г.Воронеж, ул.Средне-Московская, 6А
+7 473 239 0121, office@comnet-vrn.ru

ТИПОВОЙ ПЕРЕЧЕНЬ
услуг аудита IT-инфраструктуры, оказываемый специалистами ООО «КОМНЕТ»

Аудит IT-инфраструктуры, как правило, состоит из следующих основных этапов:

1) аудит телекоммуникационной инфраструктуры (далее – ТкИ);
2) аудит информационно-вычислительной инфраструктуры (далее – ИВИ);
3) аудит информационной безопасности;
4) систематизация и документирование результатов аудита.

1.1. В ходе аудита ТкИ обеспечивается:

- установление (уточнение) перечня, мест дислокации оборудования ТкИ (в т.ч. средств управления), моделей и функционального назначения с документированием в технические паспорта ТкИ;
- визуальное обследование, фотографирование, оценку физического состояния и условий эксплуатации оборудования ТкИ, установление режима работы оборудования ТкИ, способов его электропитания и управления с документированием полученных сведений в таблицы операционного состояния ТкИ;
- выявление выключенного и/или неработоспособного (с явными признаками неработоспособности или нештатного функционирования) оборудования ТкИ с документированием в таблицы операционного состояния ТкИ;
- систематизация имеющейся эксплуатационной и заводской документации на оборудование ТкИ, а также системы/подсистемы и сети в составе ТкИ в ведомости эксплуатационных документов ТкИ;
- сбор сведений об аппаратных характеристиках и системном программном обеспечении оборудования ТкИ, с документированием в технических паспортах ТкИ;
- сбор в электронные архивы и систематизацию актуальной конфигурационной и операционной информации для оборудования ТкИ;
- проверка работоспособности оборудования ТкИ в целом и его сетевых интерфейсов с документированием результатов в таблицы операционного состояния ТкИ;
- идентификация статуса (up/down), назначения сетевых интерфейсов оборудования ТкИ с документированием (по параметрам физического, канального и сетевого уровня) в таблицы конфигурации сети;
- установление границ, зонирование (сегментирование) ТкИ и документирование топологии сетей в схемы сетей (по сегментам, на канальном и сетевом уровнях), таблицы коммутации и таблицы граничных подключений абонентского оборудования и оборудования ИВИ;
- идентификация и классификация сетевого трафика, определение и документирование источников и маршрутов классифицированного трафика в таблицы-классификаторы информационных потоков и сетевые маршрутные схемы;

- измерение статистических показателей производительности оборудования ТкИ в целом, а также фактической загрузки (включая статистику по наличию и количеству ошибок) сетевых интерфейсов (по протоколам и портам классифицированного трафика) с документированием результатов в таблицы операционного состояния ТкИ;
- анализ структуры, конфигурации и операционного состояния ТкИ по следующим показателям:
  - степень соответствия решаемым задачам;
  - условия и режимы эксплуатации программно-технических средств, устойчивость к перебоям в электроснабжении;
  - запас на расширяемость (без существенной модернизации) и возможность масштабирования;
  - степень унификации компонент ТкИ;
  - наличие и количество точек единого отказа (отказ по которым приводит к невозможности предоставления сетевого сервиса всем или большинству пользователей);
  - наличие и количество «узких мест» (в части производительности, критической (предкритической) загрузки элементов ТкИ, наличию ошибок, частоты их появления и степени влияния на ТкИ);
  - оптимальность маршрутизации (в т.ч. количество/обоснованность наличия промежуточных узлов, наличие/устойчивость к образованию петель, устойчивость к авариям на каналах связи);
  - наличие и оптимальность профилирования трафика, достаточность/избыточность сетевых протоколов и служб;
  - наличию устаревшего и снятого с поддержки (End-To-Life/Sale/Service-Support) оборудования ТкИ;
  - управляемость и контроль функционирования.
- выяснение и анализ технических возможностей (условий) региональных операторов связи для повышения надежности, оптимизации эксплуатации и модернизации ТкИ;
- определение (с обоснованием) фрагментарных ресурсов ТкИ для переноса в ЦОД ГАУ АО «Управление ИКТ АО»;
- выяснение и анализ технических возможностей (условий) ЦОД ГАУ АО «Управление ИКТ АО» для переноса в него определенных фрагментарных ресурсов ТкИ;
- разработка рекомендаций по итогам аудита ТкИ.

1.2. В ходе аудита ИВИ обеспечивается:

- установление (уточнение) перечня, мест дислокации подключенного к ТкИ физического оборудования ИВИ (серверов, систем хранения данных, АРМ и периферийного оборудования), его ведомственной принадлежности, моделей и функционального назначения с документированием в технические паспорта ИВИ;
- визуальное обследование, фотографирование, оценку физического состояния и условий эксплуатации физического оборудования серверов и систем хранения данных, установление режима работы (круглосуточный/иной) оборудования, способов его электропитания и управления с документированием полученных сведений в таблицы операционного состояния ИВИ;
- обследование инженерных систем серверных помещений (температурно-влажностный режим, системы основного и аварийного освещения, вентиляции и кондиционирования, защиты от статического электричества и т.п.) на наличие и соответствие

стандартам и требованиям производителей оборудования с документированием в таблицы операционного состояния ИВИ;

- выявление выключенного и/или неработоспособного (с явными признаками неработоспособности или нештатного функционирования) физического оборудования серверов и систем хранения данных с документированием в таблицы операционного состояния ИВИ;

- сбор сведений об аппаратных характеристиках и системном программном обеспечении (операционная система, система управления базой данных, программное обеспечение виртуализации) оборудования ИВИ, с документированием в технических паспортах ИВИ;

- сбор сведений о параметрах виртуальных объектов вычислительной инфраструктуры, развернутых на физическом оборудовании, с документированием в технических паспортах ИВИ;

- сбор и систематизация сведений об информационных системах и подсистемах, развернутых в ИВИ, составление реестра информационных систем ИВИ;

- систематизация имеющейся эксплуатационной и заводской документации на оборудование ИВИ и информационные системы/подсистемы в ведомости эксплуатационных документов ИВИ;

- сопоставление физических/виртуальных объектов ИВИ информационным системам/подсистемам, выделение и типизация АРМ (пользователей, управления и т.п.), сопряжение типизированных объектов ИВИ со схемами топологии сетей и маршрутными схемами, сформированными на этапе аудита ТкИ, составление гибридных структурно-топологических схем организации информационно-вычислительной и телекоммуникационной инфраструктур;

- инвентаризация установленного на физических/виртуальных серверах, хранилищах данных и типовых АРМах программного обеспечения с последующей систематизацией, категоризацией (общее/специальное/иное) и типизацией установленного программного обеспечения и документированием в паспорта типового общего и типового специального программного обеспечения ИВИ, а также в таблицы некатегоризированного программного обеспечения;

- сбор в электронные архивы и систематизацию актуальной информации журналов операционных систем и иной операционной информации на физических/виртуальных серверах, хранилищах данных и основных типовых АРМ;

- измерение (расчет) статистических показателей по производительности, фактической загрузке процессоров, оперативной памяти, накопителей на жестких дисках для физических/виртуальных серверов, хранилищ данных и основных типовых АРМ с документированием результатов в таблицы операционного состояния ИВИ;

- расчет статистических показателей по наличию, частоте появления и категориям критических/предкритических ошибок из журналов операционных систем для физических/виртуальных серверов, хранилищ данных и основных типовых АРМ с документированием результатов в таблицы операционного состояния ИВИ;

- анализ структуры, конфигурации и операционного состояния ИВИ по следующим показателям:
    - степень соответствия решаемым задачам;
    - условия и режимы эксплуатации, устойчивость к перебоям в электроснабжении;
    - запас на расширяемость (без существенной модернизации) и возможность масштабирования;
    - степень унификации компонент ИВИ;
    - наличие и количество точек единого отказа (отказ по которым приводит к невозможности предоставления прикладного сервиса всем или большинству пользователей);
    - наличие и количество «узких мест» (в части производительности, критической/предкритической загрузки элементов ИВИ, наличию ошибок, частоты их появления и степени влияния на ИВИ);
    - оптимальность организации уровней хранения данных и настроек (конфигураций, политик) доступа к данным и их резервного копирования;
    - наличие технических средств и программного обеспечения, содержащих признаки несвязанности с исполнением служебных обязанностей пользователя и/или лицензионной контрафактности;
    - управляемость и контроль функционирования.
- определение (с обоснованием) фрагментарных ресурсов ИВИ для переноса и/или виртуализации в ЦОД ГАУ АО «Управление ИКТ АО»;
- выяснение и анализ технических возможностей (условий) ЦОД ГАУ АО «Управление ИКТ АО» для переноса в него (и/или виртуализации) определенных фрагментарных ресурсов ИВИ;
- разработка рекомендаций по итогам аудита ИВИ.

1.3. В ходе аудита информационной безопасности обеспечивается:

- идентификация информационных систем, информационных систем персональных данных (с использованием результатов аудита ИВИ) с документированием в таблицу объектов информатизации;
- выявление защищаемых помещений с документированием в таблицу объектов информатизации, визуальное обследование, составление планов защищаемых помещений с указанием границ контролируемой зоны;
- составление (с использованием результатов аудита) общего описания элементов ТкИ и ИВИ, эксплуатируемых в составе объектов информатизации;
- идентификация (с использованием результатов аудита) и категоризацию (межсетевые экраны, средства защиты от несанкционированного доступа, обнаружения вторжений, криптозащиты, электронной цифровой подписи и т.п.) программно-технических средств защиты информации (далее – СЗИ) с документированием в таблицы СЗИ, составление структурных схем подключения СЗИ;
- сбор и систематизацию сведений об имеющихся организационно-распорядительных документах в области защиты информации в ведомости документов по защите информации;
- определение типовых зон ответственности и ролей персонала по обеспечению информационной безопасности и требуемым правам доступа к элементам ТкИ и ИВИ с документированием (проверкой документирования) в списки (матрицы) доступа;

г.Воронеж, ул.Средне-Московская, 6А
+7 473 239 0121, office@comnet-vrn.ru

- сбор сведений об учетных записях и правах пользователей, зарегистрированных в операционных системах физических/виртуальных серверов, хранилищ данных и основных типовых АРМ с документированием результатов в таблицы учетных записей;
- сбор сведений об уязвимостях системного программного обеспечения физических/виртуальных серверов, хранилищ данных и основных типовых АРМ с документированием результатов в таблицы уязвимостей;
- комплексный анализ угроз безопасности информации (в разрезе информационных систем или защищаемых помещений), в т.ч.:
  - моделирование типов, потенциала, видов возможных нарушителей и их целей (мотиваций) для реализации угроз безопасности информации;
  - систематизация и обобщение выявленных уязвимостей программного обеспечения;
  - классификация объектов воздействия угроз несанкционированного доступа (с анализом текущей защищенности);
  - классификация возможных последствий от деструктивных действий, связанных с несанкционированным доступом (с анализом текущей защищенности);
  - классификация носителей персональных данных (с анализом текущей защищенности);
  - классификация технических каналов утечки информации (с анализом текущей защищенности);
  - классификация и описание угроз утечки по техническим каналам (с оценкой вероятности реализации угроз);
  - классификация и описание угроз несанкционированного доступа к информации (с анализом источников угроз, объектов воздействия и возможных деструктивных действий);
  - оценка уровней исходной защищенности объектов информатизации;
  - классификация и описание актуальных угроз безопасности информации объектов информатизации (с оценкой вероятности, возможности реализации угрозы, уровня опасности угрозы и возможных негативных последствий);
- классификация информационных систем (по требованиям безопасности информации) с документированием в проекты актов классификации;
- разработка рекомендаций по итогам аудита информационной безопасности.