# Отчет об аудите IT инфраструктуры

## Цели обследования

1. Определение сетевой топологии, анализ конфигурации сетевого оборудования;
2. Анализ аппаратного, программного обеспечения на серверах, анализ их функционала;
3. Выявление проблем в конфигурации сетевого и серверного оборудования;
4. Анализ состава компонентов информационных систем;
5. Предложение рекомендаций по снижению рисков информационной безопасности и надежности.

## Проведенные мероприятия

1 Анализ топологии компьютерной сети;

2 Внешний осмотр серверного и коммутационного оборудования, мест их размещения;

3 Анализ конфигурации серверов;

4 Анализ конфигурации сетевого оборудования;

5 Анализ используемых информационных систем;

6 Анализ системы резервного копирования;

7 Анализ режима хранения информации и прав доступа;

8 Анализ режима парольной защиты;

9 Анализ организационной структуры IT отдела.

# Выявленные проблемы

В целом, состояние ИТ-хозяйства можно считать удовлетворительным.

В ходе аудита были выявлены следующие проблемы:

1. RDP-доступ к большому количеству узлов локальной сети доступен через Интернет без ограничений и может осуществляться без использования VPN. В сочетании со слабыми паролями это может привести к утечке данных, а также заражению вирусами, в т.ч. шифраторами. Даже при условии использования стойких паролей не рекомендуется оставлять открытым доступ к RDP из сети интернет.

2. Помимо RDP доступа, в локальной сети присутствует очень много сервисов, доступных без ограничения через интернет. Среди них и такие, которые крайне не рекомендуется содержать в локальной сети, а следует размещать в DMZ, например, веб сервера: [redacted], [redacted], [redacted] и т. д.

3. Резервное копирование не имеет централизованного управления, не используется специализированное ПО. Для файлового сервера используется резервное копирование с помощью VSS (встроенный в ФС механизм), для баз данных — дампы, для виртуальных машин — просто копирование образов диска. Резервные копии лежат на разных серверах, там, где для них хватает объема дискового пространства. Текущая схема резервного копирования не предоставляет защиты от вируса-шифратора, проникшего в локальную сеть, не позволяет понять, что из резервного копирования функционирует успешно, а что уже давно остановилось по той или иной причине. Используемое ПО не позволяет делать инкрементальные копии, что сильно снижает глубину хранения при том же объеме хранилища РК.

4. Отсутствует резервирование серверов и запасной сервер на случай необходимости замены. При выходе из строя сервера простой будет составлять около 8 рабочих часов, а процесс восстановления непредсказуемым, т. к. отсутствуют запасные сервера и запасные части в достаточном количестве.

5. Отсутствует резервирование основного сетевого оборудования. В случае выхода из строя ключевого сетевого оборудования [redacted] (ядро сети), [redacted] (фаервол), основных коммутаторов простой будет очень длительный, т. к. запасного оборудования на замену с нужными характеристиками на площадке нет. Также на площадке в Финляндии имеется резервирование пограничного маршрутизатора, но запасного коммутатора нет.

6. Политика паролей позволяет установить слабые пароли, а также изменять пароли пользователям самостоятельно. Регулярная смена паролей не производится. При этом сервисы с доменными паролями доступны снаружи, что потенциально позволяет получить доступ ко многим системам в локальной сети простым перебором паролей.

7. Отсутствует система комплексного мониторинга серверной инфраструктуры. Установлена комплексная система мониторинга [redacted], но не настроена. Без грамотной настройки объектов и параметров мониторинга, порогов срабатывания система мониторинга не улучшает надёжности и бесперебойности работы систем.

8. Не настроены уведомления от управляемых ИБП и мониторинг их состояния.

9. Не настроены уведомления о неисправностях RAID массивов.

10. Антивирус установлен не на всех серверах.

11. Имеющийся файрвол не позволяет получать журналы входящих соединений, и статистику трафика и не предоставляет удобных средств для доступа к ресурсам локальной сети по VPN. Трудности с применением VPN приводят тому, что многие ресурсы оказываются открыты через Интернет напрямую.

12. Отсутствуют регламенты на предоставление доступа к ресурсам в локальной сети из сети Интернет, регламенты обращения с паролями, регламенты доступа к конфиденциальной информации.

13. Организационная структура IT отдела такова, что серьезную часть технически сложных работ по серверному и сетевому способен выполнять только один сотрудник ([redacted]), а также только он обладает знанием множества технических нюансов серверной и сетевой инфраструктуры, что приводит к рискам в случае болезни/отпуска/увольнения сотрудника. В наличии имеется документация в хорошем состоянии, но документация не снимает риски полностью.

# Рекомендации

1. Требуется заменить не удовлетворяющий требованиям компании файрвол, что позволит обеспечить должную безопасность периметра. Удобные средства работы с VPN с использованием разных протоколов позволят подключать всех удаленных сотрудников, а также подрядчиков, которым требуется доступ к ресурсам локальной сети. Наличие журнала соединений позволяет предотвращать утечки данных и расследовать инциденты ИБ (сейчас это невозможно см. п. 11 «Проблем»). Наличие внятной статистики также улучшает управляемость сетевой инфраструктуры. Все это поможет снять несколько из озвученных выше проблем.
2. Рекомендуется полностью запретить удаленный доступ по RDP из Интернет без использования VPN. В сочетании со слабыми паролями, доступ без VPN может привести к утечке данных, а также заражению вирусами, в т.ч. вирусами-шифраторами. Даже при условии использования стойких паролей не рекомендуется оставлять открытым доступ к RDP из сети Интернет.
3. Доступ к сервисам, которые расположены в локальной сети и требуются для работы вне офиса сотрудникам и/или контрагентам, должны предоставляться с использованием VPN. Сервисы, ориентированные на неограниченную группу лиц или которые технологически сложно предоставлять с использованием VPN, должны быть вынесены из локальной сети в DMZ (например, при помощи [redacted], [redacted]).
4. Обеспечить централизованное резервное копирование (РК) с использованием отдельных серверов резервного копирования и специализированного ПО, которое позволит
   4.1. контролировать процесс резервного копирования.
   4.2. получить большую глубину резервного копирования за счет применения инкрементального РК.
   4.3. сохранить данные полной потере площадки (например, пожар), в случае организации георазпределённого РК.
   4.4. позволит быстро выполнять заявки по восстановлению данных, в том числе частичному (отдельную папку на виртуальной машине, отдельную таблицу БД, отдельный почтовый ящик и т. д.)
   4.5. позволит защититься от ущерба от вирусов-шифровальщиков.
5. Обеспечить стойкую парольную защиту: ввести требования к минимальной сложности паролей, сменить пароли пользователей, организовать регламенты обращения с паролями. Для размера организации Заказчика допустимо менять пароли нечасто — раз в год.
6. Обеспечить частичное резервирование серверной инфраструктуры на обоих площадках. Серверная инфраструктура состоит из двух площадок, в здании завода [redacted] серверов, из них большинство виртуализированы, в ДЦ [redacted] серверов, из них

большинство виртуализированы. В каждом сервере своя дисковая корзина и любой сбой сервера делает информацию и сервисы, располагаемые на нем, недоступными на долгий срок и приведет к необходимости восстановления из резервной копии (при ее наличии) Требуется виртуализировать все сервера, для которых целесообразно резервирование и обеспечить резервирование с помощью гиперконвергентной инфраструктуры (например, VMWare VSAN), при которой дисковые ресурсы всех серверов объединяются и реплицируются между узлами кластера, что позволяет безболезненно продолжить работу в течении 15 минут без потери данных в случае сбоя любого из серверов.

7. Рекомендуется обеспечить резервирование основного сетевого оборудования (ядро сети и соседние коммутаторы, файрвол). Это позволит быстро восстановить работоспособность локальной сети при сбое какого-то сетевого оборудование. Статичность рабочей информации (файла конфигурации) сетевого оборудования позволяет обойтись просто наличием запасного устройства и резервной копии конфигурации для быстрого продолжения работы.
8. Установить антивирус на сервера, на которые он еще не установлен. Для серверов, сильно нагруженных по дисковой подсистеме (например, сервера БД), рекомендуется обеспечить мониторинг параметров производительности, чтобы обнаружить заметную деградацию производительности, если она будет, и принять меры к исправлению ситуации.
9. Составить пакет внутренних нормативов по работе с Информацией, составляющей коммерческую тайну (ИСКТ):
    9.1. Перечень ИСКТ, сотрудникам под роспись
    9.2. Регламент работы с ИСКТ: где хранить, как передавать, сотрудникам под роспись
    9.3. Перечень ресурсов для хранения ИСКТ, со списками доступа (уже есть)
10. Централизовать внутреннюю документация отдела ИТ: топология сети, список серверного и сетевого оборудования, пароли доступа к ним, список внешних подрядчиков (хостинги, телеком, SaaS и тд.) с паролями доступа и т.д. Использовать Wiki и менеджер паролей
11. Подключить управляемые ИБП к серверам для мониторинга и автоматического выключения при критическом заряде батарей, настроить отправку уведомлений о неполадках по e-mail.
12. Правильно сконфигурировать и настроить установленную ранее систему централизованного мониторинга серверов [redacted]: добавить недостающие объекты, настроить нужные параметры мониторинга, правильно настроить пороги срабатывания уведомлений, настроить уведомление по смс о критических сбоях. Расположить в серверной датчик температуры и подключить к системе мониторинга.
13. Разработать и внедрить регламенты, влияющие на ключевые компоненты

информационной безопасности: доступ к сети снаружи, пароли, доступ к конфиденциальной информации.

14. Разработать и внедрить регламенты на обновление серверного ПО, критичного к наличию установленных свежих обновлений, например, [redacted], [redacted], [redacted], [redacted].

15. Рассмотреть возможность добавления еще одного старшего системного администратора (как в штате, так и в виде аутсорсинга) для совместной с [redacted] поддержки и развития серверной и сетевой инфраструктуры.

16. Провести дополнительное обследование потенциальных динамических проблем:

    16.1. Проверить переключение каналов интернет: план действий на случай отказа одного из каналов интернет.

    16.2. Проверить возможность незаметного подключения к сети, оценить риски такого подключения.

    16.3. Проверить режим обмена платежными поручениями между 1С и БК, оценить риски ИБ.

    16.4. Проверить обновления ПО.

    16.5. Проверить все сервера на зараженность вредоносным ПО.

    16.6. Проверить лицензионную чистоту ПО.