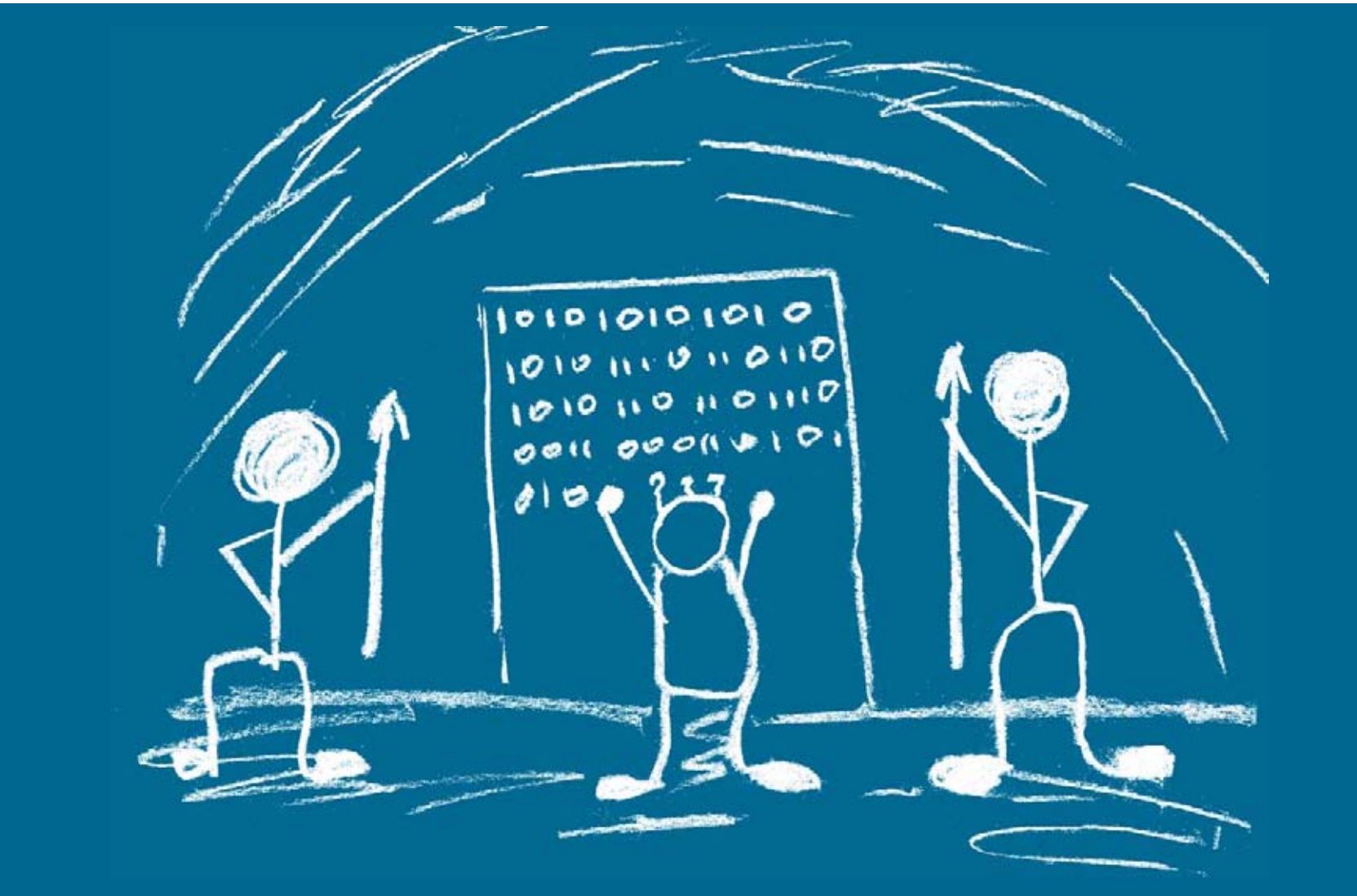
НТЦ ВУЛКАН

Каталог услуг
Информационная безопасность



Направления деятельности

Оценка защищенности

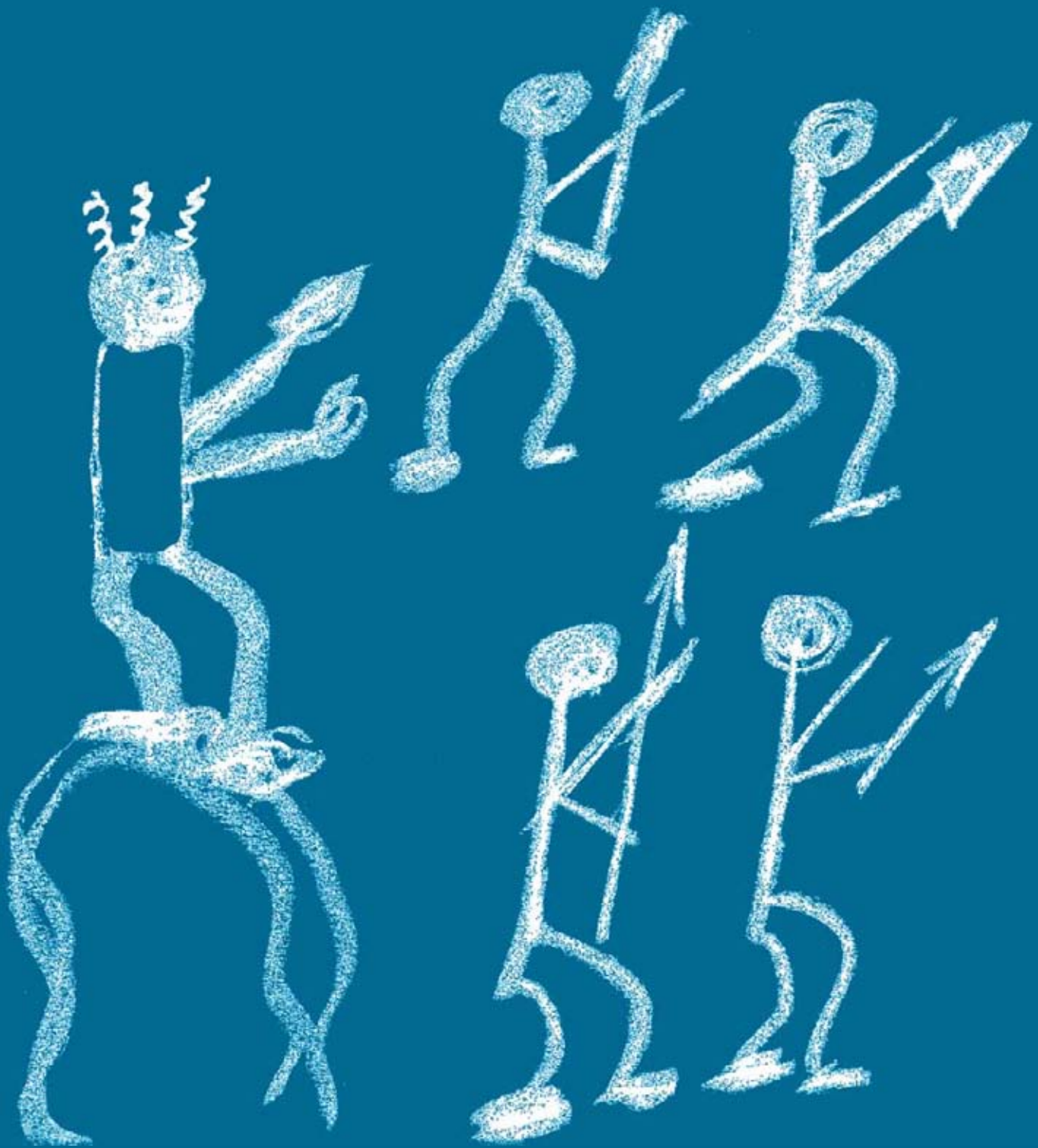
Обеспечение информационной безопасности

Соответствие требованиям

Управление информационной безопасностью

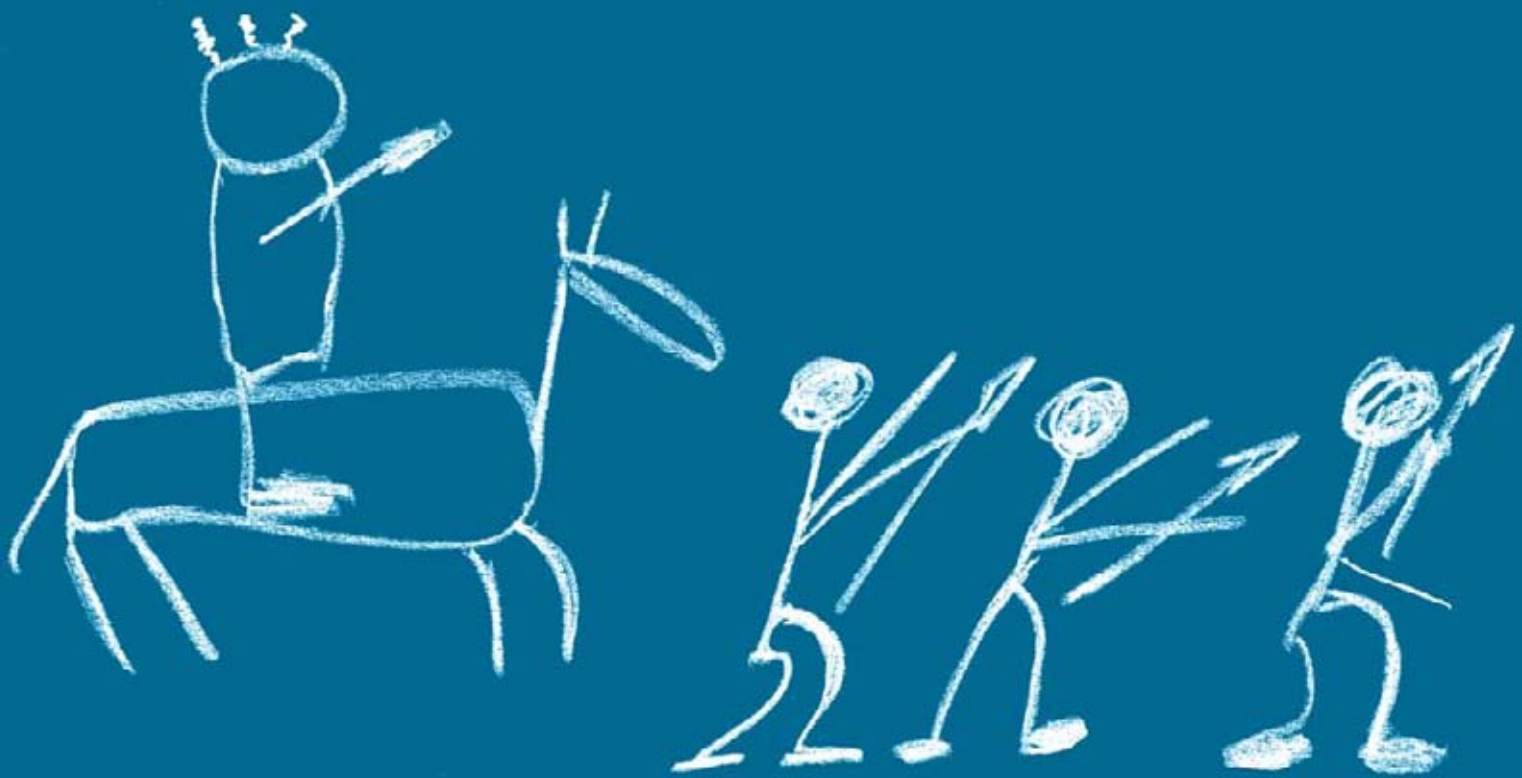
Консалтинг

СОДЕРЖАНИЕ



Управление информационной безопасностью

Создание системы управления информационной безопасностью



Для чего?

Заказчиков интересует создание СУИБ в случае:

- Наличия потребности вовлечения высшего руководства и всех сотрудников компании в процессы обеспечения ИБ
- Наличия потребности в улучшении существующей системы управления ИБ или ее интеграции с другими системами управления
- Если компания реализует процессный подход к предоставлению услуг или организации внутренней деятельности,повышая уровень зрелости
- Если компания реализует требования ISO/IEC 27001 (готовится к сертификации по данному стандарту)

Для кого?

Для компаний, реализующих комплексные меры по обеспечению ИБ и стремящихся повысить уровень зрелости в этой области.

Описание услуги

В ходе оказания услуги проводится:

- Определение и документирование требований по ИБ в организации
- Идентификация и документирование существующих защитных мер
- Анализ рисков ИБ
- Выбор целей и мер управления рисками ИБ
- Внедрение мер управления рисками и процедур управления ИБ
- Разработка и внедрение процессов управления ИБ
- Разработка и внедрение процессов обеспечения ИБ
- Разработка пакета документации по управлению ИБ

Результат и его бизнес-ценность

Результатом оказания услуги является действующая СУИБ, обеспечивающая:

- расстановку приоритетов компании в области ИБ
- оптимизацию и повышение обоснованности расходов на обеспечение информационной безопасности
- достижение «прозрачности» процессов обеспечения и управления ИБ и снижение затрат в этой области
- повышение доверия партнеров и клиентов
- соответствие критериям выхода на IPO и повышение стоимости акций при их первичном публичном размещении

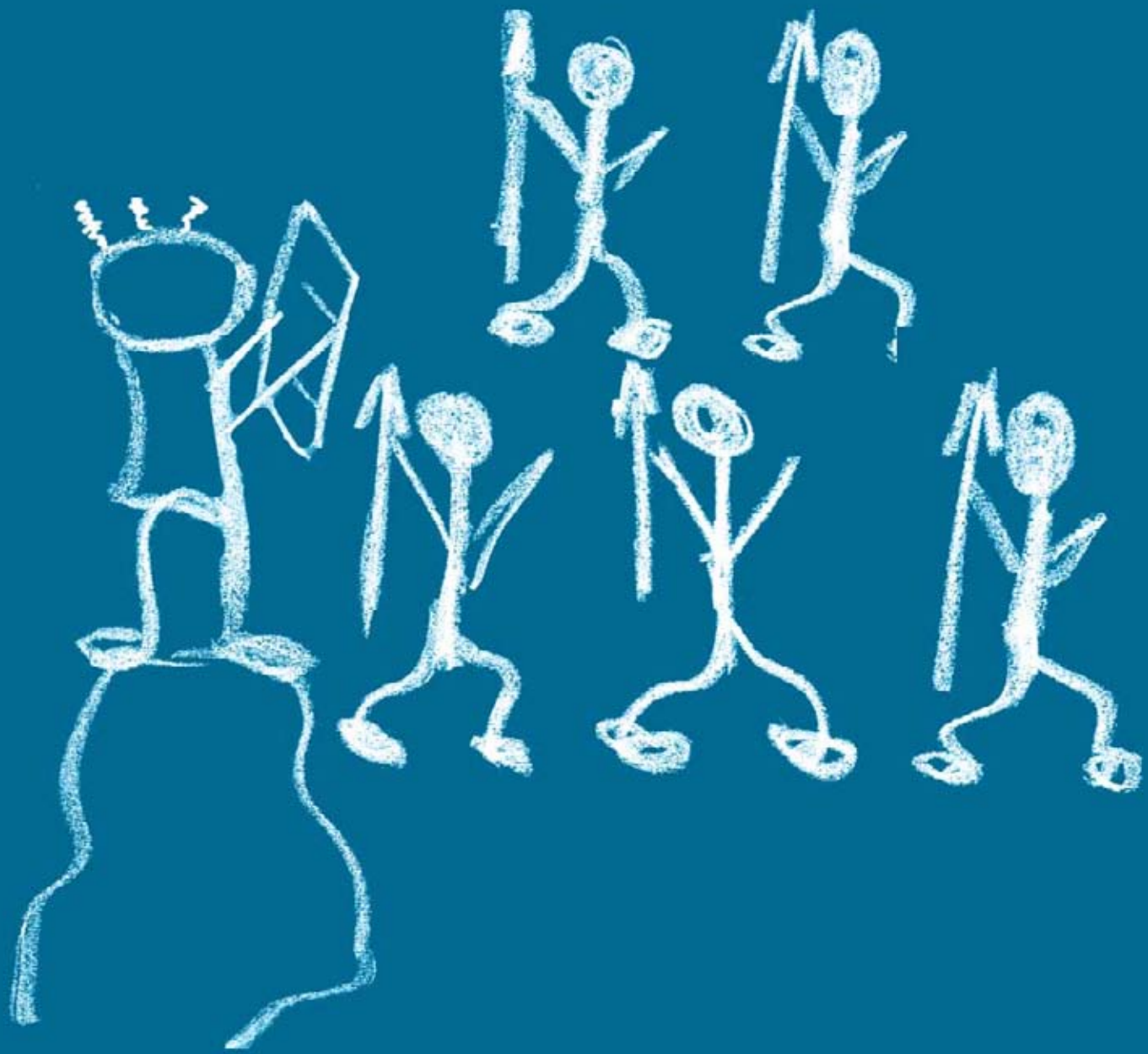
ДОПОЛНИТЕЛЬНО

Услуги оказываются в соответствии с рекомендациями комплекса стандартов ISO/IEC 2700x и ГОСТ Р ИСО/МЭК 27001-2006.

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Услуги из блока «Соответствие требованиям»

Стратегии и политики в области информационной безопасности



Для чего?

Потребность в разработке стратегий и политик возникает, когда:

- Руководство компании намерено сформировать и довести до подчиненных, а также до взаимодействующих организаций свою позицию в области обеспечения ИБ
- Необходимо задать направление формирования/развития ИБ в организации
- Необходимо построить комплексную систему обеспечения информационной безопасности (СОИБ), но «хотелось бы начать с малого»
- Происходит реорганизация бизнеса, требующая выработки единой системы взглядов на обеспечение ИБ в новой структуре

Для кого?

Корпоративным заказчикам в начальный период становления процессов обеспечения ИБ и в период их пересмотра и реорганизации.

Описание услуги

В рамках оказания услуги проводится общий анализ состояния ИБ, нормативно-правового поля, в котором действует компания, а также уровня развития и проникновения ИТ в ее основную деятельность. Формулируются цели и задачи обеспечения информационной безопасности, определяются приоритеты в обеспечении ИБ, вырабатываются принципы, которым необходимо следовать в этой области. По итогам данной деятельности разрабатываются документы трех типов (отдельно или одновременно):

- Стратегия обеспечения информационной безопасности — высокоуровневый документ, позиционирующий обеспечение ИБ как важный элемент деятельности компании и осуществляющий целеполагание в этой сфере
- Политика обеспечения информационной безопасности — заявление руководства о его взглядах на меры, принимаемые в области обеспечения ИБ. Определяет основы управления информационной безопасностью и ответственность в данной сфере
- Частные политики — документы, уточняющие положения о мерах по обеспечению ИБ для важнейших информационных систем и сервисов, исходя из их специфики

Результат и его бизнес-ценность

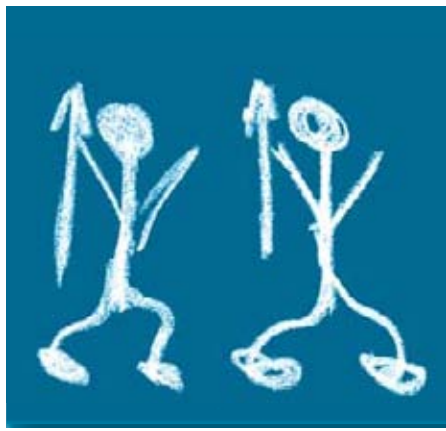
Результатом оказания услуги является утверждаемые руководством высокоуровневые документы в области обеспечения ИБ. Они закладывают фундаментальные основы всей деятельности в этой сфере. Внимание руководства к теме ИБ мотивирует и мобилизует персонал.

ДОПОЛНИТЕЛЬНО

При разработке стратегии и политик дополнительно может быть разработана архитектура перспективной СОИБ, транслирующая высокоуровневые требования на область технологий.

СВЯЗАННЫЕ УСЛУГИ

- Создание системы управления информационной безопасностью
- Документация по обеспечению информационной безопасности
- Комплексные системы обеспечения информационной безопасности



Документация по обеспечению информационной безопасности

Для чего?

Услуга актуальна для заказчиков, столкнувшихся с одной из следующих ситуаций:

- Документация в сфере ИБ отсутствует
- Документация в сфере ИБ имеет низкое качество или устарела
- Средства защиты информации внедрены, но процедуры и процессы их применения не документированы
- Происходит слияние или поглощение компаний либо сменился собственник: необходимо гармонизировать нормативную базу ИБ
- Компания реализует проекты по формализации бизнес-процессов

Для кого?

Для организаций, компаний, предприятий, реализующих комплексные меры по обеспечению информационной безопасности.

Описание услуги

В ходе оказания услуги проводится анализ процессов обеспечения ИБ и разрабатывается упорядоченный комплекс организационно-распорядительных документов в этой области, увязанный по целям, задачам и содержанию.

Иерархия разрабатываемой локальной нормативной базы включает:

- Стратегии и политики информационной безопасности
- Специализированные (частные) политики ИБ, перечни и положения
- Правила и процедуры обеспечения ИБ
- Инструкции администраторам и пользователям
- Журналы учета и формализованные отчетные документы

Результат и его бизнес-ценность

Результатом оказания услуги является систематизированный пакет документов, построенный по принципу «от общего к частному». На основе разработанной документации запускаются (совершенствуются) бизнес-процессы, связанные с обеспечением ИБ. В разработанных документах описаны принимаемые меры, четко определена и разграничена между уровнями управления ответственность за обеспечение ИБ, что обеспечивает повышение корпоративной культуры, постоянное внимание персонала к вопросам ИБ и мотивацию работников на правильное поведение в данной сфере. Это приводит к снижению издержек на поддержание заданного уровня ИБ и уменьшению рисков возникновения инцидентов, связанных с «человеческим фактором».

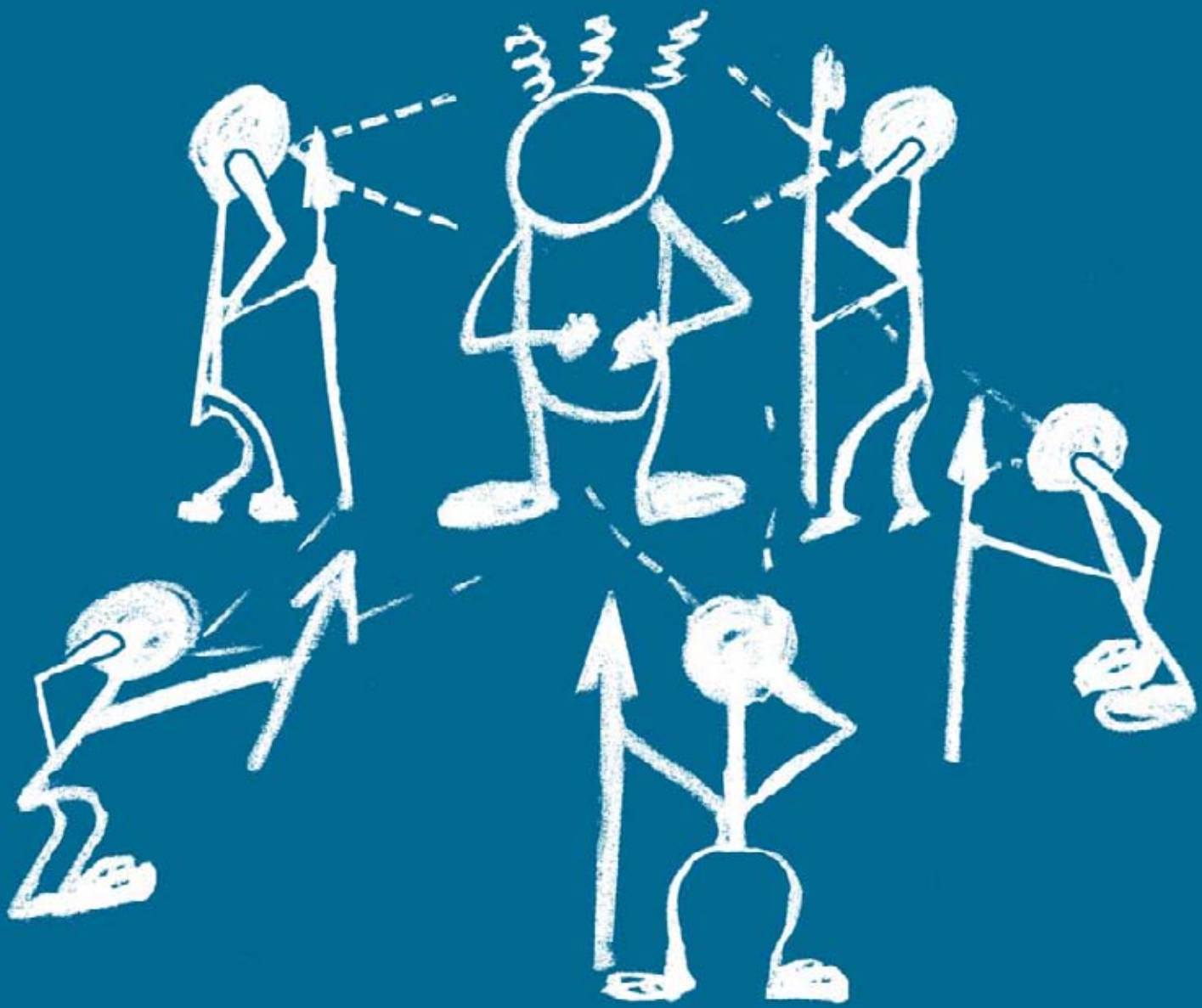
ДОПОЛНИТЕЛЬНО

Варианты построения нормативной базы в области ИБ смотрите в разделе «Услуги | Управление ИБ | Разработка документации» на интернет-сайте НТЦ «Вулкан».

СВЯЗАННЫЕ УСЛУГИ

- Создание системы управления информационной безопасностью
- Стратегии и политики в области информационной безопасности
- Комплексные системы обеспечения информационной безопасности
- Услуги из блока «Соответствие требованиям»

Управление событиями информационной безопасности



Для чего?

Потребность в услуге возникает в тех случаях, когда:

- Необходимо обеспечить единую точку сбора, хранения и анализа информации о событиях ИБ, генерируемых ИТ-инфраструктурой и средствами защиты информации
- Нужна фактура для расследования инцидентов, при этом требуется обеспечить глубокую ретроспективу «логов» (годы, месяцы)
- Необходимо оперативно выявлять аварийные ситуации и инциденты ИБ по данным корреляционного анализа событий
- Требуется автоматизировать процесс оценки соответствия требованиям (Compliance)
- В компании создается центр оперативного управления ИБ (SOC)
- В компании внедряются процессы управления ИТ на основе ITSM

Для кого?

Крупным организациям, где под управлением департамента ИТ находится масштабная гетерогенная инфраструктура, интенсивно задействованная в бизнес- и производственных процессах.

Описание услуги

В ходе оказания услуги проводится:

- Анализ ИТ-инфраструктуры и систем ИБ, потребностей в их контроле
- Определение перечней источников событий (средства защиты информации, серверы и рабочие станции, ОС, СУБД, приложения, сетевое и периферийное оборудование)
- Селекция событий для обработки, определение технологии доступа
- Выбор, поставка, установка и настройка системы управления событиями информационной безопасности (SIEM)
- Подключение источников событий к SIEM-системе, настройка параметров формирования отчетности,сигнализации и уведомлений
- Разработка и ввод в действие процедур управления событиями (самостоятельных или в комплексе с решениями по SOC)

Результат и его бизнес-ценность

Результат оказания услуги — SIEM-система, позволяющая централизованно собирать, хранить и обрабатывать события, выявлять предпосылки к авариям и инцидентам, предоставлять инструменты расследования сбоев и нарушений, обеспечивать автоматизацию процедур оценки соответствия требованиям. Внедрение SIEM разгружает ИТ/ИБ-персонал, одновременно вооружая его мощным средством контроля и управления для проактивной деятельности, обеспечивающей снижение уровня ИБ-рисков.

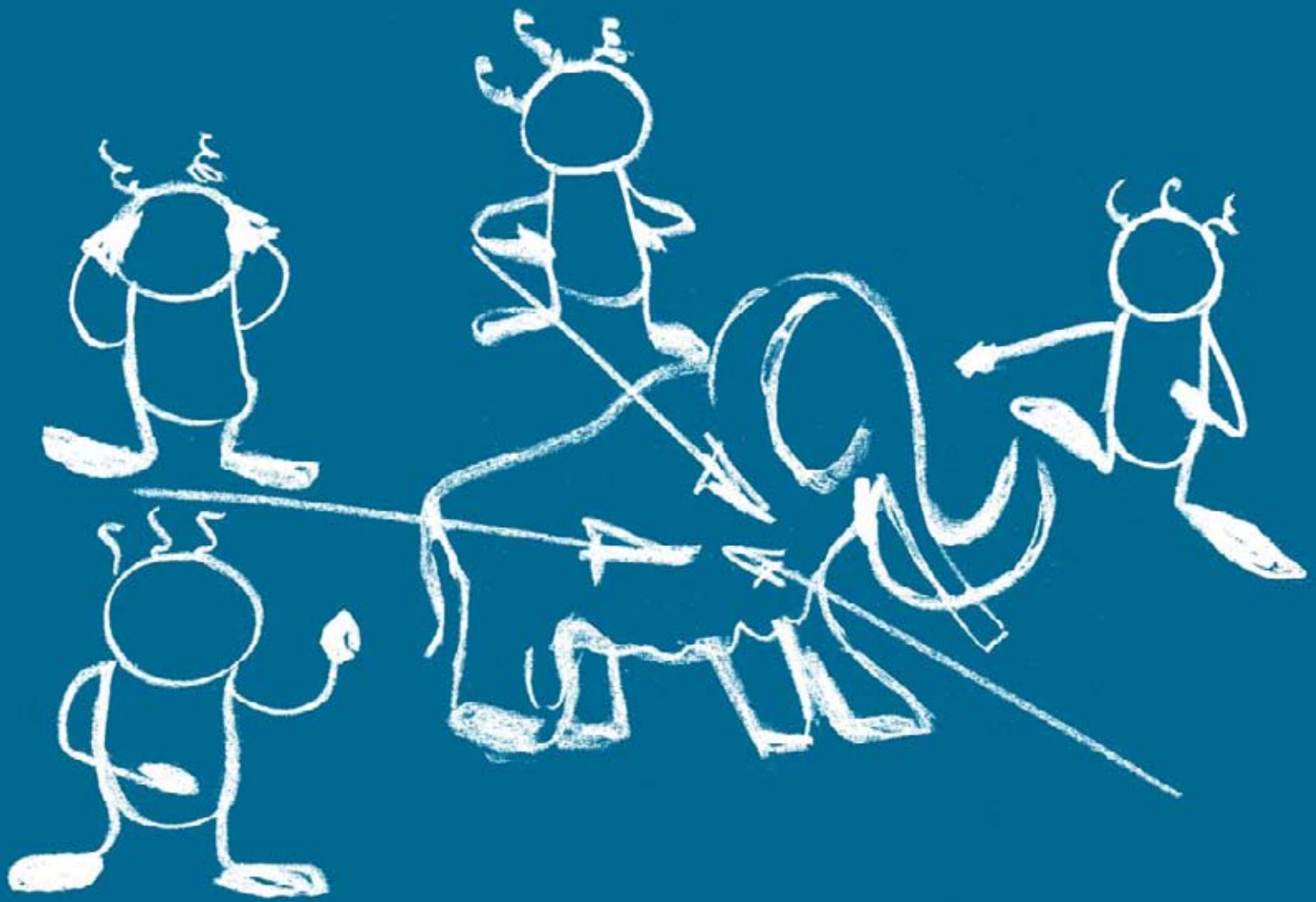
ДОПОЛНИТЕЛЬНО

Применяются передовые SIEM-решения отраслевых лидеров — RSA (The Security Division of EMC), Q1 Labs (The IBM Company), ArcSight (An HP Company).

СВЯЗАННЫЕ УСЛУГИ

- Услуги из блока «Управление информационной безопасностью»
- Комплексные системы обеспечения информационной безопасности

GRC и управление рисками



Для чего?

Потребность в проектах из области GRC (Governance, Risk Management and Compliance) формируется в компаниях с высоким уровнем зрелости в области процессов корпоративного управления:

- Когда идет постоянное развитие корпоративной культуры, политик, процессов, которые определяют общую структуру функционирования компании (Governance)
- Когда процесс управления рисками (Risk Management) формализован и выполняется, но необходимо его автоматизировать и оптимизировать (проблема управления большим числом рисков, активов)
- Когда помимо управления рисками требуется автоматизировать процессы следования и подтверждения следования законам и требованиям как внешних регуляторов, так и корпоративным политикам и процедурам (Compliance)

Для кого?

Услуга предлагается крупным компаниям, реализующим процессы управления рисками силами профильной группы или как минимум выделенного менеджера рисков, компаниям с иностранным капиталом и российским подразделениям международных корпораций.

Описание услуги

В ходе оказания услуги проводится:

- Определение целей, описание бизнес-процессов и задач, требующих автоматизации
- Выбор способов автоматизации (обоснование и разработка логики и аппарата работы GRC-решения)
- Выбор GRC-платформы, ее установка и настройка
- Ввод информации об активах, формирование базы знаний (в случае необходимости)
- Реализация процессов и логики расчета показателей
- Настройка параметров формирования отчетности, сигнализации и уведомлений

Результат и его бизнес-ценность

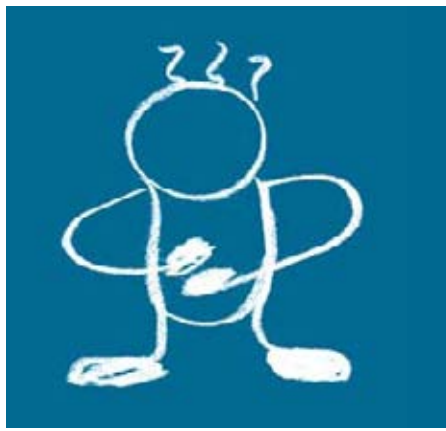
В результате оказания услуги создается единая централизованная управленческая платформа на базе GRC-решения. За счет этого существенно улучшается корпоративная культура управления, обеспечивается более эффективный Risk Management (в области финансовых, операционных, правовых и IT-рисков), достигается высокий уровень соответствия регулятивным требованиям. Подобное совершенствование позволяет повысить капитализацию компании за счет соответствия положениям таких законов и стандартов, как SOX или Basel-II.

ДОПОЛНИТЕЛЬНО

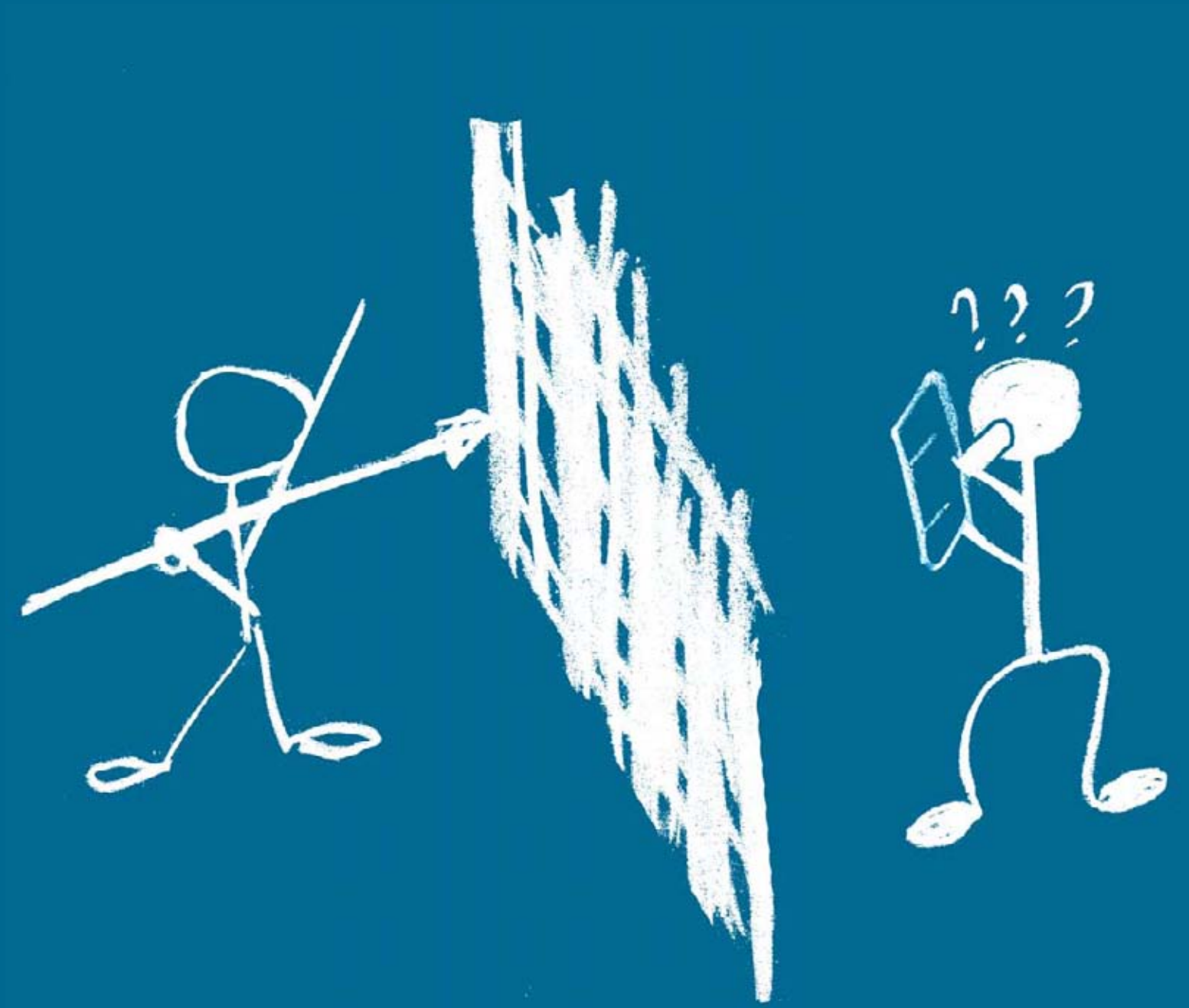
Подробнее об области Governance, Risk Management and Compliance смотрите в разделе «Центр компетенции | GRC» на сайте НТЦ «Вулкан»

СВЯЗАННЫЕ УСЛУГИ

- Услуги из блока «Управление информационной безопасностью»



Управление уязвимостями



Для чего?

«Драйверами» услуги являются:

- Признаки «бумажной безопасности»
- Потребность в контроле ИТ-подразделений, в т.ч. в филиалах
- Наличие критичных информационных систем
- Проблемы управления безопасностью сложной гетерогенной ИТ-инфраструктуры
- Потребность в разумном управлении уязвимостями/рисками ИБ

Для кого?

Для организаций с развитой, преимущественно централизованно управляемой ИТ-инфраструктурой.

Описание услуги

Услуга оказывается в несколько этапов:

- Анализ процессов управления ИТ и ИБ, требований к обеспечению информационной безопасности
- Экспресс-анализ защищенности ИТ-инфраструктуры
- Разработка процедур управления уязвимостями
- Разработка технических решений по управлению уязвимостями
- Внедрение процедур и реализация технических мер процесса Vulnerability Management

Результат и его бизнес-ценность

Результатом оказания услуги является работающая организационно-техническая система управления уязвимостями, обеспечивающая:

- Постоянную управленческую отчетность о защищенности ИТ, повышение информированности менеджмента, принятие обоснованных решений в отношении качества работы ИТ-персонала
- Высокую степень автоматизации процесса Vulnerability Management
- Оперативное устранение новых уязвимостей (особенно в критичных ИТ-системах)
- Рациональное распределение ресурсов ИТ-департамента за счет разумного принятия низкоприоритетных и остаточных рисков

Это позволит уменьшить совокупную стоимость владения комплексом ИТ-систем и снизить риски возникновения инцидентов ИБ.

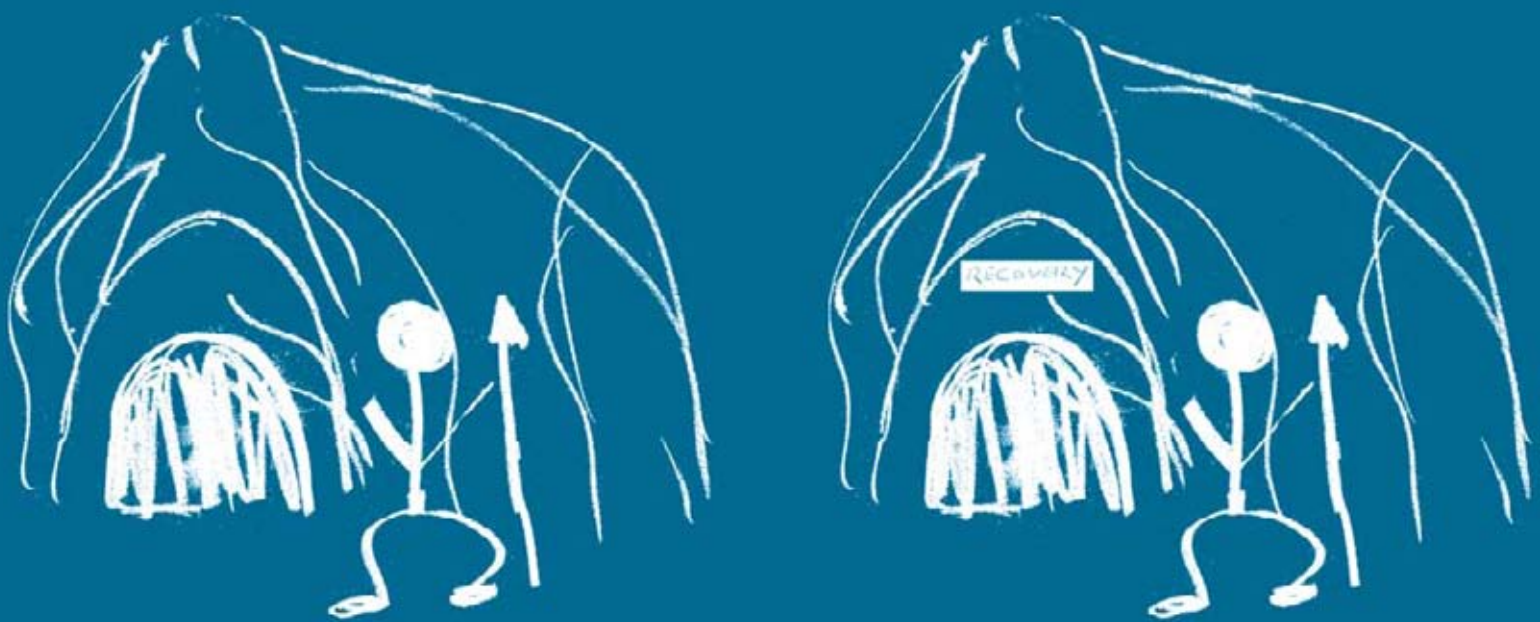
ДОПОЛНИТЕЛЬНО

Услуги оказываются с применением сертифицированного комплекса контроля и анализа защищенности «MaxPatrol» разработки компании Positive Technologies, официального партнера НТЦ «Вулкан». Также применяются штатные механизмы службы каталогов.
Возможно бесплатное проведение пилотных проектов.

СВЯЗАННЫЕ УСЛУГИ

- Создание системы управления информационной безопасностью
- Аудит информационной безопасности
- Контроль защищенности
- Услуги из блока «Соответствие требованиям»

Непрерывность ИТ-сервисов



Для чего?

Для повышения уровня надежности предоставляемых ИТ-услуг (как инсорсинг, так и аутсорсинг).
Типичные потребности:
- Необходимо заблаговременно создать механизмы оперативного устранения незапланированных прерываний ИТ-услуг
- Требуется повысить уровень надежности ИТ-сервисов
- Необходим четкий план восстановления
- Требуется восстанавливать работоспособность ИТ-сервисов в требуемые для бизнеса и заранее оговоренные с ним сроки

(Иными словами, требуется реализовать процесс IT Service Continuity Management в рамках процессного подхода к предоставлению ИТ-услуг на базе ITSM)

Для кого?

В услуге заинтересованы заказчики, производственная и управленческая деятельность которых существенно зависит от качества ИТ-услуг.

Описание услуги

В ходе оказания услуги проводится:

- Определение перечня ИТ-услуг, включаемых в контур проекта
- Анализ влияния простоя ИТ-услуг на бизнес (BIA) и оценка рисков
- Расчет максимально допустимого времени простоя ИТ-сервисов (MTD)
- Определение стратегии управления непрерывностью ИТ-услуг
- Разработка планов обеспечения непрерывности ИТ-услуг (ITSCP) и их восстановления после сбоев (DRP)
- Тестирование ITSCP и DRP

Результат и его бизнес-ценность

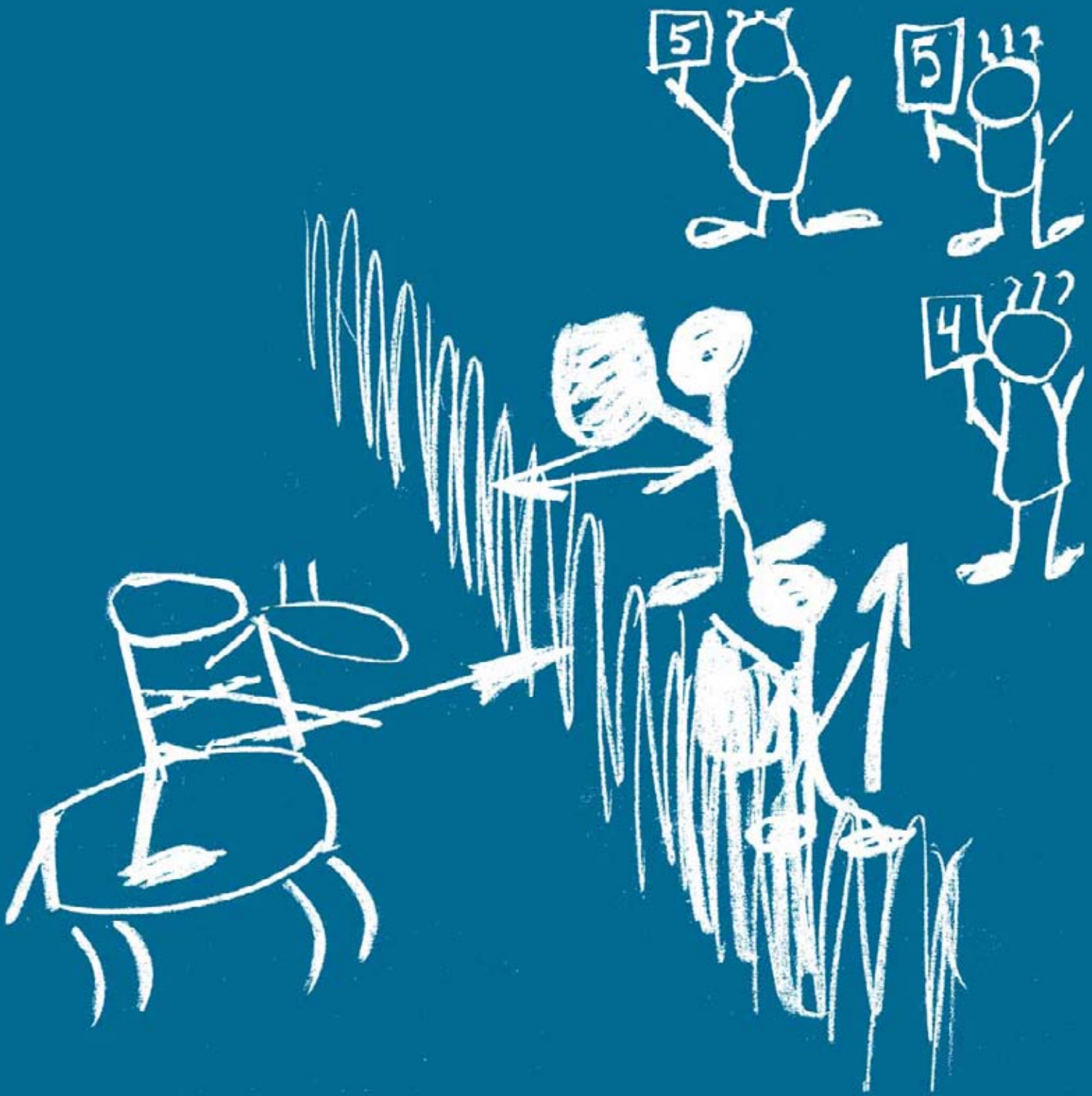
Результатом оказания услуги является существенное повышение степени готовности компании к оперативному устранению незапланированных прерываний ИТ-сервисов. Это позволяет уменьшать потери за счет минимизации времени простоя благодаря планированию и обоснованным превентивным мерам.
Кроме того, на восстановление ИТ-сервисов может тратиться на 30–60% меньше ресурсов, нежели происходит в ситуации «ручного управления в условиях общего хаоса».
Заблаговременное планирование обеспечения непрерывности позволяет более ритмично и прогнозируемо управлять ИТ-бюджетом компании.

ДОПОЛНИТЕЛЬНО

Услуги оказываются в соответствии с рекомендациями Information Technology Infrastructure Library (ITIL).

СВЯЗАННЫЕ УСЛУГИ

- Услуги из блока «Управление информационной безопасностью»
- Резервное копирование


5
5
4

Оценка защищенности

Аудит информационной безопасности

Для чего?

Аудит информационной безопасности проводится для получения ответа на вопрос: насколько реальный уровень ИБ соответствует декларируемому?

Этот вопрос поднимается как в плановом порядке, с периодичностью примерно один раз в год, так и вне плана, когда аудит ИБ требуется провести в связи с определенным событием, таким как:

- запуск новой ИТ-системы, значительные изменения инфраструктуры
- устранение последствий атаки или разрешение инцидента ИБ
- выявление признаков подготовки атаки (подозрения)
- смена ключевого ИТ/ИБ-персонала
- изменение собственника (слияние-поглощение компаний)

Для кого?

Для широкого круга заказчиков, заинтересованных в независимой оценке состояния информационной безопасности.

Описание услуги

В ходе оказания услуги проводится:

- Определение границ и критериев аудита ИБ
- Экспресс-сканирование (в целях срочного устранения наиболее существенных уязвимостей)
- Структурный анализ: инвентаризация ресурсов, анализ информационных потоков, документации, процессов управления ИБ, персонала, организации планирования деятельности в области ИБ
- Функциональный анализ: конфигурационные файлы и настройки (сетевое оборудование, информационные системы и сервисы, средства защиты информации), сканирование узлов сети (внутреннее / внешнее), анализ сетевого трафика, мониторинг радиоэфира
- Подведение итогов и подготовка рекомендаций

Результат и его бизнес-ценность

Результатом оказания услуги являетсяотчет об аудите, содержащий сведения о соответствии реального уровня ИБ декларируемому (заданному федеральными НПА, отраслевыми стандартами или внутренними политиками ИБ). Отчет ориентируется на три категории менеджеров:

Часть 1 –резюме для руководителя, главные выводы
Часть 2 – аналитика и roadmap для операционных менеджеров
Часть 3 – технические отчеты и рекомендации для ИТ/ИБ-специалистов

На основании данных отчета принимаются решения о дальнейшей деятельности в области обеспечения ИБ компании. Повышается внимание руководства к проблемам безопасности. Растет значимость ИТ/ИБ-службы.

ДОПОЛНИТЕЛЬНО

Аудит может быть проведен как в отношении всей ИТ-инфраструктуры, так и по отдельной информационной системе.

СВЯЗАННЫЕ УСЛУГИ

- Услуги из блока «Управление информационной безопасностью»
- Тест на проникновение
- Анализ коммуникативных связей

Тест на проникновение

Для чего?

Назначением теста на проникновение (Penetration Test) являются:

- Практический контроль эффективности мер по защите информации
- Поиск и устранение уязвимостей в механизмах безопасности критичных информационных систем и сервисов
- Проверка компетентности администраторов
- Проверка соблюдения требований корпоративной политики ИБ
- Проверка устойчивости информационных систем и сервисов к атакам
- Контроль защищенности в рамках Compliance

Для кого?

Для широкого круга заказчиков, заинтересованных в независимой оценке технологической защищенности (практического обеспечения ИБ).

Описание услуги

В ходе оказания услуги проводится:

- Определение границ проекта, согласование методики теста
- Реализация мероприятий теста на проникновение
- Подведение итогов и подготовка рекомендаций

Тактика и сценарий выполнения теста варьируется в зависимости от объекта проверки и в общем случае включает этапы подготовки (поиск по открытым источникам и сетевым информационным службам), обнаружения уязвимостей (fingerprinting, сканирование, анализ работы систем), реализации найденных уязвимостей (с оценкой потенциального ущерба, возможных направлений дальнейших действий, возможности «заметания следов»).
В методиках пентестов НТЦ «Вулкан» активно применяются положения методологий OSSTMM и OWASP.
Для «заказных» систем дополнительно предлагается проведение анализа исходных кодов критичных процедур на наличие уязвимостей, позволяющих реализовать атаки XSS и SQL-инъекции либо обойти встроенные механизмы безопасности.
Мероприятия проводятся подготовленными специалистами по ethical hacking, сетевым технологиям и безопасности приложений.

Результат и его бизнес-ценность

В результате оказания услуги заказчик получит квалифицированный ответ на вопрос: уязвима ли информационная система к атакам потенциальных злоумышленников? Результаты теста продемонстрируют болевые точки в обеспечении ИБ (проблемы в настройках, незакрытые уязвимости, ошибки в администрировании, халатность) и позволят устранить недостатки до того, как система будет взломана и компании будет нанесен ущерб.

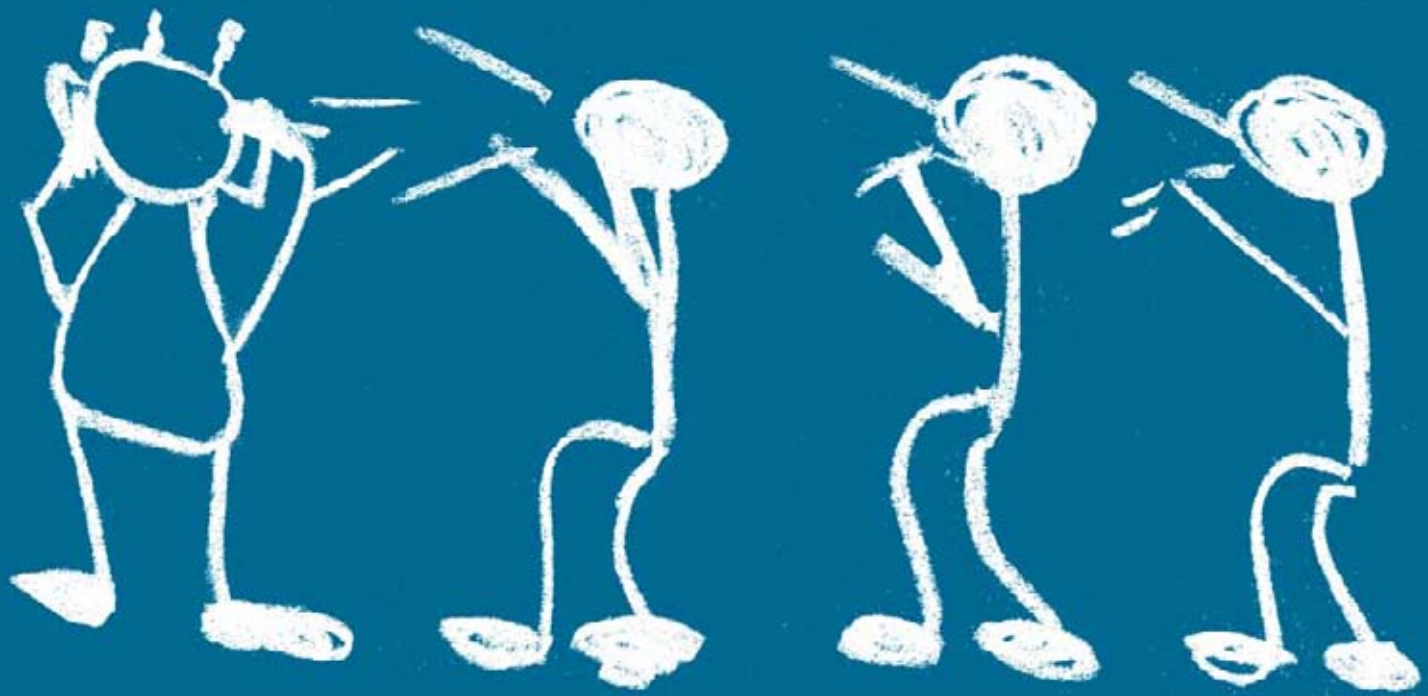
ДОПОЛНИТЕЛЬНО

При необходимости в ходе реализации теста на проникновение могут быть использованы приемы социальной инженерии.

СВЯЗАННЫЕ УСЛУГИ

- Аудит информационной безопасности
- Контроль и анализ защищенности

Анализ коммуникативных связей



Для чего?

Анализ коммуникативных связей — это «нетехнический» метод решения задачи обеспечения ИБ, направленный на выявление злоумышленника (инсайдера) путем анализа данных о его взаимодействии с информационными системами, коллегами, заказчиками, партнерами, третьими лицами. Услуга позволяет:

- отследить устойчивые группы общения сотрудников
- проанализировать«внешние» коммуникации
- идентифицировать неформальных лидеров
- выявить наиболее активных сотрудников и наиболее тесные связи между ними
- отследить взаимодействия конкретных абонентов и групп по различным временным срезам

Для кого?

Компаниям, активно использующим в повседневной деятельности средства электронных коммуникаций.
Службам экономической безопасности и внутреннего контроля.

Описание услуги

Постановка задачи варьируется в зависимости от рода деятельности заказчика и цели оказания услуги. Типичный сценарий анализа коммуникативных связей предполагает:

- Составление профиля коммуникационной активности (по данным об организационно-штатной структуре, основной деятельности сотрудников и оснащенности компании средствами связи и ИТ)
- Отбор источников данных и получение регистрационной информации (в качестве источников выступают журналы регистрации событий средств электронных коммуникаций — почтовых серверов, сетевого оборудования, средств защиты, УАТС)
- Анализ полученной информации с помощью информационно-аналитической системы «i2», получение визуализированных диаграмм, подготовка отчетов о выявленных аномалиях и пиковых значениях

Примечание. ИАС «i2» может быть развернута у заказчика на постоянной основе: НТЦ «Вулкан» осуществляет поставку ПО, подключение источников данных, подготовку шаблонных отчетов, техническую поддержку и обучение.

Результат и его бизнес-ценность

Результатом оказания услуги является предотвращение возможных злоупотреблений, хищений, нецелевого использования ресурсов компании, а также профилактика должностных нарушений и общее повышение эффективности процессов управления персоналом.

ДОПОЛНИТЕЛЬНО

О других задачах корпоративной и общественной безопасности, решаемых с применением системы «i2», можно узнать на интернет-сайте НТЦ «Вулкан» в разделе «Центр компетенции | ИАС».

СВЯЗАННЫЕ УСЛУГИ

- Аудит информационной безопасности
- Предотвращение утечек данных

Обеспечение информационной безопасности

Комплексные системы обеспечения информационной безопасности

Для чего?

Комплексная СОИБ предназначена для снижения рисков реализации полного спектра угроз информационной безопасности. Это достигается за счет совместного применения сразу нескольких технологий и средств защиты информации, развернутых под единым управлением и опирающихся на единую организационно-нормативную базу.
Услуга ориентирована на защиту ИТ-инфраструктуры (сеть, ЦОД, пространство рабочих станций), а также предоставляемых на ее базе информационных и телекоммуникационных сервисов (служба каталогов, почта, удаленный доступ, файловое хранилище, сетевая печать, доступ в Интернет) и охватывает не только технологический, но и организационный уровень обеспечения ИБ.

Для кого?

Широкому кругу заказчиков, использующих ИТ-системы и электронные коммуникации в управленческой и производственной деятельности.

Описание услуги

Создание комплексной СОИБ осуществляется поэтапно:

- 1 этап: обследование объекта защиты, разработка модели нарушителя и модели угроз, разработка политики ИБ, организационно-распорядительных документов по обеспечению информационной безопасности и архитектуры СОИБ
- 2 этап: техническое проектирование СОИБ (выбор и обоснование средств защиты информации и встроенных механизмов безопасности, разработка технических решений по их применению)
- 3 этап: комплектация СОИБ средствами защиты, монтаж, установка и настройка средств защиты, обучение персонала, пусконаладочные работы, опытная эксплуатация и приемочные испытания СОИБ.

Примечание. В состав СОИБ как правило включаются следующие подсистемы: управления доступом, межсетевого экранирования (защиты периметра), регистрации событий, контроля целостности, антивирусной защиты, контроля и анализа защищенности, предотвращения вторжений, криптографической защиты, предотвращения утечек, а также подсистема централизованного управления ИБ.

Результат и его бизнес-ценность

В результате оказания услуги заказчик получает работоспособную комплексную СОИБ, снабженную необходимой локальной нормативной базой и обеспечивающую минимизацию всех существенных рисков ИБ для действующей ИТ-инфраструктуры. Высокий уровень безопасности достигается за счет перекрытия всех выявленных актуальных каналов реализации угроз (в отличие от «латания дыр», т.е. фрагментарного подхода к обеспечению ИБ). За счет объединения в одном проекте нескольких потоков работ обеспечивается снижение капитальных затрат (CapEx).

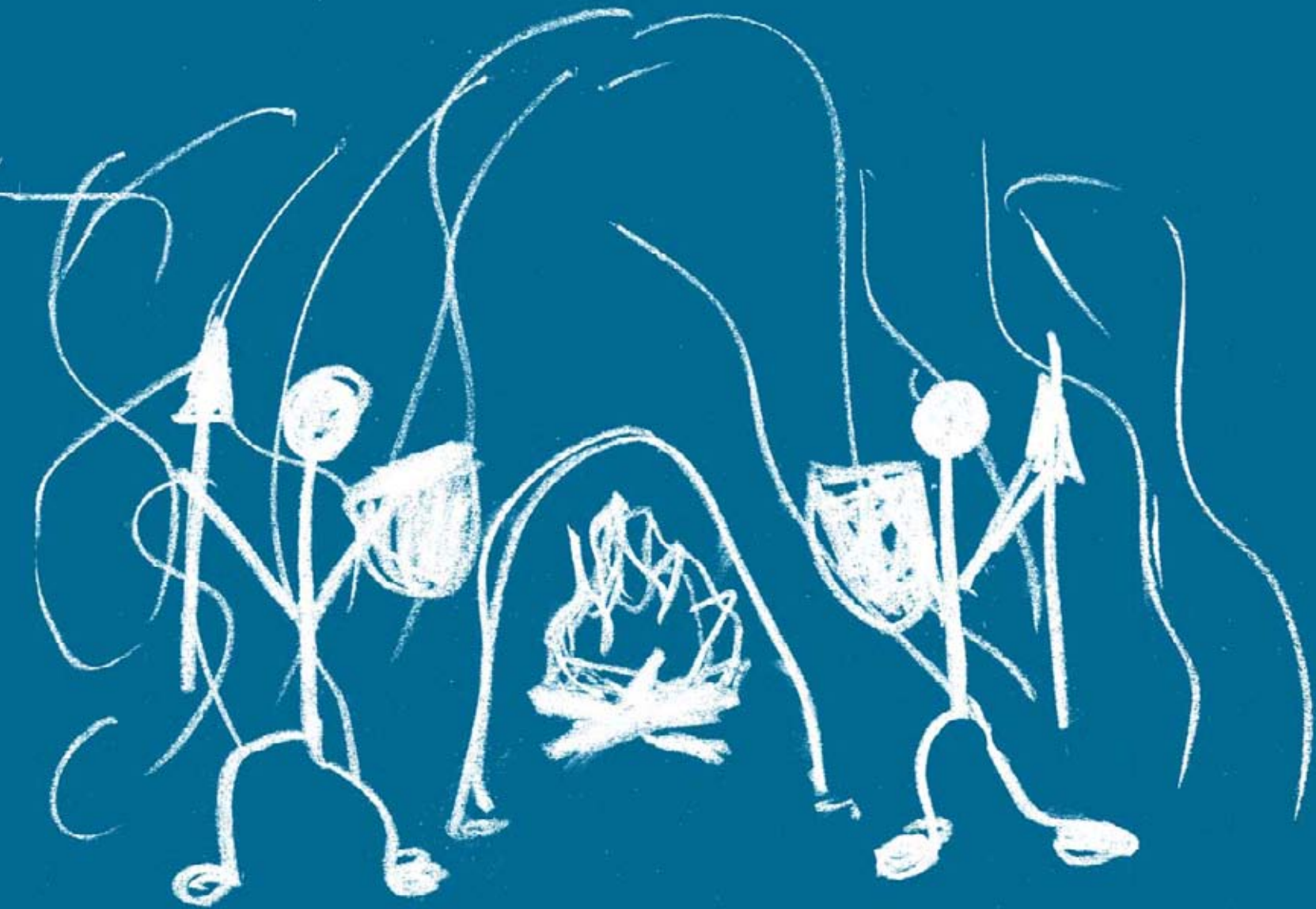
ДОПОЛНИТЕЛЬНО

В необходимых случаях по окончании работ может быть проведена аттестация объекта защиты по требованиям безопасности информации.

СВЯЗАННЫЕ УСЛУГИ

- Тест на проникновение
- Услуги из блока «Управление информационной безопасностью»

Безопасность информационных систем



Для чего?

Услуга ориентирована на обеспечение информационной безопасности отдельных информационных систем. Как правило такие ИС играют важную роль в производственной и управленческой деятельности. К ним относятся:

- CRM, ERP, Inventory, BI, корпоративные порталы
- АБС, СДБО
- АСУ ТП и системы диспетчерского управления (SCADA-системы)
- системы OSS/BSS

Для кого?

Компаниям и организациям любого профиля, нуждающимся в защите своих ключевых информационных систем.

Описание услуги

Создание системы обеспечения информационной безопасности отдельной корпоративной ИС осуществляется поэтапно:

- 1 этап: обследование объекта защиты, разработка модели нарушителя и модели угроз, разработка частной политики ИБ информационной системы, доработка (разработка) организационно-распорядительных документов по обеспечению информационной безопасности ИС
- 2 этап: техническое проектирование системы обеспечения ИБ (выбор и обоснование средств защиты и встроенных механизмов безопасности, разработка технических решений по их применению)
- 3 этап: поставка, монтаж, установка и настройка средств защиты, обучение персонала, пусконаладочные работы, опытная эксплуатация и приемочные испытания системы обеспечения ИБ

Примечание. Система обеспечения информационной безопасности создается с учетом архитектуры и технологических особенностей защищаемой ИС и ее компонентов (аппаратной платформы,приложений, СУБД). В рамках работ может быть проведен анализ исходного кода критичных процедур, а также выработаны рекомендации разработчикам системы по устранению выявленных недостатков и уязвимостей ПО.

Результат и его бизнес-ценность

В результате оказания услуги заказчик получает работоспособную комплексную СОИБ информационной системы, снабженную необходимой нормативной базой и обеспечивающую минимизацию всех существенных рисков ИБ.

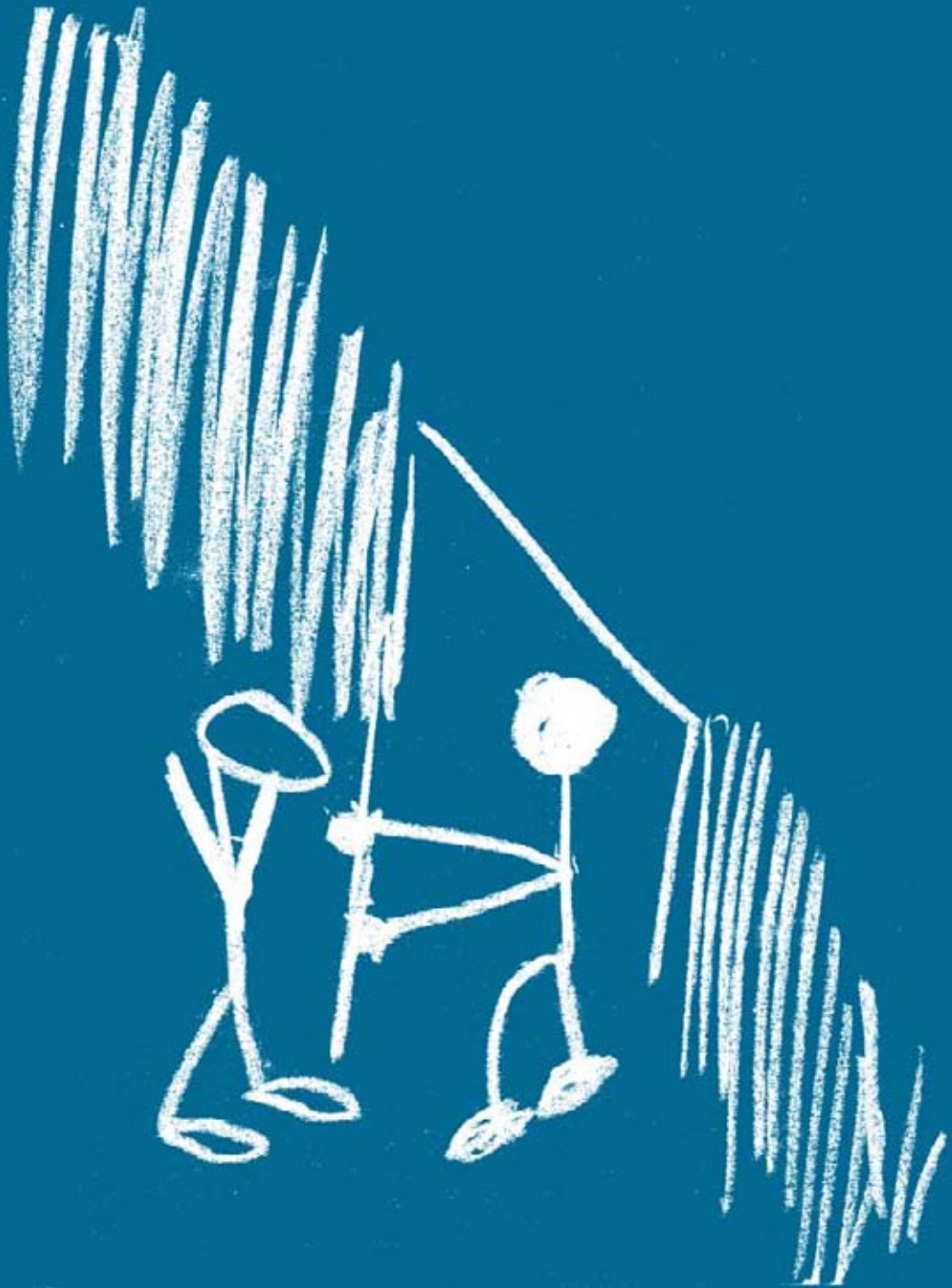
ДОПОЛНИТЕЛЬНО

При необходимости применяются государственные и отраслевые нормы, устанавливающие требования к обеспечению защиты информации для ИС соответствующего класса (например, КСИИ, ИСПДн, ИСОП).

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Непрерывность ИТ-сервисов
- Тест на проникновение
- Услуги из блока «Соответствие требованиям»

Управление доступом



Для чего?

Услуга предусматривает реализацию различных механизмов идентификации, аутентификации и авторизации в информационных системах и сервисах и является актуальной, если:

- Существует потребность в разграничении и контроле доступа сотрудников к информационным ресурсам
- Имеется необходимость усиленной защиты информационных активов на основе технологий многофакторной аутентификации
- Компания реализует требования Федерального закона № 152-ФЗ «О персональных данных» или Федерального закона № 98-ФЗ «О коммерческой тайне», других НПА в части обеспечения ИБ
- Организация банковской системы России реализует требования комплекса стандартов СТО БР ИББС

Для кого?

Для широкого круга заказчиков, заинтересованных в повышении уровня ИБ и противодействии угрозам несанкционированного доступа.

Описание услуги

В ходе оказания услуги:

- Определяются перечни объектов и субъектов доступа
- Формируется матрица доступа
- Устанавливаются требования к процедуре аутентификации (сквозная (SSO), однофакторная или многофакторная)
- Определяются технические решения по применению встроенных механизмов безопасности и/или наложенных средств защиты
- Осуществляется установка и настройка средств управления доступом
- Настраиваются параметры сигнализациии уведомлений
- Разрабатываются правила и инструкции, проводятся испытания и ввод в эксплуатацию

Результат и его бизнес-ценность

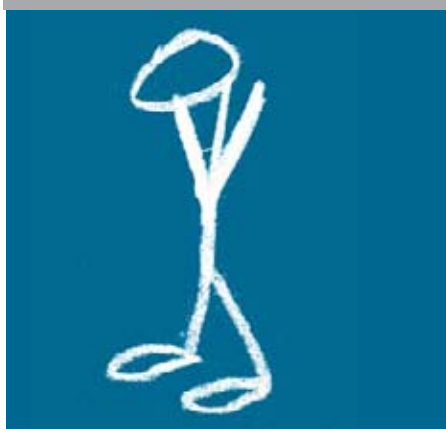
Управление доступом позволяет уменьшить риски НСД к важным информационным ресурсам, тем самым снижая возможные потери от разглашения информации, а также помогает оптимизировать бизнес-процессы за счет сквозной аутентификации, повышая производительность труда.

ДОПОЛНИТЕЛЬНО

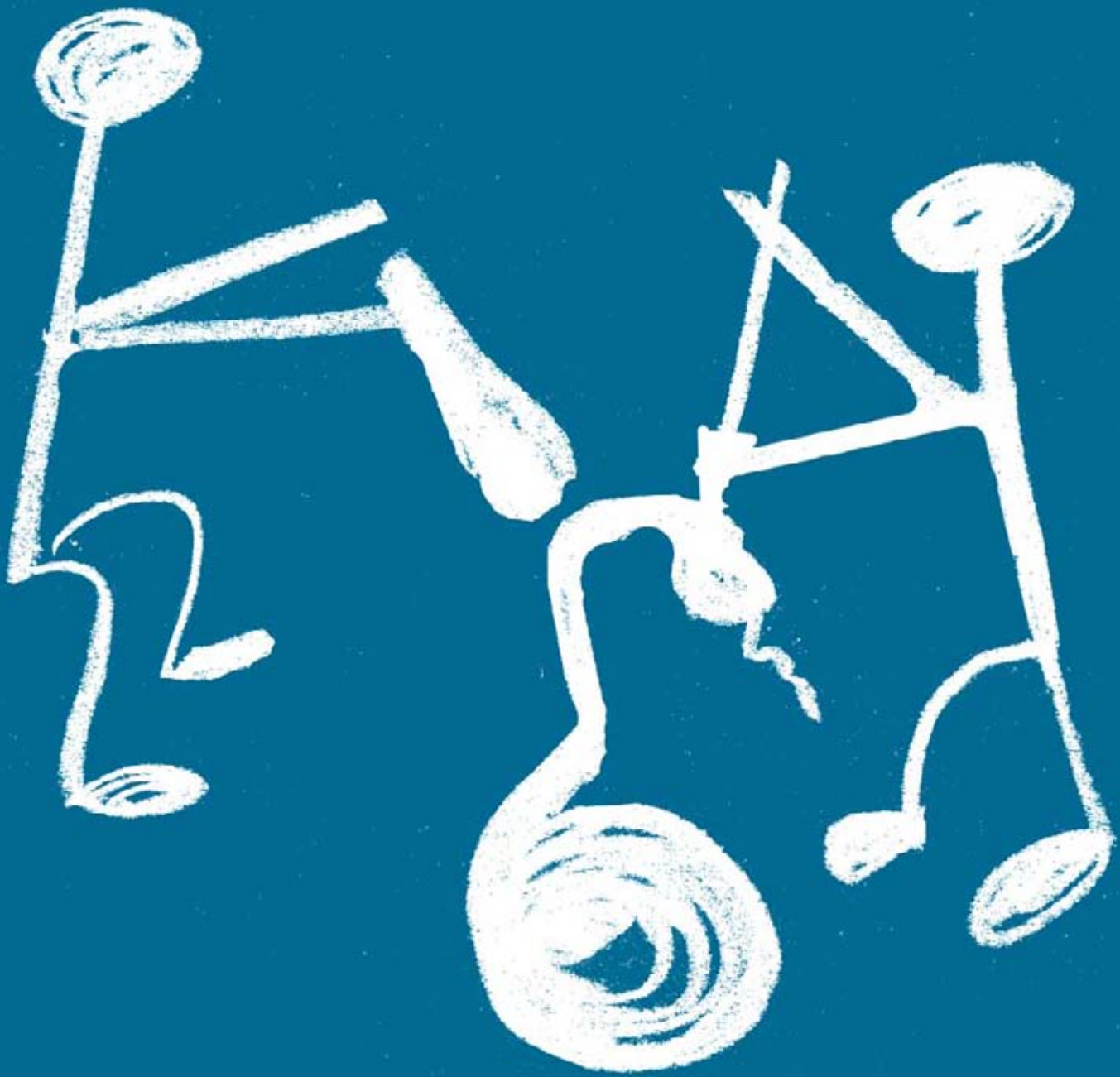
Аутентификация обеспечивается за счет применения встроенных механизмов ОС, СУБД и/или приложений, а также специализированных программных и аппаратных средств (в т.ч. токенов и смарт-карт, средств защиты от НСД, наложенных IAM-решений для СУБД) отечественного и зарубежного производства, в т.ч. сертифицированных по требованиям безопасности информации.

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Безопасность информационных систем
- Инфраструктуры PKI и удостоверяющие центры



Антивирусная защита



Для чего?

Услуга предполагает развертывание корпоративной системы, обеспечивающей централизованную антивирусную защиту для рабочих станций, серверов и прикладных шлюзов.

Правильный подход к созданию антивирусной инфраструктуры обеспечивает:
- Блокировку основных угроз безопасности ИТ-инфраструктуры
- Унификацию и отказ от «зоопарка» антивирусных решений
- Единое управление, минимальное время реакции на обнаружение и предотвращение заражений вирусами
- Снижение ресурсных затрат на администрирование антивирусов
- Снижение ресурсных затрат на обновление баз сигнатур
- Интеграцию средств антивирусной защиты с другими сервисами ИБ

Для кого?

Для широкого круга заказчиков, применяющих информационные технологии в своей повседневной деятельности.

Описание услуги

В ходе оказания услуги:

- Производится анализ объекта защиты и выбор корпоративного антивирусного продукта, для сложных объектов разрабатывается инженерно-техническое решение по антивирусной защите
- Осуществляется поставка антивирусных средств
- Корпоративная антивирусная система разворачивается в сети заказчика, производится настройка параметров ее функционирования
- Разрабатываются необходимые правила и инструкции, проводится обучение персонала

Результат и его бизнес-ценность

Корпоративная антивирусная система снижает риски, связанные с активностью злонамеренного ПО. Централизация управления и обновлений позволяет снизить операционные издержки (OpEx).

ДОПОЛНИТЕЛЬНО

Для реализации антивирусной защиты применяются решения ведущих вендоров:
- Лаборатория Касперского
- DrWeb
- McAfee
- eSet
- Symantec
- Sophos

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Безопасность информационных систем
- Защита от спама

Контроль защищенности

Для чего?

Услуга нацелена на создание и запуск в компании процесса контроля и анализа защищенности в целях подтверждения соответствия мер защиты требованиям руководящих и методических документов, корпоративной политики ИБ, техническим решениям по защите информации.

Процесс систематического контроля и анализа защищенности базируется на двух составляющих:

- Проверка организационных вопросов обеспечения ИБ
- Техническая проверка безопасности ИТ-систем и сервисов, а также эффективности работы средств и механизмов защиты информации

Для кого?

Для широкого круга заказчиков, применяющих информационные технологии в своей повседневной деятельности.

Описание услуги

В ходе оказания услуги:

- Производится анализ объекта информатизации (корпоративной сети, информационной системы) и применяемых мер защиты
- С учетом технологии обработки и информации, архитектуры объекта и состава средств защиты и осуществляется разработка процесса контроля и анализа защищенности (мероприятия, периодичность, ответственные, входы и выходы процесса, взаимосвязи с другими процессами управления ИТ и ИБ)
- Осуществляется выбор инструментального средства контроля и анализа защищенности (сканера безопасности), для сложных объектов разрабатывается инженерно-техническое решение
- Осуществляется поставка и развертывание средств контроля и анализа защищенности
- Разрабатываются необходимые правила и инструкции, предусматривающие проведение как экспертных, так и инструментальных проверок
- Проводится обучение персонала и запуск процесса систематического контроля и анализа защищенности

Результат и его бизнес-ценность

В результате внедрения процесса обеспечивается должный контроль за уровнем информационной безопасности, что позволяет подтверждать соответствие требованиям по обеспечению заданного уровня ИБ и оперативно выявлять недостатки в обеспечении ИБ и уязвимости ИТ-систем и сервисов. Тем самым существенно снижаются риски нарушения ИБ и связанные с ними издержки.

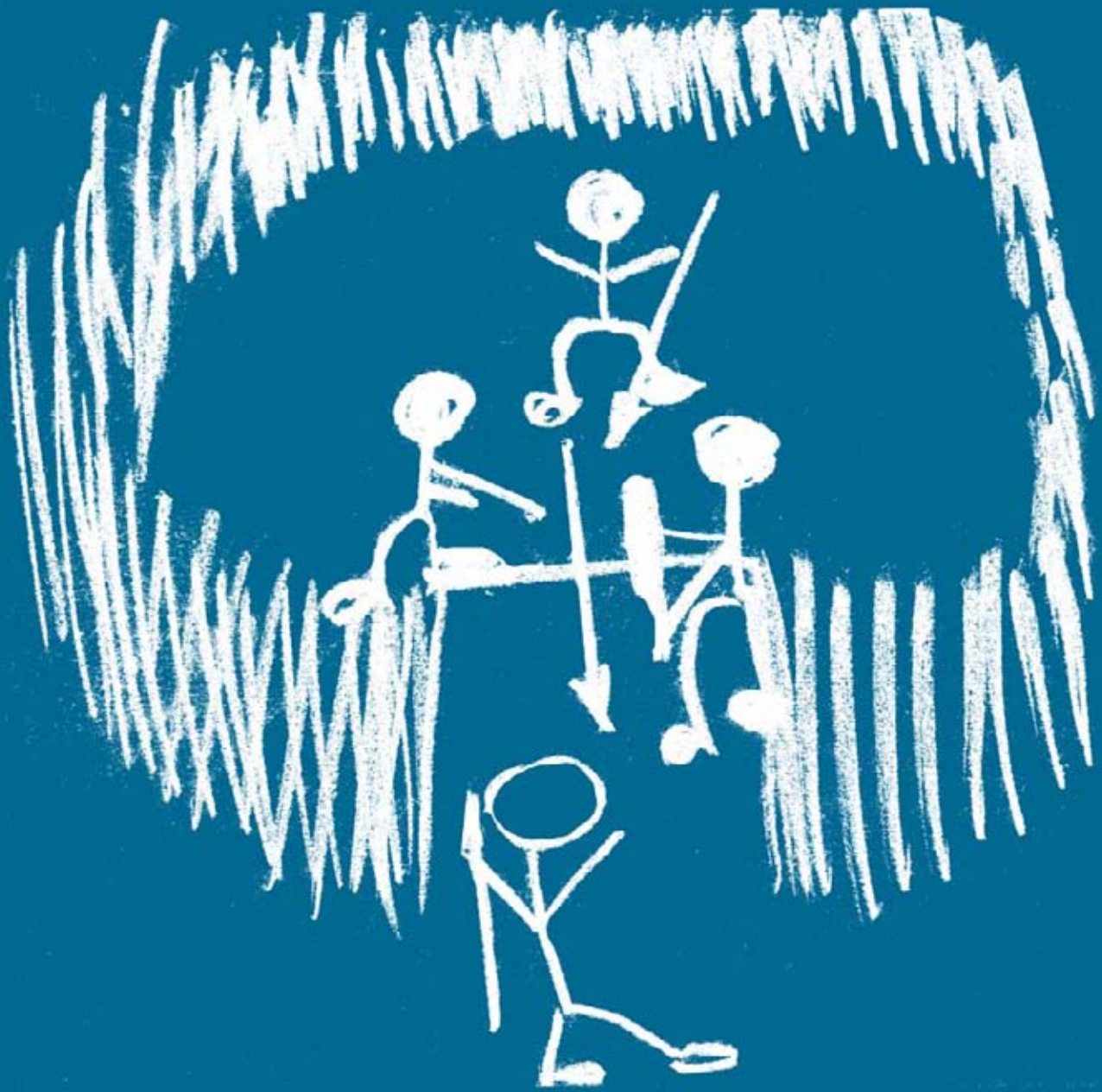
ДОПОЛНИТЕЛЬНО

В качестве сканеров безопасности применяются сертифицированные продукты Xspider и MaxPatrol, а также их зарубежные аналоги.

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Безопасность информационных систем

Обнаружение и предотвращение вторжений



Для чего?

Целью предоставления услуги является обеспечение информационной безопасности при подключении к внешним информационно-вычислительным сетям (сеть Интернет, сети сторонних организаций, сеть оператора связи) и внутри корпоративной сети за счет обнаружения в сетевом трафике признаков попыток реализации атак. Дополнительными мотивирующими факторами могут быть:

- Наличие web-ресурсов, требующих высокого уровня доступности
- Наличие корпоративных информационных систем с front-end, размещенным в сети Интернет
- Потребность в обеспечении комплексной сетевой безопасности информационно-вычислительных ресурсов
- Реализация требований Федерального закона № 152-ФЗ «О персональных данных»
- Реализация требований комплекса стандартов СТО БР ИББС
- Реализация требований стандарта PCI DSS

Для кого?

Для широкого круга компаний, заинтересованных в повышении уровня доступности ИТ-ресурсов и сервисов, а также испытывающих потребности в противостоянии угрозам типа «Отказ в обслуживании» (DoS/DDoS) и в раннем выявлении злонамеренной активности на уровне сети.

Описание услуги

В ходе оказания услуги проводится:

- Анализ объекта защиты, определение порядка и точек доступа к защищаемым ИТ-ресурсам и сервисам, выявление нагрузочных характеристик и стандартного профиля активности
- Выбор IDS/IPS, разработка инженерно-технического решения (для сложных или высоконагруженных объектов)
- Поставка, установка и настройка IDS/IPS, настройка параметров сигнализациии формирования уведомлений
- Разработка необходимой документации и ввод системы обнаружения и предотвращения вторжений в эксплуатацию

Результат и его бизнес-ценность

Установленная и настроенная система предотвращения вторжений позволяет обеспечить раннее обнаружение атак и своевременную реакцию на них до наступления неблагоприятных последствий. Повышается уровень доступности информационных ресурсов и сервисов, за счет чего обеспечивается снижение потерь, связанных с простоями вследствие реализации угроз ИБ.

ДОПОЛНИТЕЛЬНО

Для реализации услуги применяются высокотехнологичные IDS/IPS производства Cisco Sysytems, CheckPoint, Juniper Networks, StoneSoft, McAfee.

СВЯЗАННЫЕ УСЛУГИ

- Межсетевое экранирование: защита периметра
- Комплексные системы обеспечения информационной безопасности

Межсетевое экранирование: защита периметра

Для чего?

Целью предоставления услуги является обеспечение ИБ при подключении к внешним информационно-вычислительным сетям за счет управления прохождением сетевого трафика через границу (периметр безопасности) сети.
Услуга удовлетворяет широкий спектр потребностей в обеспечении сетевой безопасности информационно-вычислительных ресурсов.
Кроме того, межсетевое экранирование является обязательным условием выполнения требований по защите персональных данных, применяется при реализации положений законодательства об охране конфиденциальной информации и при реализации требований СТО БР ИББС и PCI DSS.

Для кого?

Для широкого круга заказчиков, заинтересованных в противостоянии сетевым угрозам как изнутри, так и извне.

Описание услуги

В ходе оказания услуги проводится:

- Определение топологии сети, точек доступа во внешние сети, профиля активности штатных ИТ-средств, а также требований к средствам межсетевого экранирования
- Выбор продукта, разработка политики безопасности межсетевого экрана (для объектов сложной топологии или высоконагруженных разрабатывается комплексное инженерно-техническое решение)
- Поставка, установка и общая настройка межсетевого экрана (экранов)
- Настройка списков управления доступом
- Организация виртуальных частных сетей (если предусмотрено требованиями или инженерно-техническим решением)
- Настройка параметров сигнализации и формирования уведомлений
- Настройка дополнительных параметров межсетевого экрана (аутентификация, прикладные посредники, балансировка нагрузки, NAT, VLAN, отказоустойчивость, другие опции)

Результат и его бизнес-ценность

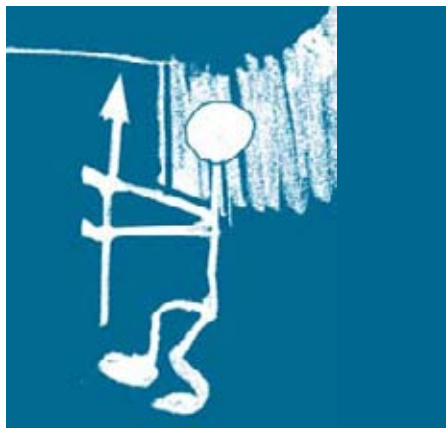
Установленный и корректно настроенный межсетевой экран становится ключевым элементом сетевой безопасности, снижая риски возникновения инцидентов ИБ и обеспечивая контролируемый и разграниченный доступ к информационным ресурсам как изнутри, так и снаружи. Дополнительным эффектом является снижение нецелевого использования сетевых ресурсов персоналом и повышение производственной дисциплины.

ДОПОЛНИТЕЛЬНО

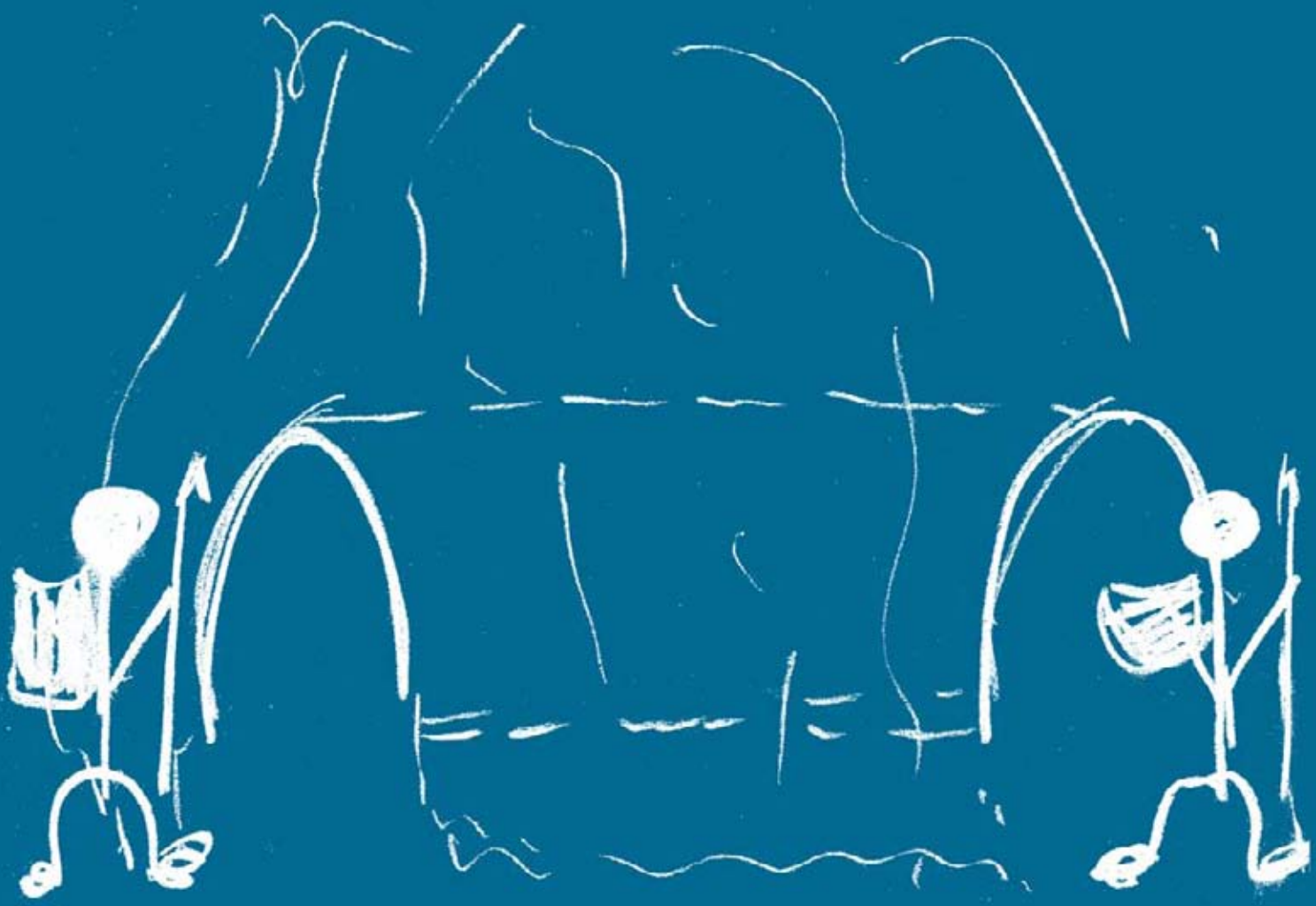
При оказании услуги применяются высокотехнологичные межсетевые экраны производства Cisco Systems, CheckPoint, Juniper Networks, StoneSoft, McAfee, Fortinet, а также отечественные сертифицированные средства.

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Виртуальные частные сети
- Обнаружение и предотвращение вторжений



Виртуальные частные сети



Для чего?

Потребность в развертывании виртуальных частных сетей (VPN) возникает в случае если сетевое взаимодействие (передача данных) осуществляется по недоверенным каналам связи:

- При взаимодействии территориально разнесенных площадок (подразделений, филиалов, «дочек» внутри холдинга)
- При организации санкционированного удаленного подключения к ресурсам сети компании извне
- При передаче конфиденциальнойинформации по сетям связи общего пользования (сеть Интернет, сети операторов связи)

Кроме того, необходимость в применении VPN-решений может возникнуть в ходе реализации требований Федерального закона № 152-ФЗ «О персональных данных», Федерального закона № 98-ФЗ «О коммерческой тайне», иных НПА в части обеспечения ИБ, а также отраслевых норм, таких как Комплекс БР ИББС.

Для кого?

Для компаний, заинтересованных в оптимизации своей деятельности за счет использования удаленных/мобильных ресурсов.

Описание услуги

В ходе оказания услуги проводится:

- Определение топологии существующей или перспективной территориально-распределеннойсети компании
- Выбор продукта для реализации виртуальной частной сети (для объектов сложной топологии разрабатывается ИТР)
- Поставка, установка и настройка программно-технических средств
- Интеграция с инфраструктурой PKI (в случае необходимости)
- Формирование VPN-туннелей
- Формирование правил управления доступом (ACL)
- Настройка параметров сигнализациии формирования уведомлений

Результат и его бизнес-ценность

Результатом оказания услуги является развернутая VPN-сеть, позволяющая организовать защищенное экстерриториальное межсетевое взаимодействие в рамках единого информационного пространства компании, обеспечивая совместную работу удаленных подразделений и филиалов, а также сотрудников, деятельность которых связана с командировками и разъездами либо осуществляется дистанционно.

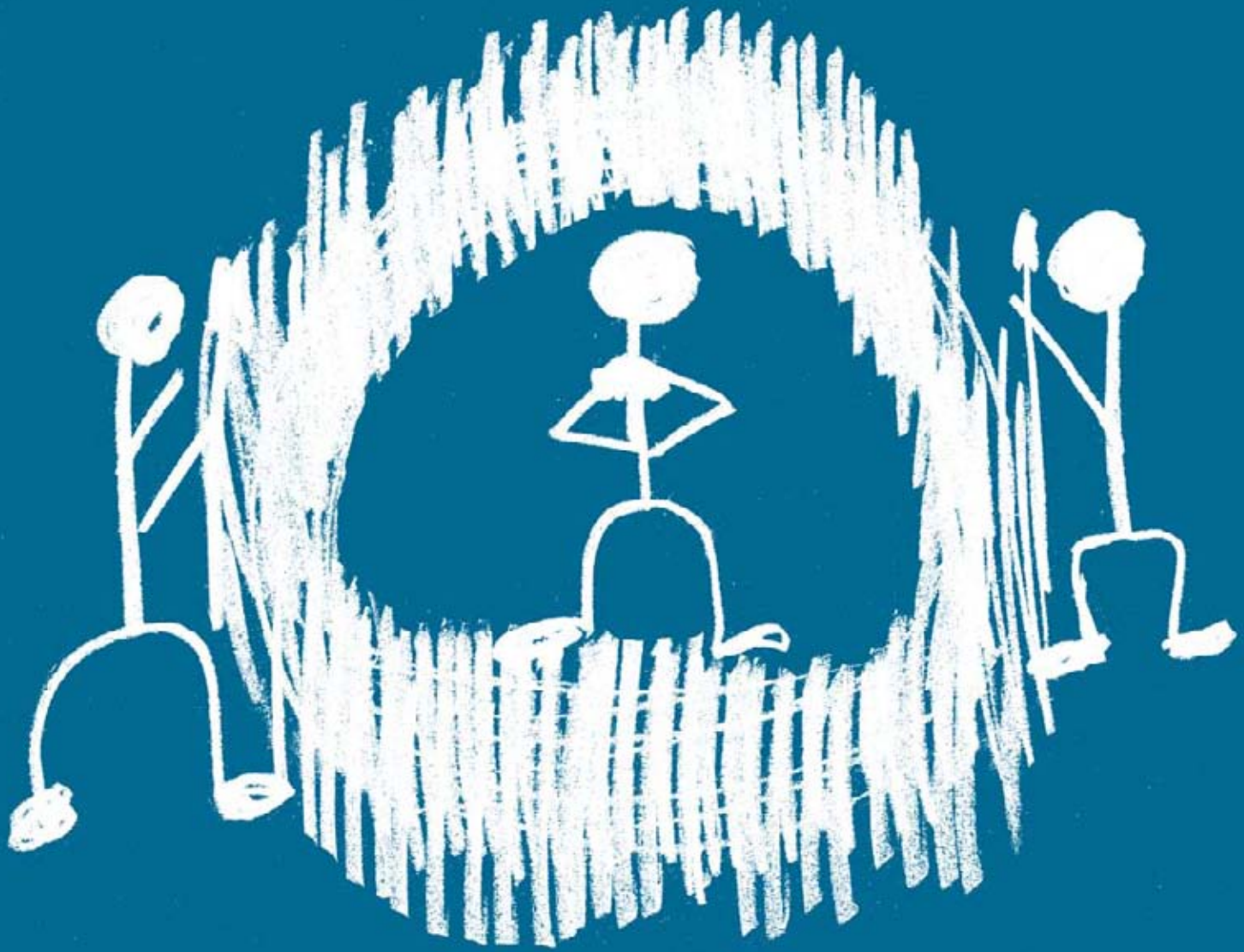
ДОПОЛНИТЕЛЬНО

Возможна реализация VPN с применением отечественных криптоалгоритмов на базе продуктов, прошедших сертификацию в ФСБ России.

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Межсетевое экранирование: защита периметра
- Инфраструктуры PKI и удостоверяющие центры

Предотвращение утечек данных



Для чего?

Услуга предназначена для создания условий по выявлению и блокированию попыток несанкционированного распространения в электронном виде (копирования, передачи) конфиденциальной информации, представляющей для ее владельца коммерческую или иную ценность. Тем самым на технологическом уровне осуществляется противодействие инсайду, а также профилактика негативных последствий халатного обращения с информацией ограниченного доступа и нарушения правил ее обработки:

- При использовании стандартных ИТ-сервисов (печать, сетевое хранилище, файловый доступ)
- При использовании средств электронных коммуникаций (электронная почта, IM, WWW)
- При работе с информационными системами (доступ к базам и хранилищам данных, порталам)
- При использовании съемных носителей информации

Для кого?

Компаниям, деятельность которых чувствительна к утечкам конфиденциальной информации.

Описание услуги

В ходе оказания услуги проводится:

- Классификация защищаемых ресурсов, определение типов и представлений конфиденциальной информации
- Определение каналов утечки информации, подлежащих контролю
- Выбор DLP-системы и разработка ИТР по ее применению
- Поставка, установка и настройка системы
- Формирование политик, связывающих тип конфиденциальной информации, канал утечки и реакцию на нарушение политики
- Настройка параметров формирования инцидентов ИБ, отчетности, сигнализации и уведомлений
- Разработка документации, опытная эксплуатация, «обучение» системы

Результат и его бизнес-ценность

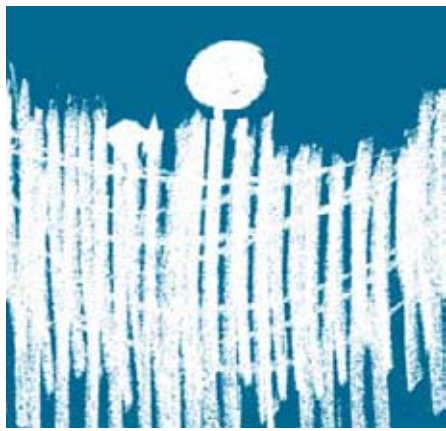
Ключевая ценность развернутого DLP-решения заключается в минимизации потерь, связанных с утечками данных к конкурентам, в СМИ и в другие нежелательные места. DLP-система с актуальными политиками позволяет обеспечить превентивную защиту от инсайдеров и нарушений правил обработки информации, оказать поддержку службам HR и внутренней безопасности, а также снизить издержки на поддержание заданного уровня защищенности ИТ-инфраструктуры за счет автоматизации процесса локализации конфиденциальных данных.

ДОПОЛНИТЕЛЬНО

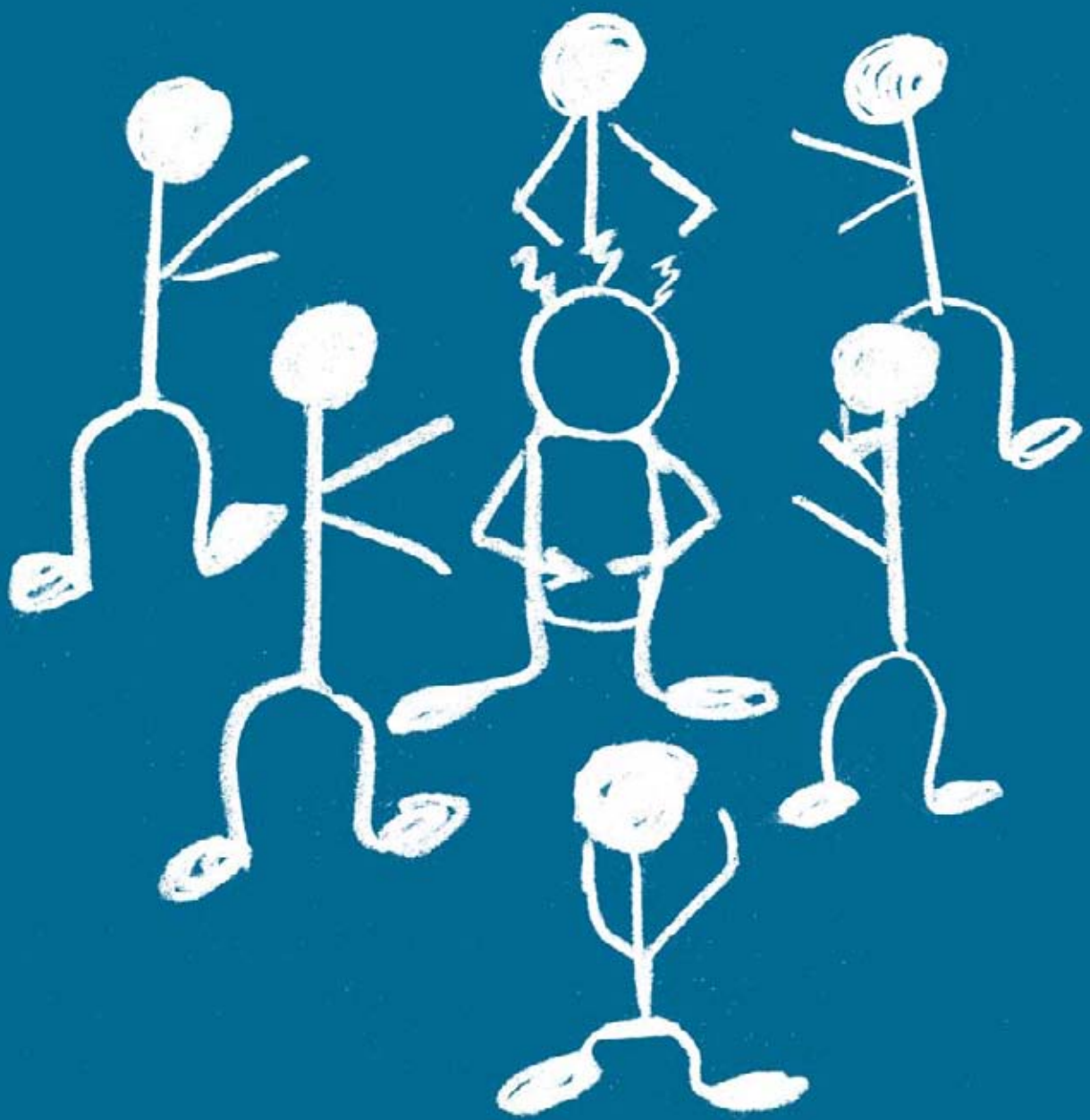
Услуга оказывается на основе DLP-систем разработки McAfee и RSA, а также российских продуктов.

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Анализ коммуникативных связей



Инфраструктуры PKI и удостоверяющие центры



Для чего?

Множество потребностей являются причиной для развертывания инфраструктуры открытых ключей (PKI) и создания удостоверяющего центра. Среди них:

- Необходимость в строгой аутентификации для доступа к ИТ-сервисам и системам
- Необходимость обеспечения защищенного обмена документами, в том числе по электронной почте
- Обеспечение аутентичности и неотказуемости действий пользователей при работе с информационными ресурсами компании
- Организация юридически значимого документооборота
- Реализация положений Федерального закона № 63-ФЗ «Об электронной подписи»
- Автоматизация процессов управления жизненным циклом сертификатов ключей проверки электронных подписей

Для кого?

Компаниям, заинтересованным в повышении уровня ИБ за счет создания централизованной инфраструктуры для поддержки функций авторизации, доверия, защиты информации или линий связи.

Описание услуги

В ходе оказания услуги проводится:

- Определение целей использования PKI
- Выбор типа электронной подписи (в случае необходимости)
- Выбор, установка и настройка средств удостоверяющего центра (при необходимости разрабатывается инженерно-техническое решение)
- Документирование процедур, связанных с работой удостоверяющего центра и обращением со средствами криптографической защиты
- Ввод в действие развернутой инфраструктуры PKI

Результат и его бизнес-ценность

Результатом оказания услуги является развернутая PKI или отдельные средства УЦ, позволяющие обеспечить решение широкого перечня централизованных задач ИБ, снижая при этом стоимость владения активами (ИТ-системами и средствами обеспечения ИБ) за счет упрощения администрирования и удобства дальнейшего наращивания спектра применяемых средств и технологий. Внедрение PKI делает возможным перевод значительной части документооборота в электронную форму с сохранением юридической значимости, тем самым снижая общие операционные расходы компании (OpEx).

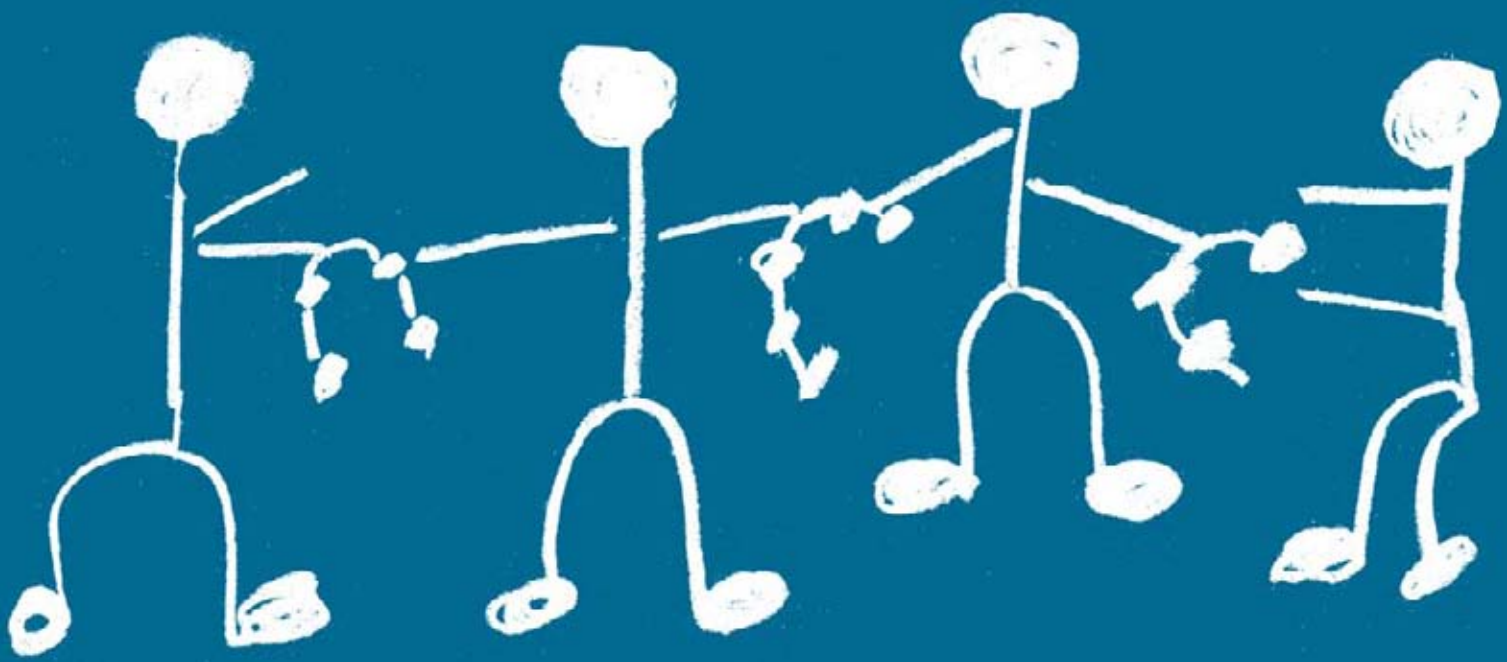
ДОПОЛНИТЕЛЬНО

На стадии ввода PKI в действие может быть проведена юридически значимая «церемония» выпуска корневого сертификата (Root Key Ceremony).

СВЯЗАННЫЕ УСЛУГИ

- Управление доступом
- Шифрование данных
- Виртуальные частные сети

Шифрование данных



Для чего?

Услуга актуальна для заказчиков, которым требуется обеспечить:

- Защиту от хищения данных и неправомерного доступа к информационным ресурсам
- Безопасность информации, хранящейся на переносных устройствах (ноутбуки, нетбуки, коммуникаторы, съемные носители и т.п.) в случае их утери или кражи
- Защищенную передачу информации (в том числе резервных копий) на хранение за пределы компании
- Доверенную загрузку операционных систем

Для кого?

Компаниям, стремящимся повысить уровень конфиденциальности информационных ресурсов.

Описание услуги

В ходе оказания услуги проводится:

- Определение целей использования средств криптографической защиты информации
- Выбор методов шифрования информациии обоснование их применения
- Выбор, установка и настройка СКЗИ (для сложных объектов защиты разрабатывается инженерно-техническое решение)
- Интеграция с PKI (в случае необходимости)
- Документирование процедур, связанных с обращением со средствами криптографической защиты информации

Результат и его бизнес-ценность

Результатом оказания услуги является комплекс СКЗИ, который на основе документированных процедур обеспечивает конфиденциальность информации путем ее шифрования. За счет этого снижаются потери и издержки, связанные с неправомерным доступом к важным данным в случае потери носителей информации, при случайном доступе со стороны неавторизованного персонала вследствие нарушения или халатности, при попытках доступа к данным со стороны лиц, ознакомление которых с защищаемой информацией нежелательно.

ДОПОЛНИТЕЛЬНО

Для доступа к зашифрованным данным может применяться надежная двухфакторная аутентификация.

СВЯЗАННЫЕ УСЛУГИ

- Инфраструктуры PKI и удостоверяющие центры
- Управление доступом

Безопасность сетей Windows

Для чего?

Операционные системы семейства Microsoft Windows являются наиболее распространенными, что предопределило их положение в фокусе внимания злоумышленников (хакеров, разработчиков вирусов, мошенников, недобросовестных сотрудников). Вместе с тем, ОС Windows содержат большое количество встроенных механизмов безопасности, грамотное применение которых наряду с выполнение рекомендаций по безопасной настройке способно существенно повысить уровень ИБ Windows-сетей. Дополнительными факторами, принимаемыми во внимание, следует считать:

- Потребность в повышении уровня ИБ без использования дополнительных (наложенных) средств защиты информации
- Потребность в повышении отдачи от имеющихся продуктов линейки Microsoft Windows
- Потребность в централизованном управлении учетными записями пользователей и компьютерами в сети Windows
- Потребность в унифицированной реализации политик конфигурирования и безопасности в сетях Windows

Для кого?

Широкому кругу заказчиков, применяющих ОС Microsoft Windows.

Описание услуги

В ходе оказания услуги проводится:

- Сбор необходимой информации о компонентах ИТ-инфраструктуры
- Конфигурация контроллера(ов) домена
- Создание учетных записей пользователей, пользовательских групп, установка индивидуальных и групповых параметров в Active Directory
- Создание и настройка объектов групповых политик
- Создание и настройка шаблонов безопасности
- Организация сервиса централизованной установки обновлений
- Настройка правил доступа к файлам и папкам (SACL)
- Настройка параметров сигнализации и формирования уведомлений

Результат и его бизнес-ценность

Активированные механизмы безопасности ОС Windows обеспечивают необходимый базовый уровень защиты, снижая риски возникновения инцидентов ИБ на уровне операционных систем и службы каталогов. Централизация и автоматизация администрирования Windows-сети снижает операционные затраты на ИТ, а также позволяет в дальнейшем легко разворачивать новые ИТ/ИБ-сервисы и системы.

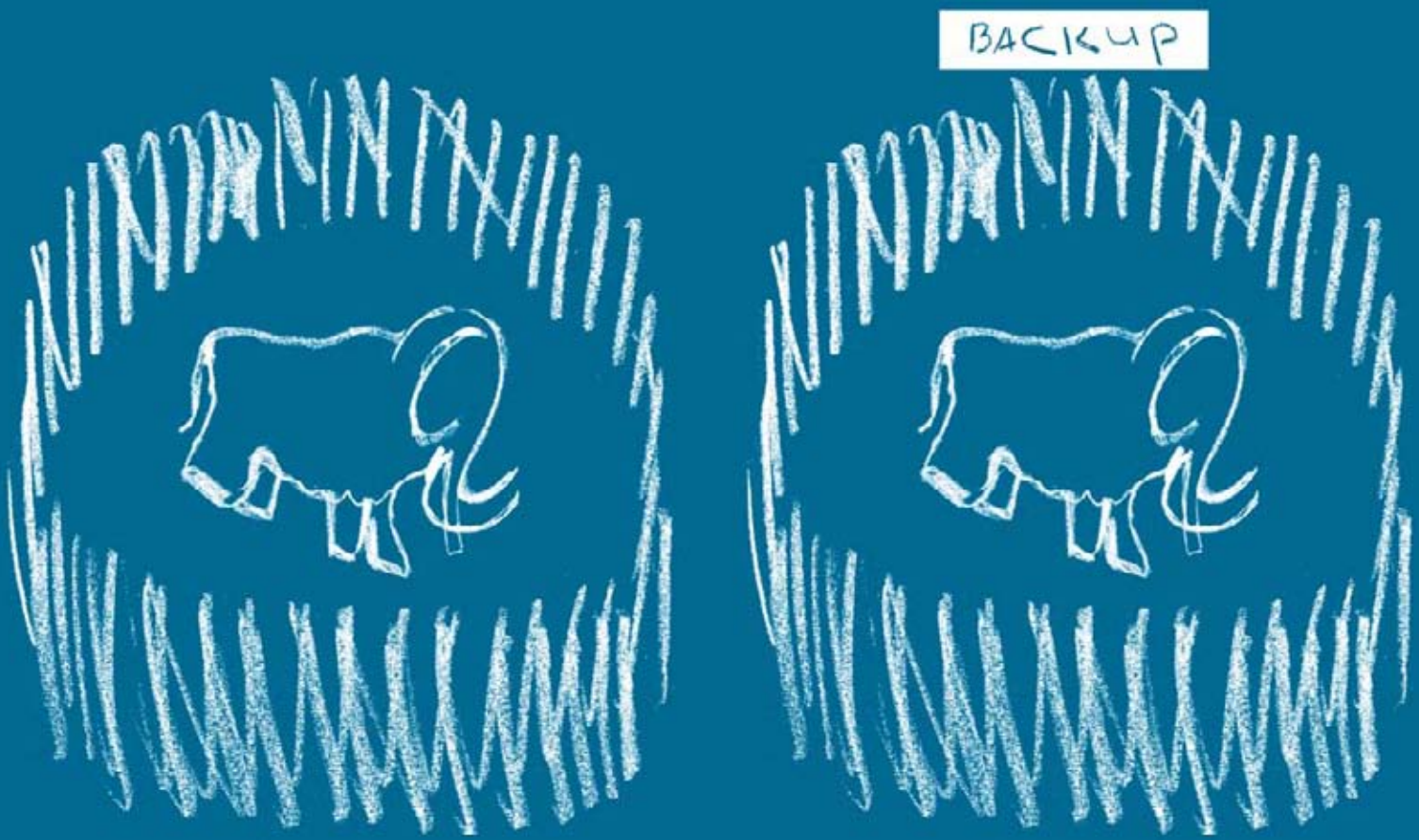
ДОПОЛНИТЕЛЬНО

При оказании услуги учитываются положения рекомендаций компании-разработчика (Microsoft Windows Security Guide).

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Безопасность информационных систем

Резервное копирование



Для чего?

Услуга ориентирована на удовлетворение следующих потребностей:

- Необходимость повышения уровня доступности и целостности информационных ресурсов
- Обеспечение оперативного восстановления поврежденных информационных ресурсов
- Обеспечение оперативного восстановления работоспособности ИТ-систем и сервисов в случае сбоев или отказов оборудования

Для кого?

Заказчикам, стремящимся снизить вероятность потери значимой информации и обеспечить высокий уровень непрерывности ключевых ИТ-систем.

Описание услуги

В ходе оказания услуги проводится:

- Определение информационных ресурсов, подлежащих резервированию, уточнение архитектурных особенностей информационных систем
- Выбор способов и технологий резервированного копирования
- Разработка политики резервирования данных
- Сайзинг оборудования, выбор, установка и настройка средств резервного копирования
- Настройка параметров сигнализации и уведомлений
- Разработка и ввод в действие процедуры резервного копирования и восстановления данных

Результат и его бизнес-ценность

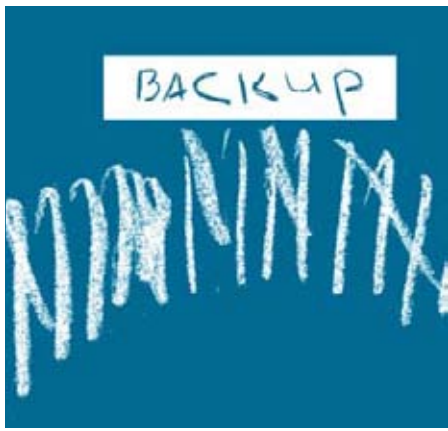
Результатом оказания услуги является комплекс средств резервного копирования и восстановления информации, который на основе действующей процедуры резервирования и восстановления позволяет обеспечить высокий уровень доступности и целостности информационных ресурсов компании, снизить риски потери информации и уменьшить время простоя за счет минимизации времени восстановления информации после сбоя или отказа.

ДОПОЛНИТЕЛЬНО

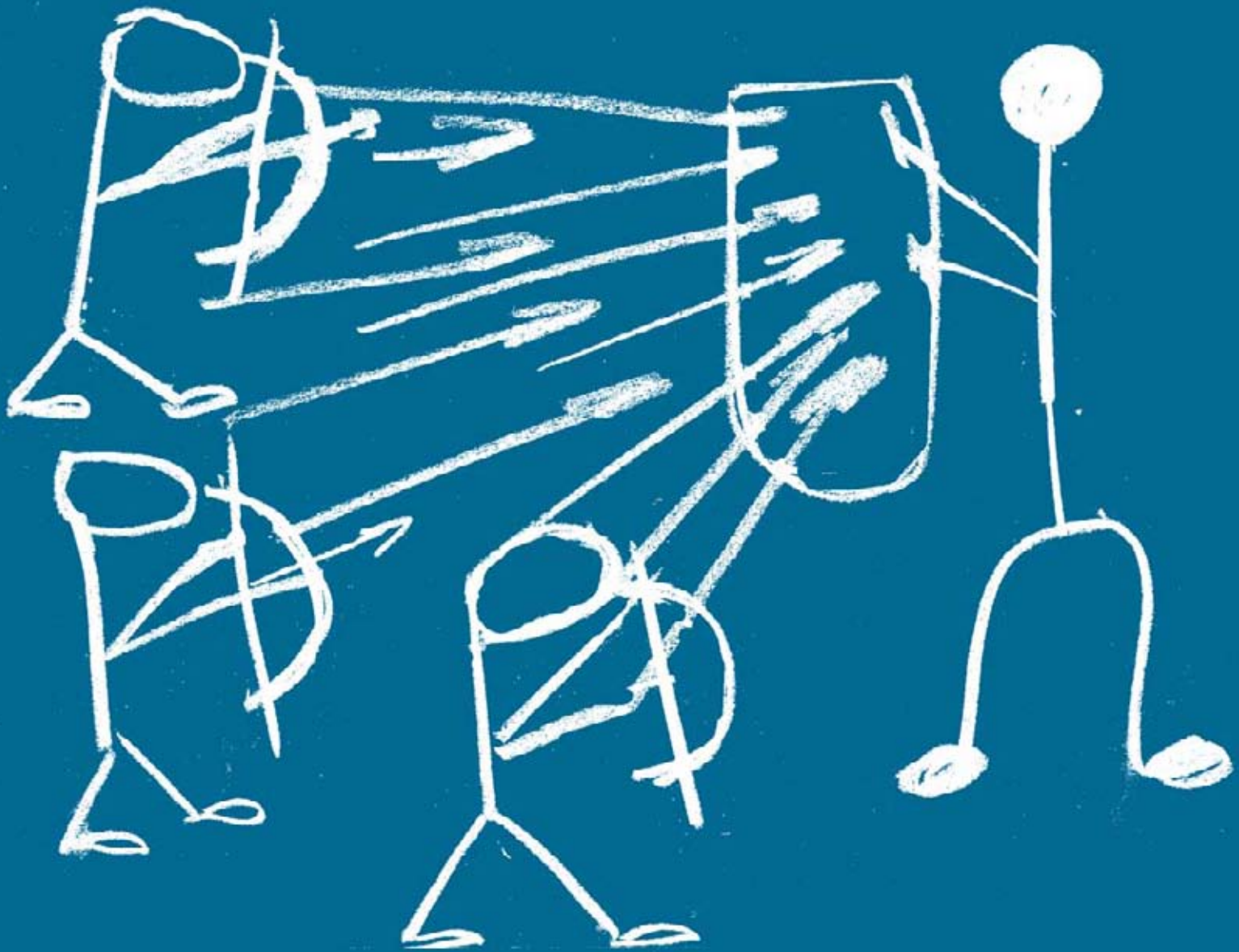
Для оказания услуги применяются встроенные средства ОС, СУБД и информационных систем, специализированное ПО а также промышленные решения для резервирования и восстановления данных на основе дисковых и ленточных систем хранения.

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Безопасность информационных систем
- Шифрование данных
- Непрерывность ИТ-услуг



Защита от спама



Для чего?

Услуга предоставляется в целях противодействия распространению нежелательной электронной почты и устранения комплекса негативных факторов, связанных с этим явлением:

- Снижение производительности почтовых серверов
- Потеря «легальных» сообщений или нарушение процесса их доставки
- Распространение вирусов и вытекающие из этого риски нарушения информационной безопасности
- Потери рабочего времени сотрудников
- Репутационные потери

Для кого?

Компаниям, активно использующим в повседневной деятельности сервис электронной почты.

Описание услуги

В ходе оказания услуги проводится:

- Анализ корпоративного сервиса электронной почты (архитектура, реализация, балансировка нагрузки, схема маршрутизации почты, нагрузочные показатели, контингент пользователей)
- Выбор решения класса «Антиспам», разработка ИТР по его применению (схема включения, политика и технологии фильтрации, нагрузочные характеристики, отказоустойчивость, управление)
- Установка и настройка антиспам-решения
- Опытная эксплуатация и оптимизация (тонкая настройка) политики фильтрации

Результат и его бизнес-ценность

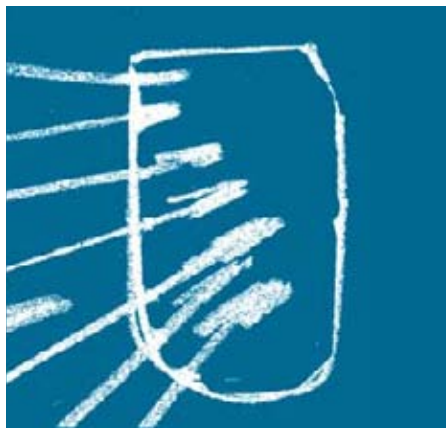
Результатом оказания услуги является настроенный и запущенный сервис информационной безопасности «Антиспам». Его применение обеспечивает снижение общих издержек и повышение производительности компании за счет устранения комплекса негативных факторов, связанных с распространением спама.

ДОПОЛНИТЕЛЬНО

Одновременно с защитой от спама как правило решается задача антивирусной защиты корпоративного почтового сервиса.

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Антивирусная защита



Безопасность мобильных устройств (EMM, MDM)

Для чего?

Услуга предоставляется в качестве ответной меры на резкий рост применения мобильных устройств (планшетов, коммуникаторов, смартфонов) в деловой и производственной сфере и связанные с этим риски нарушения ИБ:

- Несанкционированный доступ к информации на мобильном устройстве при его утере
- Нарушения ИБ как результат деятельности вирусов
- Несанкционированный доступ к корпоративным информационным системам при утере мобильного устройства, с которого возможен доступ к таким ИС
- Нецелевое использование корпоративных мобильных устройств (постороннее ПО, превышение лимита на услуги связи)

Для кого?

Заказчикам, активно использующим в повседневной деятельности мобильные устройства, в т.ч. по модели BYOD («Bring your own device»).

Описание услуги

В ходе оказания услуги проводится:

- Анализ корпоративных мобильных сервисов и информационных ресурсов, доступных с мобильных устройств
- Изучение контингента пользователей мобильных устройств
- Анализ особенностей и параметров группировки мобильных устройств (платформы, версии, ПО, сервисы)
- Определение целей и задач реализации услуги (в контексте Enterprise Mobility Management)
- Выбор EMM-решения, установка и настройка ПО
- Разработка документации, обучение администраторов, информирование пользователей
- Опытная эксплуатация и оптимизация (тонкая настройка) политик EMM

Результат и его бизнес-ценность

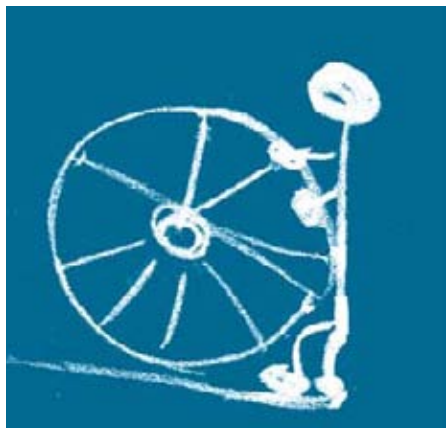
Результатом оказания услуги является развернутый сервис EMM (MDM), который упорядочит применение планшетов, коммуникаторов, смартфонов в повседневной деятельности. Для мобильных устройств, принадлежащих как сотрудникам, так и компании, обеспечивается такой же уровень защиты и контроля, который применяется для ноутбуков и настольных компьютеров. EMM не только повышает уровень ИБ, но и позволяет снизить затраты на управление мобильными устройствами и поддержку, а также сократить совокупную стоимость владения благодаря максимальному использованию имеющейся ИТ-инфраструктуры и личных устройств.

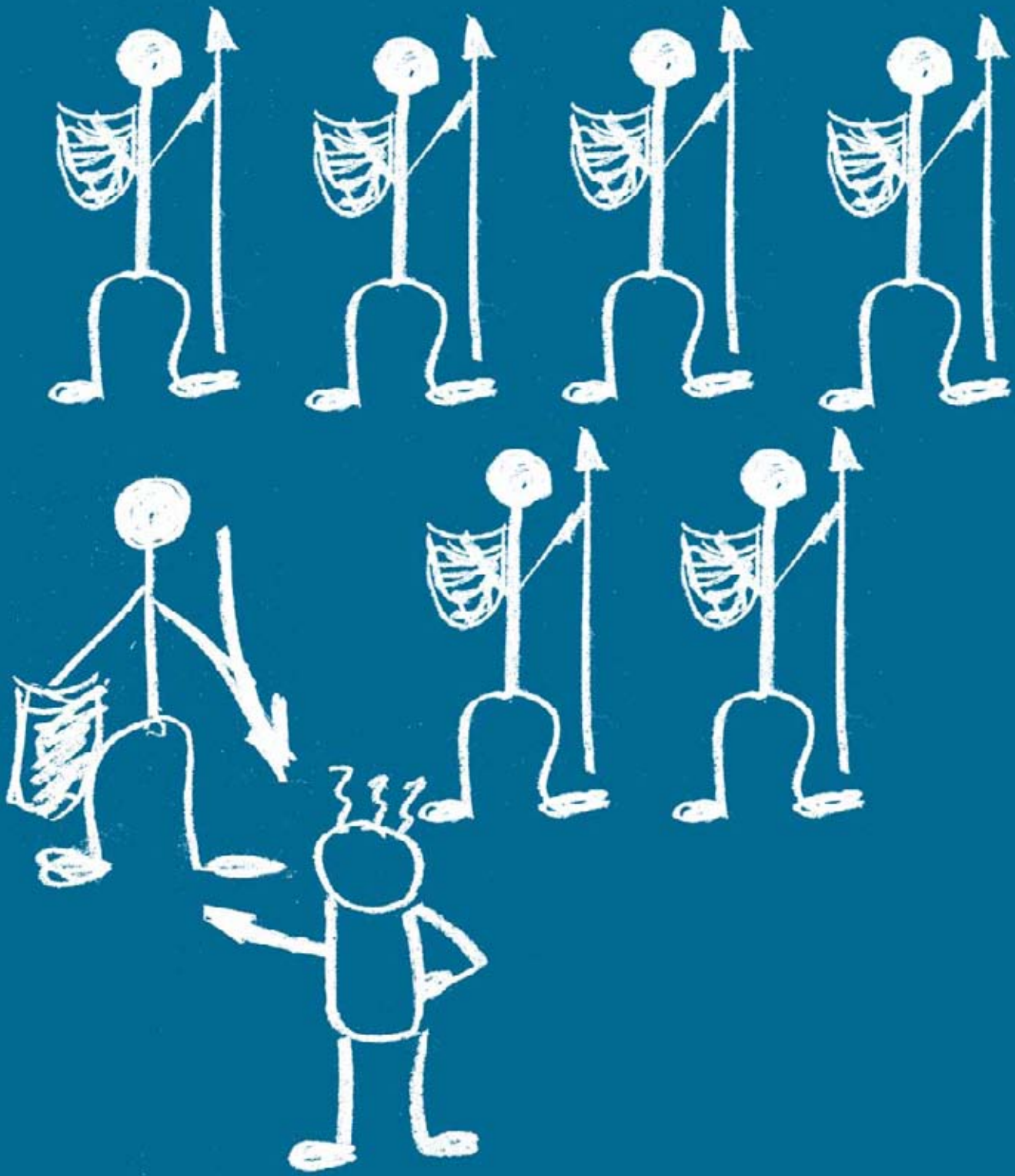
ДОПОЛНИТЕЛЬНО

Услуга предоставляется с использованием продуктов McAfee EMM, Mobile Iron Virtual Smartphone Platform, других EMM (MDM)-вендоров.

СВЯЗАННЫЕ УСЛУГИ

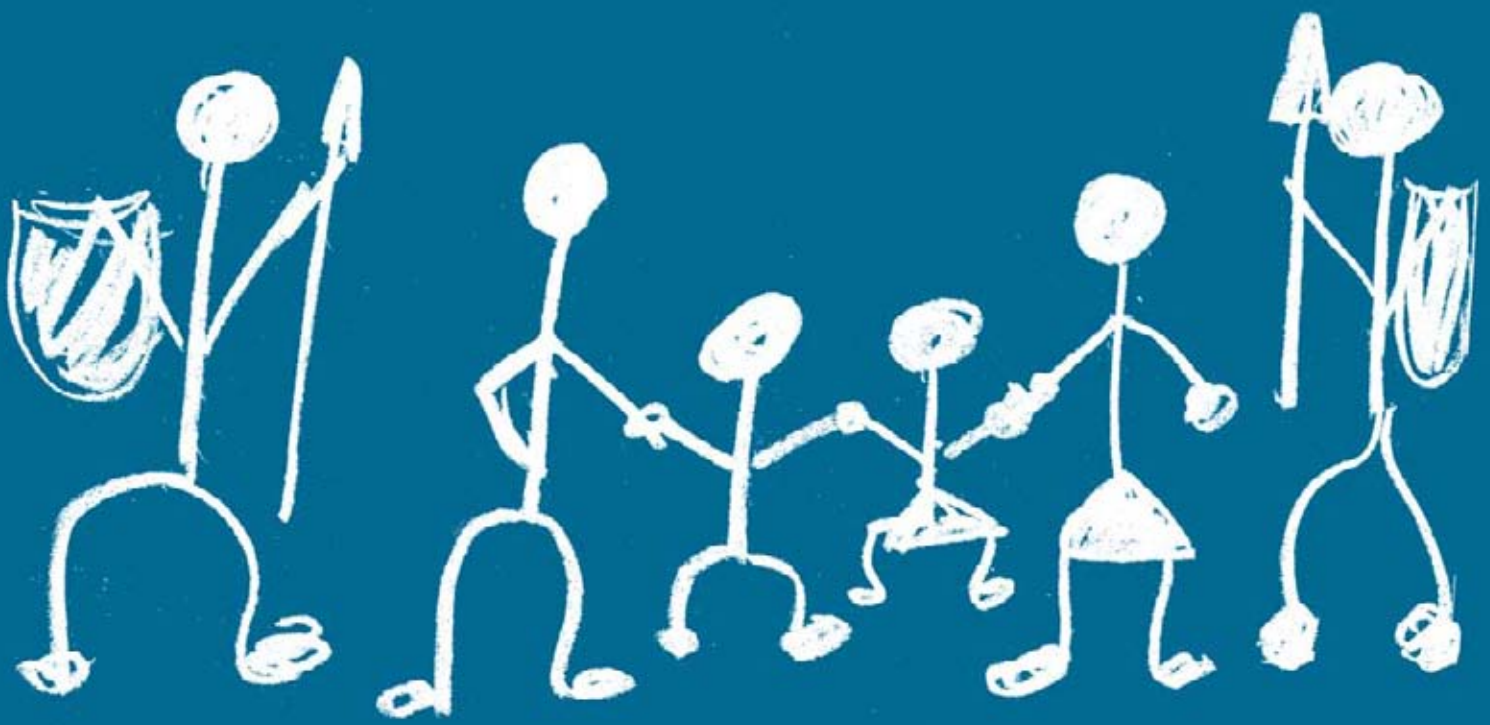
- Комплексные системы обеспечения информационной безопасности
- Шифрование данных





Соответствие требованиям

Обработка и защита персональных данных (152-ФЗ)



Для чего?

Услуга нацелена на приведение процессов обработки и защиты персональных данных (ПДн) в соответствие с требованиями действующего законодательства. Решение о передаче этой задачи на аутсорсинг интегратору обычно вызвано:

- Значительным объемом нормативных правовых актов в этой области и сложностью описанных в них требований и рекомендаций
- Высокой трудоемкостью комплексной реализации требований
- Отсутствием подготовленных специалистов, а также других ресурсов для качественной организации обработки и защиты ПДн
- Вниманием со стороны государственных регуляторов (ФСТЭК и ФСБ России, Роскомнадзор) к обработке персональных данных

Для кого?

Операторам, осуществляющим обработку персональных данных.

Описание услуги

В ходе оказания услуги проводится:

- Анализ процессов обработки ПДн и информационных систем персональных данных (в т.ч. классификация и моделирование угроз)
- Разработка организационно-распорядительных документов, регламентирующих процессы обработки и защиты ПДн
- Разработка технического проекта на систему защиты ПДн (СЗПДн)
- Поставка средств защиты информации, развертывание и настройка СЗПДн, ее опытная эксплуатация и испытания, внедрение необходимых организационных процессов
- Аттестация ИСПДн (для государственных и муниципальных органов — обязательно, для прочих операторов — при необходимости)
- Информирование (повышение осведомленности) руководителей организации и пользователей ИСПДн
- Операционная поддержка процессов обработки и защиты ПДн

Результат и его бизнес-ценность

Результат оказания услуги: документы + процессы + система защиты. Этим комплексом обеспечивается надлежащий порядок обработки и высокий уровень безопасности ПДн. Это позволяет снизить или обосновать принятие таких рисков, как:

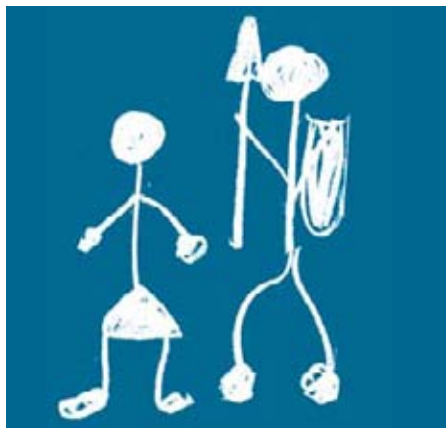
- помехи в деятельности со стороны субъектов ПДн, инициированные обращениями по вопросам обработки их ПДн (в т.ч. судебные иски)
- помехи в деятельности со стороны госрегуляторов, включая возможные издержки (штрафы, отвлечение персонала и т.п.)
- репутационные потери (распространение информации в СМИ о проблемах в обработке ПДн) и связанные с ними издержки

ДОПОЛНИТЕЛЬНО

При оказании услуг могут учитываться требования отраслевой нормативной базы

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности



Обеспечение защиты информации в платежных системах (НПС)

Для чего?

Федеральный закон № 161-ФЗ «О национальной платежной системе» и ряд подзаконных актов Правительства РФ и Банка России обязали участников Национальной платежной системы (НПС) обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством РФ. Решение о передаче этой комплексной задачи на аутсорсинг интегратору обычно вызвано:

- Значительным объемом нормативно-правовых актов в данной области и многообразием требований по защите различных видов информации ограниченного доступа
- Высокой трудоемкостью комплексной реализации требований
- Отсутствием ресурсов для качественной организации работ

Для кого?

Участникам НПС: операторам по переводу денежных средств, банковским платежным агентам (субагентам), операторам платежных систем, операторам услуг платежной инфраструктуры.

Описание услуги

В ходе оказания услуги проводится:

- Анализ защищенности автоматизированных систем
- Анализ и оценка рисков информационной безопасности
- Оценка выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств (аудит субъектов НПС на соответствие требованиям Положения № 382-П)
- Разработка рекомендаций по улучшению процессов обеспечения ИБ
- Разработка модели угроз безопасности информации
- Разработка организационно-распорядительной документации в соответствии с требованиями НМД
- Разработка и проектирование системы защиты в соответствии с требованиями НМД
- Внедрение средств защиты информации (шифровальных (криптографических) средств, средств защиты информации от несанкционированного доступа, средств антивирусной защиты, средств межсетевого экранирования, системы обнаружения вторжений, средств контроля (анализа) защищенности)
- Помощь в подготовке отчетности по формам ЦБ РФ в рамках НПС

Результат и его бизнес-ценность

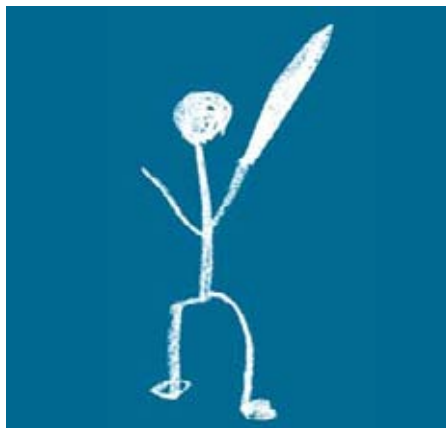
Результатом оказания услуги является комплексная система защиты информации, снабженная необходимой локальной нормативной базой, отвечающей требованиям законодательства в области НПС. Кроме выполнения требований законодательства, внедрение подобной системы позволит повысить доверие партнеров и клиентов организаций-участников НПС. За счет объединения в одном проекте нескольких потоков работ обеспечивается снижение капитальных затрат (CapEx).

ДОПОЛНИТЕЛЬНО

Возможна поэтапная реализация проекта

СВЯЗАННЫЕ УСЛУГИ

- Аудит информационной безопасности
- Обработка и защита персональных данных (152-ФЗ)



Безопасность организаций банковской системы РФ: СТО БР ИББС

Для чего?

Комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы РФ» (Комплекс БР ИББС) является одним из наиболее проработанных отраслевых стандартов в области ИБ в России. Несмотря на рекомендательный характер, Комплекс БР ИББС де-факто является стратегической линией российских банков или рассматривается в качестве таковой. С расширением за счет положений об обработке и защите персональных данных Комплекс БР ИББС приобрел новое качество практического руководства к действию в этой области.

Поскольку стандарты и рекомендации СТО БР ИББС построены с учетом лучших практик и специфики банковской деятельности, применение его положений в работе ИТ/ИБ-департаментов кредитно-финансовых учреждений позволяет им находиться на передовом рубеже технологий управления и обеспечения информационной безопасности.

Для кого?

Организациям банковской системы России.

Описание услуги

Услуга делится на два взаимосвязанных блока:

- Аудит на соответствие требованиям СТО БР ИББС: проверка уровня реализации требований стандарта в организации банковской системы
- Приведение в соответствие СТО БР ИББС: разработка документации и бизнес-процессов, проектирование и внедрение СОИБ в соответствии с положениями Комплекса БР ИББС, итоговая оценка соответствия

Результат и его бизнес-ценность

Результат оказания услуги на каждом этапе работ характеризуется целым рядом приобретаемых выгод:

- Возможность обоснованно и планомерно повышать уровень ИБ, устранять недостатки и уязвимости
- Действенная методическая поддержка отраслевого регулятора, выраженная в виде разъяснений и регулярно обновляемых стандартов
- Положительный PR-эффект за счет возможности демонстрировать соответствие СТО БР ИББС, повышение уровня доверия к банку
- Сбалансированная организация обработки и защиты ПДн по адекватным требованиям, согласованным с госрегулятором

В конечном итоге заказчик получает возможность обеспечить у себя реальную, а не «бумажную» безопасность, минимизируя риски ИБ и снижая издержки на ИБ за счет построения единой системы управления.

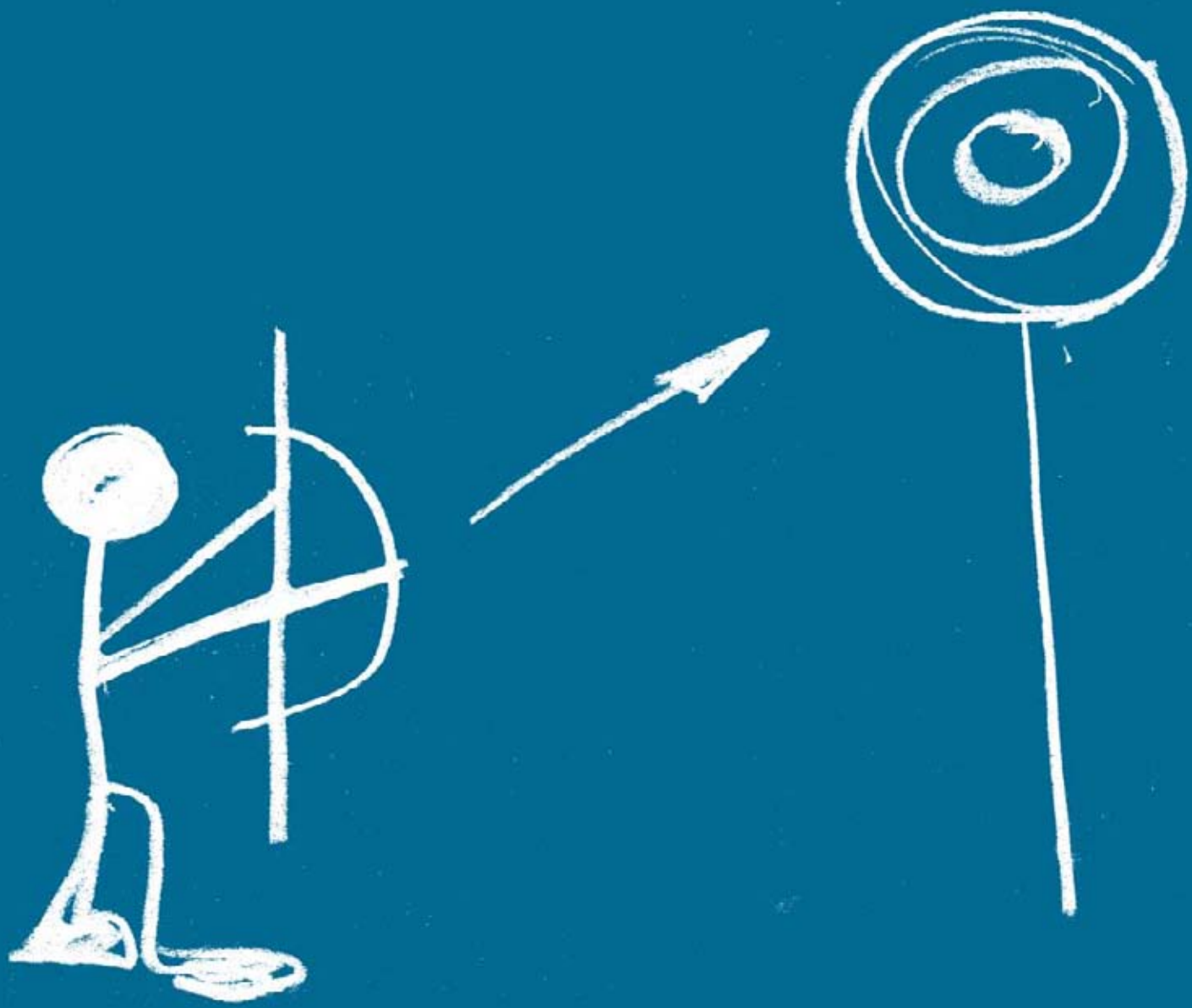
ДОПОЛНИТЕЛЬНО

Подробности приведены на сайте «Вулкана» в разделе «Услуги | Соответствие требованиям | СТО БР ИББС».

СВЯЗАННЫЕ УСЛУГИ

- Создание системы управления информационной безопасностью
- Управление уязвимостями
- Непрерывность ИТ-сервисов

Аттестация объектов информатизации



Для чего?

Аттестация объектов информатизации (ОИ) — это комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК (Гостехкомиссией) России. Как правило, аттестация является заключительным этапом комплексных проектов в области защиты информации, проводимых в интересах государственных и муниципальных органов.

Аттестация предшествует началу обработки подлежащей защите информации и вытекает из необходимости официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

Для кого?

Проведение аттестации необходимо государственным и муниципальным органам при выполнении работ по защите конфиденциальной информации.

Описание услуги

Порядок проведения аттестации включает следующие действия:

- Подачу и рассмотрение заявки на аттестацию
- Предварительное ознакомление с аттестуемым ОИ
- Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом ОИ (при необходимости)
- Разработка программы и методики аттестационных испытаний
- Заключение договоров на аттестацию
- Проведение аттестационных испытаний ОИ
- Оформление, регистрация и выдача «Аттестата соответствия» (при наличии положительного заключения)
- Осуществление госконтроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованного ОИ
- Разработка пакета документации по управлению ИБ.

Результат и его бизнес-ценность

Результат оказания услуги — «Аттестат соответствия», выданный на период, в течение которого обеспечивается неизменность условий функционирования ОИ и технологии обработки защищаемой информации, но не более чем на 3 года. При условии выполнения правил эксплуатации объекта и неизменность условий его функционирования «Аттестат соответствия» является формальным свидетельством выполнения организаций установленных требований в области защиты информации для заданного ОИ.

ДОПОЛНИТЕЛЬНО

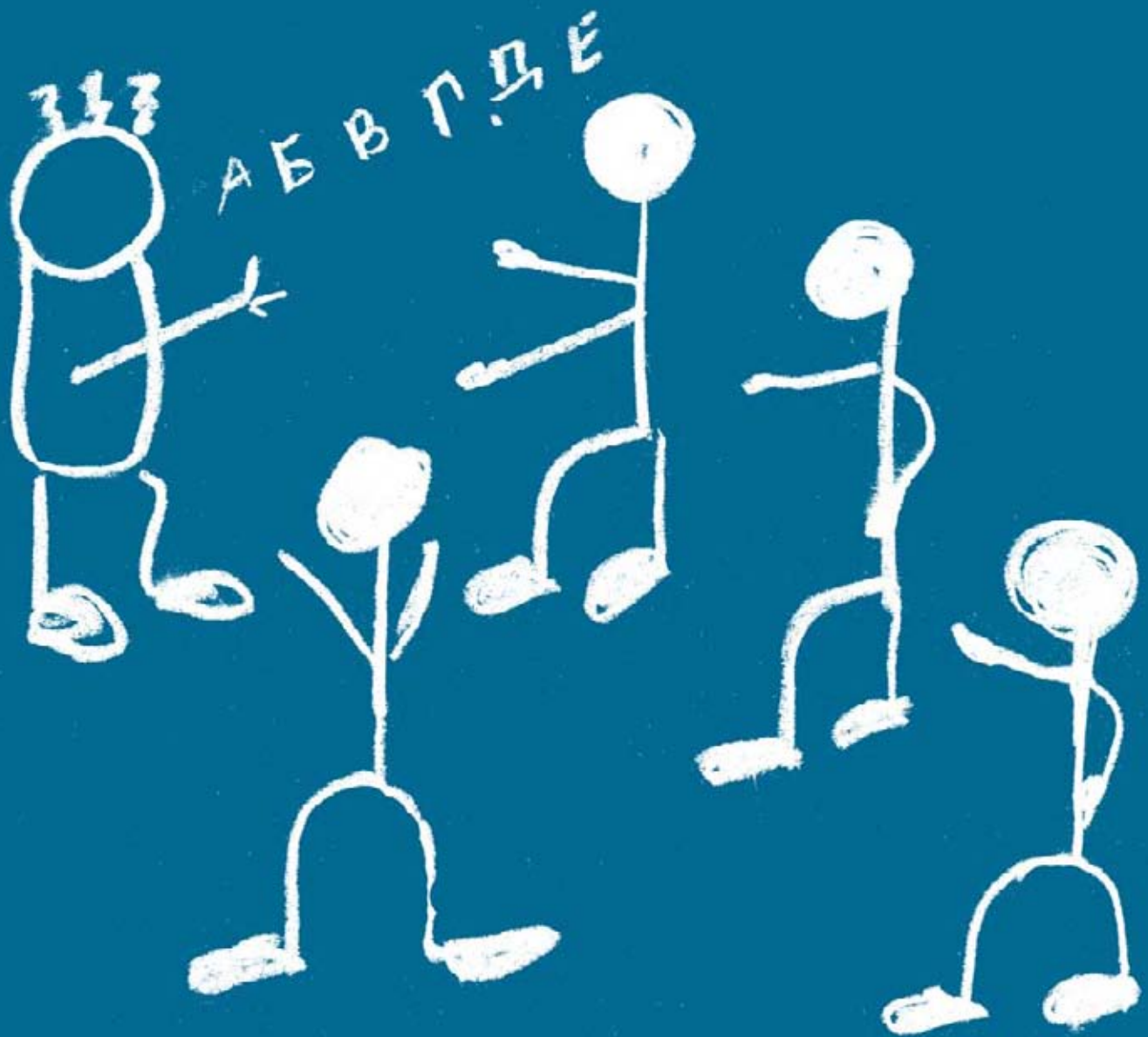
Аттестация выполняется в соответствии с положениями руководящих и нормативно-методических документов ФСТЭК (Гостехкомиссии) России.

СВЯЗАННЫЕ УСЛУГИ

- Безопасность информационных систем
- Обработка и защита персональных данных (152-ФЗ)

Консалтинг

Соискателям лицензий ФСТЭК и ФСБ России



Для чего?

Компании руководствуются различными мотивами, побуждающими их стать лицензиатами ФСТЭК и/или ФСБ России. Для одних это — потребность бизнеса, для других — возможность работать с госзаказчиками, для третьих — обязательное условие осуществления основной деятельности. Вне зависимости от этих причин, соискатели лицензий должны пройти по пути выполнения лицензионных требований. В этом вопросе часто необходима квалифицированная помощь и поддержка.

Для кого?

Соискателям лицензий ФСТЭК России на следующие виды деятельности:

- Разработка и производство средств защиты конфиденциальной информации
- Техническая защита конфиденциальной информации

Соискателям лицензий ФСБ Россиина следующие виды деятельности*:

- Разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств
- Выполнение работ, оказание услуг в области шифрования информации, ТО шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (крипто графических) средств

* виды деятельности сгруппированы для наглядности

Описание услуги

В процессе предоставления услуги осуществляется:

- Методическое сопровождение подготовки необходимых документов и подачи заявления в ФСТЭК России и/или ФСБ России
- Разработка организационно-распорядительных документов
- Подготовка и аттестация АС
- Подготовка и аттестация защищаемого помещения

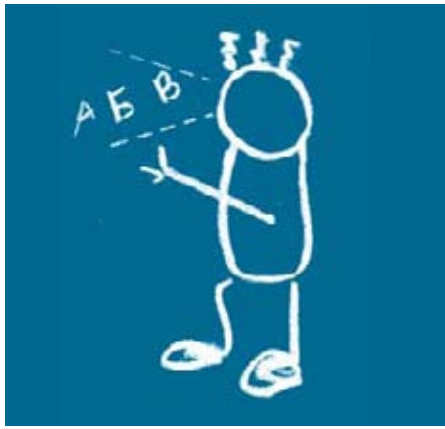
Результат и его бизнес-ценность

Результат оказания услуги — максимально полная реализация лицензионных требований в организации-соискателе и высокая степень готовности к успешному прохождению процесса выдачи лицензий на виды деятельности.

Обращение к профессиональным консультантам обеспечит снижение издержек на лицензирование, оптимизацию затрачиваемого времени и преодоление вероятных «подводных камней» на ранней стадии процесса подготовки.

ДОПОЛНИТЕЛЬНО

Основные НПА: Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности», постановления Правительства Российской Федерации от 3 февраля 2012 г. № 79, от 3 марта 2012 г. № 171 и от 16 апреля 2012 г. № 313, нормативно-методические документы ФСТЭК и ФСБ России (в части касающейся).



Расследование инцидентов

Для чего?

Заинтересованность в услуге «Расследование инцидентов» обусловлена наиболее неблагоприятными обстоятельствами, а именно — обнаружением факта нарушения ИБ или наличием существенных подозрений.

Целевыми установками заказчика в этом случае являются:

- Остановка негативного воздействия, если нарушение продолжается или развивается
- Определение обстоятельств и идентификация уязвимостей, способствовавших наступлению события
- Определение сценария развития инцидента (реализации атаки)
- Поиск виновных должностных лиц, определение источника атаки (идентификация злоумышленника в целях возмещения ущерба)
- Сбор доказательств для передачи в правоохранительные органы
- Предотвращение возникновения подобных инцидентов в будущем

Для кого?

Организациям, зафиксировавшим серьезный инцидент ИБ либо подозревающим существование данного факта по косвенным признакам.

Описание услуги

Методики расследования инцидентов ИБ варьируются в зависимости от особенностей объекта и условий нарушения. Они ориентированы на получение полной и достоверной (насколько это возможно при данных конкретных условиях) информации о факторах и обстоятельствах, предшествовавших событию и сопровождавших инцидент. Источниками информации служат регистрационные файлы, данные о статистике сетевого трафика, записи в журналах событий средств защиты, операционных систем, СУБД. В некоторых случаях необходимая информация может быть предоставлена сервис-провайдером телекоммуникационных услуг. Кроме того, при расследовании инцидентов проводятся опросы персонала, прямо или косвенно имеющего отношения к обстоятельствам возникновения инцидента. Применяются специализированные технологии восстановления удаленной информации.

Полученные данные анализируются, позволяя воссоздать сценарий нарушения. Сформулированные на основе такого анализа выводы докладываются руководству пострадавшей организации.

Результат и его бизнес-ценность

Результат оказания услуги — отчет о расследовании инцидента ИБ (с приложением доказательной информации), содержащий сведения о сценарии нарушения и его причинах, а также рекомендации по улучшению мер защиты информации. Принятие указанных мер обеспечивает снижение возможных потерь от инцидентов ИБ. Кроме того, материалы расследования предоставляют возможность возмещения нанесенного ущерба.

СВЯЗАННЫЕ УСЛУГИ

- Восстановление данных
- Тест на проникновение

Восстановление данных

Для чего?

Хранение данных в электронном виде сопровождает практически любую деятельность современной компании (предприятия). Нередки ситуации, когда из-за отказов аппаратуры или сбоев программного обеспечения доступ к данным на машинном носителе становится невозможным. Кроме того, информация может быть удалена случайно, а штатные возможности по ее восстановлению — ограничены. В случае отсутствия резервной копии зачастую единственным способом вернуть утраченное является применение специализированных электронных технологий.

Для кого?

Организациям и частным лицам, столкнувшимся с потерей информации на носителе вследствие неосторожного удаления данных или программного/аппаратного сбоя.

Описание услуги

Методики восстановления данных на машинных носителях варьируются в зависимости от характера и обстоятельств каждого конкретного случая.

Путем работы с запоминающим устройством на низком уровне (физический носитель (микросхемы памяти), микроконтроллер (микросхемы управления), микропрограммное обеспечение), а также с использованием специализированного ПО может быть восстановлен доступ к информации, ставшей недоступной по техническим причинам или в силу «человеческого фактора».

Для реализации различных сценариев восстановления данных используется самое современное оборудование и передовое программное обеспечение, а также знания и многолетний опыт экспертов.

Результат и его бизнес-ценность

Результат оказания услуги — полностью или частично восстановленная информация либо квалифицированное заключение о том, что восстановление данных на предоставленном носителе не представляется возможным.

ДОПОЛНИТЕЛЬНО

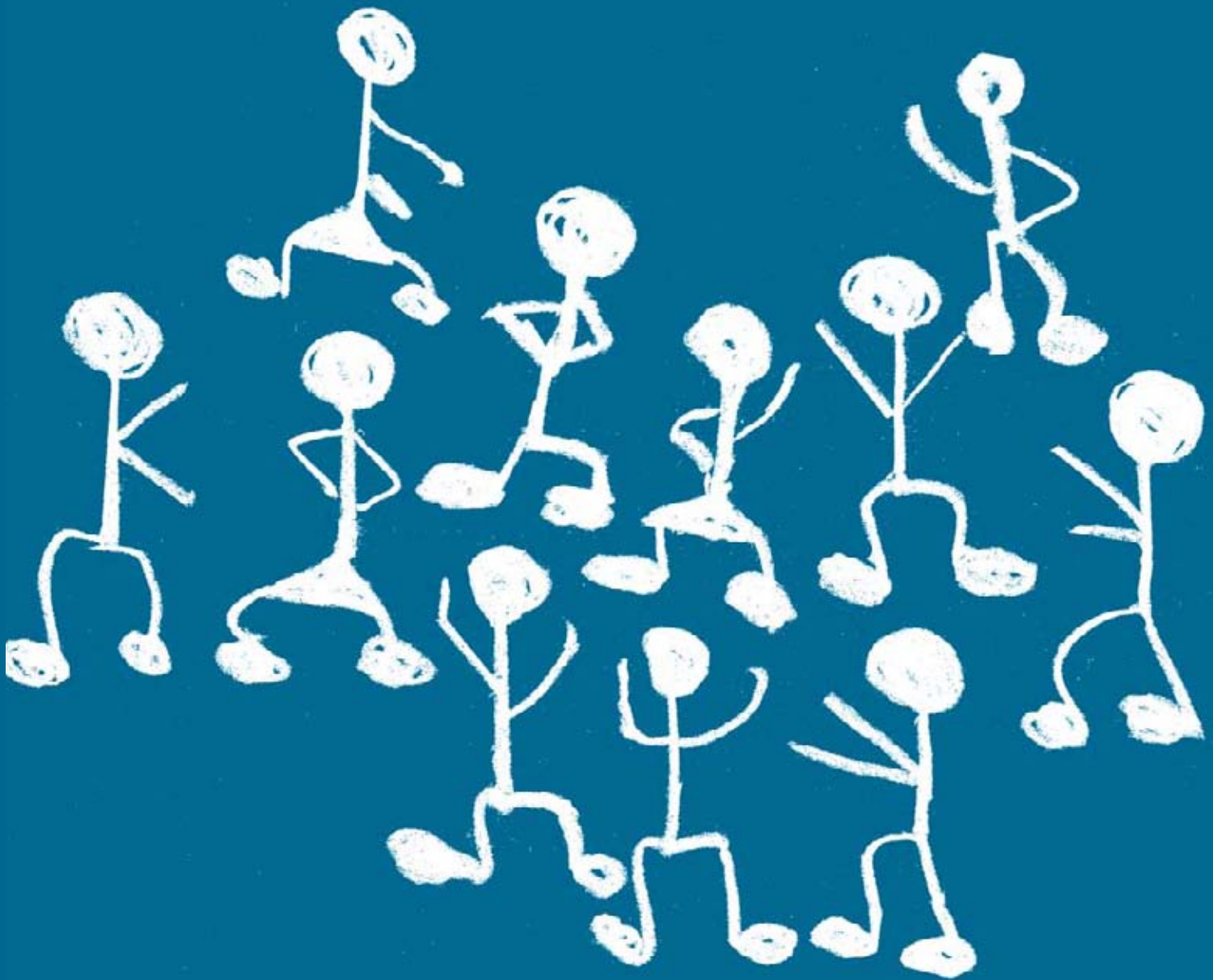
Работы по восстановлению данных выполняются для следующих типов носителей информации:

- НЖМД с различными интерфейсами доступа
- Твердотельные накопители:
- USB-Flash
- Compact Flash
- Memory Stick
- Secure Digital (SD) card
- miniSD card
- microSD card
- SSD

СВЯЗАННЫЕ УСЛУГИ

- Расследование инцидентов информационной безопасности
- Резервное копирование и восстановление

Политика работы в социальных сетях



Для чего?

Широкое распространение социальных сетей — объективная реальность современного мира. Все без исключения компании сталкиваются с использованием социальных сетей своими работниками. Зачастую присутствие в социальной сети менеджеров, специалистов или обобщенного пресс-персонажа является частью бизнес-деятельности компании.

Наличие таких инфокоммуникационных сервисов, как социальные сети, приводит к необходимости четкого определения политики их использования в корпоративной среде.

Для кого?

Компаниям с большой численностью персонала. Организациям, работники которых имеют точки присутствия в социальных сетях.

Описание услуги

В ходе оказания услуги проводится общий анализ практики использования ресурсов социальных сетей работниками компании (в т.ч. при исполнении ими своих служебных обязанностей — маркетинг, работа со СМИ, PR, реклама). С учетом полученных сведений разрабатывается Политика работы в социальных сетях — документ, определяющий взгляды руководства компании на использование ресурсов и возможностей Social Networking Service (SNS). В частности, Политика определяет: цели и задачи, особенности SNS как инфокоммуникационного сервиса, риски использования SNS для личности, риски использования SNS для компании, условия, при которых доступ в SNS возможен в рабочее время, ограничения по использованию SNS, рекомендации по безопасному взаимодействию с SNS, корпоративные учетные записи в SNS и порядок их использования, а также другие вопросы в зависимости от специфики деятельности компании.

Результат и его бизнес-ценность

Результат оказания услуги — документированные принципы цивилизованного использования социальных сетей работниками компании (организации). Наличие Политики дает понять персоналу, что данная сфера находится в фокусе внимания руководства. Тем самым повышается дисциплинированность работников, обеспечивается целевое использование ИТ в их повседневной деятельности, а также снижаются риски формирования негативного информационного фона, ассоциируемого с организацией при неадекватном поведении ее сотрудников в социальной сети. Одновременно снижаются риски реализации традиционных угроз ИБ (вирусы, фишинг), распространяющихся по каналам SNS.

ДОПОЛНИТЕЛЬНО

Положения Политики работы в социальных сетях увязываются с ОРД компании в области ИБ и с документами, определяющими миссию, принципы деятельности, политику обеспечения качества, политику HRM.

СВЯЗАННЫЕ УСЛУГИ

- Стратегии и политики информационной безопасности
- Документация по обеспечению информационной безопасности

Курсы, тренинги и обучающие семинары

Для чего?

Потребность в услугах интегратора по проведению обучающих семинаров, курсов и тренингов возникает, как правило, в следующих ситуациях:

- В компании реализуется крупный проект по созданию СОИБ
- В компании реализуется крупный проект по созданию СЗПДн
- В организации банковской системы реализуется крупный проект по приведению в соответствие СТО БР ИББС
- Осуществляется поставка новых сложных систем и средств защиты
- CIO/CISO стремится донести до топ-менеджмента важность проблем обеспечения ИБ (в целях обоснования бюджета, внутреннего PR, с информационной целью)
- ИТ/ИБ-департамент стремится довести до персонала правила и порядок безопасной работы с ИТ
- Необходимо повысить уровень осведомленности в вопросах ИБ специалистов из филиалов
- Необходимо быстро получить необходимую информацию и/или навыки администрирования сложного оборудования и ПО «из рук» специалистов-практиков

Для кого?

Широкому кругу заказчиков в коммерческом и государственном секторе.

Описание услуги

Занятия и семинары проводятся с группами различного размера по имеющимся или индивидуально разрабатываемым программам. Время и режим проведения занятий могут варьироваться в широких пределах.

Обучающие мероприятия проводятся как на базе НТЦ «Вулкан» и его партнеров, так и на территории заказчика.

Слушатели получают необходимый раздаточный материал на русском языке. Практические занятия проводятся на оборудовании компании.

К проведению занятий привлекаются ведущие специалисты компании с широким опытом работы в области информационной безопасности. При необходимости в тренингах участвуют представители компаний-вендоров.

Результат и его бизнес-ценность

После прохождения курсов, тренингов или обучающих семинаров, проводимых специалистами НТЦ «Вулкан», заказчики получают:

- вооруженных новыми знаниями сотрудников ИТ/ИБ-подразделений
- персонал, понимающий суть и основы процессов обеспечения ИБ, а также свои задачи и действия в этом процессе

Обучение, проведенное «Вулканом», позволит быстро и удобно расширить компетенции специалистов либо экономичным способом существенно поднять степень осведомленности основного контингента работников компании.

ДОПОЛНИТЕЛЬНО

Актуальный перечень доступных тем размещен на интернет-сайте НТЦ «Вулкан»

СВЯЗАННЫЕ УСЛУГИ

- Комплексные системы обеспечения информационной безопасности
- Услуги из блока «Соответствие требованиям»

Научно-технический центр «Вулкан» — это команда профессионалов в области современных информационных технологий и обеспечения информационной безопасности, готовых разделить свой опыт и компетенцию с бизнесом, правительственными организациями, общественными институтами.

Миссия НТЦ «Вулкан» — находить эффективные, прагматичные и красивые решения сложных задач.

Компания располагает всеми необходимыми лицензиями федеральных органов исполнительной власти.

Клиенты НТЦ «Вулкан» как в государственном, так и в коммерческом секторе вправе рассчитывать на грамотное понимание нами управленческих целей, их эффективное достижение путем качественного и своевременного решения поставленных задач, а также на получение результата, гармонично вписывающегося в их бизнес и технологии.

Эффективное решение масштабных задач в ИТ и ИБ — главный приоритет НТЦ «Вулкан». Деятельность компании построена как на соответствии стандартам и нормативам, так и на опыте лучших практик, что дает максимальный эффект при реализации проектов. Рекомендации ведущих экспертных советов, мощь высокотехнологичных продуктов лидеров отрасли, энергия и профессионализм команды НТЦ «Вулкан» воплощаются в комплексных решениях, обеспечивающих достижение целей с наилучшими показателями.

Высокий потенциал коллектива НТЦ «Вулкан» является залогом успеха при выполнении самых разнообразных проектов, включая разработку комплексных технических решений в сфере ИТ и ИБ, выполнение профильных НИОКР, анализ бизнес-процессов, разработку стратегий и планов, оперативное консультирование и сопровождение. К услугам клиентов «Вулкана» — профессиональная команда специалистов с большим опытом работы. Современная технологическая база компании обеспечивает высокое качество технических решений и их соответствие самым строгим требованиям со стороны заказчиков.

105318, г. Москва, ул. Ибрагимова, д.31
тел./факс: +7 (495) 663-95-16
http://ntc-vulkan.ru
info@ntc-vulkan.ru