AD, СУБД) может стоить от 300 тыс. руб. и проводиться за три недели. Для любого типа аудита

потребуется минимум несколько дней на сбор информации.

2. ИТ-аудит в соответствии со стандартными методологиями управления ИТ-услугами: COBIT, ITIL или ISO 20000

- **ITIL** — это самое распространенное в мире руководство по управлению ИТ-услугами, фокусирующееся на концепции жизненного цикла услуг и операционной модели создания ценности услуг. Набор 34 практик стандарта ITIL 4 позволяет более точно рассмотреть все аспекты ИТ-процессов организации.
- **ISO 20000** — это международный стандарт требований к системе менеджмента ИТ-сервисов, определяющий ответственность за их инициирование, выполнение и поддержку в организациях. Применение методологии позволяет оценивать процессы (предоставления сервисов, управления взаимодействием, контроля, управления релизами) и их эффективность с учетом специфики бизнеса.
- **COBIT** — это методология руководства и управления корпоративной информацией и технологиями, охватывающая всю организацию. Она разработана для интеграции с другими отраслевыми методологиями и стандартами, известными профильным специалистам: ISO, ITIL и TOGAF.

Последняя версия методологии руководства и управления корпоративной информацией и технологиями COBIT 2019 предлагает рекомендации по лучшим практикам для ряда ключевых областей управления ИТ — интеграция ИТ с бизнесом, соответствие требованиям и стандартам, принятым у игроков рынка, поддержание работоспособности ИТ, управление затратами и оптимизация стоимости.

Такое исследование особенно полезно сервисным компаниям, которым необходимо поддерживать высокую скорость решения запросов пользователей, следить за эффективностью ИТ-процессов и повышать Return

on investment (ROI, отдачу от инвестиций). Этот тип аудита занимает, как правило, от двух месяцев.

Стоимость зависит от количества и степени зрелости рассматриваемых ИТ-процессов (управления инцидентами, изменениями, мощностями и инвестициями) в компании. Стоимость подобных проектов обычно начинается от 500 тыс. руб.

3. Аудит экономической эффективности ИТ

Такой аудит помогает навести порядок в программных активах компании и оптимизировать их жизненный цикл. Он позволяет сократить затраты на ИТ без ущерба бизнес-процессам, закрыть риски, связанные с нарушениями условий использования ПО, а также выгодно приобрести только нужные бизнесу лицензии. Исследование может быть проведено при помощи разных методологий, например Software Asset Management (SAM — оптимизация жизненного цикла программных активов в компании) или Solution Assessment (SA — исследование для подбора оптимальной модели ИТ-инфраструктуры и оптимизации инвестиций). Подойдут и другие инструменты качественного анализа с расчетом показателей эффективности ИТ-проектов.

Такой аудит рекомендуют автоматизировать, так как он включает в себя инвентаризацию используемого ПО, нормализацию этих данных, сопоставление с актуальной информацией о модели лицензирования — это рутинные и трудоемкие операции. В результате анализа даются рекомендации по управлению лицензиями, инвестициями в ИТ, адаптированные под план развития компании.

Минимальный срок аудита составляет две–четыре недели. Если обследование относится к ПО Microsoft, оно проводится бесплатно. Для

других систем стоимость составляет 1–5% от стоимости ПО, при этом экономия на закупке лицензий может достичь 50%.

4. Аудит информационной безопасности

Проект обследования позволяет проанализировать технологические процессы обработки информации, определить виды и перечни конфиденциальной информации, обрабатываемой в организации, составить перечень подразделений и работников, допущенных к обработке. Также проводится анализ внутренних документов на соответствие законодательству в области ИБ, анализируется ИТ-инфраструктура и архитектура информационных систем, взаимодействия с внешними информационными системами и (или) сетями, оценивается состояние обеспечения безопасности конфиденциальной информации. В результате разрабатываются рекомендации по оптимизации бизнес-процессов, как можно эффективно организовать управление информационной безопасностью и внедрить технические средства защиты информации. В среднем проекты аудита ИБ занимают от двух месяцев и стоят от 1 млн руб.

Алгоритм проведения ИТ-аудита

- сбор информации;
- анализ полученных данных;
- разработка рекомендаций и защита результатов аудита перед бизнес-заказчиком;
- контроль выполнения рекомендаций, разработка ИТ-стратегии (опционально).

Периодичность внешнего ИТ-аудита выбирается с учетом целого ряда параметров и событий: количество и качество изменений информационной структуры бизнеса, необходимость регулярной верификации

результативности процессов ИТ, реорганизация бизнес-структуры, сертификация компании по процессам ISO, изменение стратегии развития и «дорожной карты» и при других ситуациях, когда прозрачность ИТ, процессы, ресурсы и экономическая эффективность оказываются под вопросом.

Как правило, рекомендуется проводить процедуры аудита раз в два-три года. За этот период компании внедряют новые информационные системы, ИТ-инфраструктура сильно меняется, вендоры меняют политику лицензирования, поэтому стоит регулярно проверять и отслеживать эти изменения.

Каких результатов можно достичь при помощи ИТ-аудита

1. Снижение операционных затрат на ИТ до 50%

ИТ-аудит помогает найти точки оптимизации бюджета, за счет чего можно снизить затраты на ИТ-инфраструктуру, например сократить лицензионную нагрузку без ущерба бизнес-процессам. Большую роль в этом играют SAM (методология оптимизации жизненного цикла программных активов в компании) и специализированные решения для управления и мониторинга программными активами.

Проектный опыт показывает: в результате экономия превышает расходы на аудит в три-четыре раза, а пилотный проект занимает несколько недель. Так, в одном из проектов удалось выявить экономию от 3 до 6 млн руб. в год только за счет оптимизации по одному программному продукту.

Существенно снизить затраты можно и с SA-исследованием, анализом ИТ-инфраструктуры для подбора оптимальной модели и оптимизации инвестиций — например, при помощи ранжирования пользователей и

перехода с одного облачного решения на другое. Есть случаи, когда экономия составила 50% за счет замены решений Google на Microsoft 365. При этом функциональность и удобство использования не изменились.

2. ИТ-аутсорсинг к месту

Один из результатов ИТ-аудита — рекомендации, как повысить эффективность работы ИТ-службы. Например, за счет передачи непрофильных задач на аутсорсинг. В результате компания получает необходимое количество ресурсов квалифицированных специалистов и оптимизирует ФОТ. В 2020 году число организаций, желающих отдать на аутсорсинг обслуживание ИТ, удвоилось с 23 до 45%, подсчитали аналитики NTT.

3. Защита от кибермошенничества

ИТ-аудит помогает выявить потенциальные уязвимости в корпоративных системах, которыми могут воспользоваться злоумышленники. Например, необновленные серверы почтового сервиса Exchange могут привести к успешной фишинговой атаке и эксплуатации элементов социальной инженерии. Также в 2021 году отсутствие обновлений на стандартной службе печати Microsoft Windows Server может привести к проникновению вредоносного ПО в корпоративную сеть с последующим шифрованием данных на общедоступных сетевых ресурсах.

Отдельного внимания заслуживают ситуации с утечками конфиденциальной информации. Среди недавних примеров — инцидент в банке «Дом.РФ», который произошел из-за уязвимости в дистанционной подаче первичных заявок на получение кредита наличными. По оценкам «Ростелеком-Солар», в первом полугодии 2020 года российские компании потеряли 1,8 млрд руб. из-за утечек информации. Вовремя проведенный аудит позволяет распознать риск и принять меры по устранению уязвимостей.

Главные ошибки при проведении ИТ-аудита:

- неправильно поставленные цели аудита или недостаточные сроки для успешного сбора и анализа данных;
- сбор информации со слов ответственных лиц без последующей проверки фактического состояния;
- поверхностное обследование или недостаточная глубина погружения в процессы и ситуацию в заказчике;
- взаимодействие с командой заказчика на уровне проверяющих органов — это приводит к тому, что сотрудники заказчика стараются свести к минимуму доступ к информации и остаться в стороне от проекта;
- выбор специалистов для проведения аудита несоответствующей специализации или с недостаточным уровнем экспертизы.

Все это необходимо учитывать при проведении ИТ-аудита, чтобы получить объективную информацию и правильно спланировать дальнейшие шаги.