Руководство по ключевым мерам цифровой безопасности IT-инфраструктуры автовокзала, автоматизированного при помощи системы «Авибус: Управление автовокзалами»

Введение

В современной цифровой экономике информационные системы являются основой функционирования любого предприятия. Система Авибус базируется на платформе 1С:Предприятие и концентрирует в себе наиболее критичные бизнес-данные: персональные данные пассажиров, продажи на рейсы и в разрезе подразделений/по кассирам, взаиморасчеты с перевозчиками, финансовую отчетность, коммерческую информацию. Эта концентрация делает систему мишенью для кибератак.

Угрозы варьируются от широкомасштабных кампаний по распространению программ-шифровальщиков, способных парализовать деятельность компании на недели, до целенаправленных атак с целью промышленного шпионажа и кражи данных, а также внутренних угроз, исходящих от недобросовестных или неосторожных сотрудников. Последствия успешной атаки на систему 1С могут быть катастрофическими, включая прямые финансовые потери, репутационный ущерб, нарушение законодательных требований (например, о защите персональных данных) и полную остановку операционной деятельности.

Сфокусируемся на жизненно важных мерах, которые дают максимальный эффект и формируют прочный фундамент безопасности для любой инфраструктуры 1С:Предприятие.

Настоящий документ представляет собой исчерпывающее техническое руководство для системных администраторов, IT-специалистов и инженеров по безопасности, ответственных за защиту систем на платформе 1С:Предприятие. В нем последовательно рассматриваются три ключевых эшелона обороны. Сначала мы заложим фундамент, рассмотрев незыблемые принципы безопасности, такие как отказоустойчивое резервное копирование, управление привилегиями и гигиена обновлений. Затем мы перейдем к защите сетевого периметра, предоставив детальные инструкции по настройке межсетевых экранов и безопасной публикации веб-сервисов. Наконец, мы рассмотрим меры по укреплению непосредственно серверов и рабочих станций, включая оптимальную настройку антивирусного ПО и контроль использования периферийных устройств.

Раздел 1. Фундамент Безопасности: Незыблемые Принципы

Этот раздел посвящен основополагающим стратегиям, которые являются обязательными для любой безопасной инсталляции 1С.

1.1. Резервное Копирование: Стратегия «3-2-1» как Последний Рубеж Обороны

В контексте современных угроз резервное копирование перестало быть просто инструментом для восстановления после сбоя оборудования.

Золотым стандартом в индустрии для обеспечения отказоустойчивости данных является правило «3-2-1».[2] Оно гласит, что для критически важных данных необходимо:

- Иметь как минимум **три** копии данных (одна рабочая и две резервных).
- Хранить эти копии на **двух** разных типах носителей (например, на дисковом массиве сервера и на ленточном накопителе или внешнем диске).
- Хранить **одну** из копий за пределами основной площадки (off-site), в географически удаленном месте.

Применение этого правила к среде 1С напрямую зависит от режима работы.

Практическая реализация:

- **Файловый режим:** Резервное копирование сводится к копированию файла базы данных (.1CD) и, при необходимости, каталогов с внешними компонентами или отчетами. Для автоматизации можно использовать встроенные средства операционной системы, такие как «Система архивации данных Windows Server», или утилиты командной строки, например, robocopy в Windows или rsync в Linux, обернутые в скрипты и запускаемые по расписанию.
- **Клиент-серверный режим:** Процесс более сложен и надежен. Резервное копирование должно выполняться средствами системы управления базами данных (СУБД), на которой работает 1С (например, MS SQL Server или PostgreSQL). Это гарантирует консистентность данных на момент создания копии. Следует настроить регулярное создание полных бэкапов (например, раз в неделю) и дифференциальных или инкрементальных бэкапов (например, ежедневно), а также бэкапов логов транзакций (для модели восстановления Full в MS SQL) для возможности восстановления на

определенный момент времени.

- Подробно процесс создания резервного копирования средствами MS SQL описан в документации.
- Организация бэкапа средствами PostgreSQL подробно описана на ресурсах PostgresPro , PostgreSQL и на Habr

Ключевым аспектом стратегии «3-2-1» в борьбе с программами-шифровальщиками является природа «удаленной» или «изолированной» копии. Современные зловреды целенаправленно ищут и шифруют не только рабочие данные, но и доступные по сети резервные копии.[1] Если ваш бэкап-сервер постоянно подключен к основной сети и доступен с сервера 1С, он с высокой вероятностью будет атакован вместе с основной системой.

Следовательно, третья копия должна быть по-настоящему изолированной. Этого можно достичь несколькими способами:

1. **Физическая изоляция (Air Gap):** Использование сменных носителей, таких как внешние жесткие диски или ленточные картриджи, которые физически отключаются от системы после завершения копирования.
2. **Логическая изоляция:** Репликация резервных копий в облачное хранилище, поддерживающее технологии WORM (Write Once, Read Many), такие как Блокировка версии объекта (object lock) в Яндекс облаке. Эти технологии на уровне провайдера запрещают изменение или удаление объектов, делая их неуязвимыми для шифровальщиков.
3. **Использование специализированных бэкап-систем:** Некоторые современные решения для резервного копирования создают изолированную среду для хранения копий и имеют встроенные механизмы для обнаружения аномальной активности, похожей на шифрование.

Таким образом, недостаточно просто иметь три копии. Качество, а главное, изоляция третьей копии — это решающий фактор, который определяет, сможет ли компания восстановиться после серьезной кибератаки без потерь и уплаты выкупа. Регулярное тестирование процедуры восстановления из всех типов резервных копий является обязательным элементом этой стратегии.

1.2. Принцип Наименьших Привилегий: Управление Доступом в 1С и ОС

Принцип наименьших привилегий (Principle of Least Privilege, PoLP) — это фундаментальная концепция кибербезопасности, согласно которой любой пользователь, программа или процесс должны обладать только минимальным набором полномочий, необходимым для выполнения своих задач. Внедрение этого принципа в инфраструктуре 1С резко снижает потенциальный ущерб от скомпрометированных учетных записей и усложняет для злоумышленника продвижение по сети (lateral movement).

Реализация этого принципа должна охватывать все уровни системы:

- **Уровень приложения 1С:** Платформа 1С:Предприятие предоставляет мощный механизм ролей и профилей доступа. Категорически запрещается предоставлять обычным пользователям (бухгалтерам, менеджерам, кладовщикам) предопределенный профиль «Полные права». Вместо этого необходимо создавать кастомные профили, включающие только те роли, которые соответствуют должностным обязанностям сотрудника.
- **Уровень операционной системы:** Ни один пользователь 1С не нуждается в правах локального администратора на своей рабочей станции для выполнения повседневных задач. Предоставление таких прав — одна из самых распространенных и опасных ошибок. Если рабочая станция такого пользователя будет скомпрометирована (например, через фишинговое письмо), вредоносное ПО немедленно получит полный контроль над системой, сможет отключать антивирус, устанавливать кейлоггеры и извлекать из памяти другие учетные данные. Аналогично, серверные компоненты 1С (агент сервера, рабочие процессы) должны запускаться от имени специально созданной низкопривилегированной учетной записи службы (service account), а не от имени системных учетных записей SYSTEM (в Windows) или root (в Linux).
- **Уровень системы управления базами данных (СУБД):** В клиент-серверном режиме подключение от сервера 1С к серверу СУБД также должно осуществляться с минимальными правами. Учетной записи, используемой сервером 1С для доступа к базе данных, достаточно иметь права на чтение и запись данных (например, роли db_datareader и db_datawriter в MS SQL) в рамках конкретной информационной базы. Предоставление этой учетной записи прав системного администратора СУБД (sysadmin) или владельца базы данных (db_owner) создает огромную и неоправданную угрозу. В случае компрометации сервера 1С злоумышленник сможет получить полный

контроль над всеми базами данных на сервере СУБД.

- **Сложность паролей и регламенты смены в ОС и в системе Авибус:** Чтобы пароль был надежным, он должен быть сложным и уникальным. Современные требования к сложности паролей включают:
    - Минимальную длину (обычно 8–12 символов);
    - Использование комбинации разных типов символов:
        - Заглавные буквы (A, B, C);
        - Строчные буквы (a, b, c);
        - Цифры (1, 2, 3);
        - Специальные символы (!, @, #, $);
    - Отсутствие легко угадываемых данных, таких как имена, даты рождения и пр.

  Необходимо соблюдать регламенты по смене паролей, они направлены на снижение риска компрометации учетных записей.

    - Регулярная смена: Сотрудникам может быть предписано менять пароли каждые 90 дней. Однако, многие современные подходы рекомендуют не принуждать к частой смене, а фокусироваться на силе пароля и использовании многофакторной аутентификации (МФА);
    - Запрет на повторное использование: Система не должна позволять пользователю использовать один и тот же пароль или его вариации (например, password123, password124);
    - История паролей: Система должна хранить историю паролей, чтобы предотвратить их повторное использование.

  Ключевой аспект информационной безопасности — немедленное прекращение доступа сотрудника к системе после его увольнения. Это необходимо для предотвращения несанкционированного доступа к конфиденциальным данным, саботажа или кражи информации.

1.3. Управление Обновлениями: Гигиена Платформы, ОС и СУБД

Инфраструктура 1С представляет собой сложный технологический стек, и для обеспечения ее безопасности требуется целостный, а не фрагментарный подход к обновлениям.

- **Платформа 1С:Предприятие:** Фирма «1С» регулярно выпускает новые

релизы платформы и конфигураций, в которых не только добавляется новый функционал, но и исправляются обнаруженные уязвимости. Необходимо поддерживать технологическую платформу и типовые конфигурации в актуальном состоянии, следуя рекомендациям вендора.

- **Операционная система:** Как серверы, так и рабочие станции должны своевременно получать обновления безопасности для операционной системы. В корпоративных средах Windows для этого следует использовать службу Windows Server Update Services (WSUS), которая позволяет централизованно управлять процессом обновлений, тестировать их перед развертыванием и контролировать установку. В средах Linux необходимо настроить регулярное обновление пакетов с помощью встроенных менеджеров, таких как apt (для Debian/Ubuntu) или yum/dnf (для CentOS/RHEL).
- **Система управления базами данных и веб-сервер:** СУБД (MS SQL, PostgreSQL) и веб-серверы (IIS, Apache), используемые для публикации веб-клиентов и сервисов, также являются критически важными компонентами.

Экосистему 1С следует рассматривать как единую цепь, прочность которой определяется прочностью самого слабого звена. Уязвимость в любом из компонентов — ОС, СУБД, веб-сервер, сама платформа 1С — может привести к компрометации всей системы. Поэтому политика управления обновлениями должна быть холистической и охватывать все без исключения компоненты технологического стека. Необходимо внедрить регулярный процесс сканирования на уязвимости и применять исправления в соответствии с их критичностью, предварительно тестируя их на нерабочей копии системы для предотвращения сбоев.

Раздел 2. Защита Сетевого Периметра

После того как заложен фундаментальный уровень безопасности, следующим шагом является минимизация поверхности атаки — сокращение всех возможных точек входа для злоумышленника. Наиболее эффективный способ сделать это — жестко контролировать сетевой трафик с помощью межсетевых экранов.

2.1. Архитектура и Сетевые Порты Сервера 1С:Предприятие

Прежде чем настраивать правила фильтрации, необходимо четко понимать, как компоненты сервера 1С:Предприятие взаимодействуют друг с другом и с клиентами по сети. В клиент-серверном варианте развертывания участвуют несколько ключевых процессов:

- ragent.exe (Агент сервера): Это главный управляющий процесс кластера. Он прослушивает один статический порт (по умолчанию 1540) и отвечает за прием запросов на создание новых соединений от менеджеров кластера.
- rmngr.exe (Менеджер кластера): Отвечает за управление сеансами, распределение нагрузки между рабочими процессами и обработку запросов от клиентов. Он также использует статический порт (по умолчанию 1541). Это основной порт, к которому подключаются клиенты 1С.
- rphost.exe (Рабочий процесс): Непосредственно выполняет код 1С и обрабатывает запросы пользователей. Каждому сеансу или группе сеансов выделяется рабочий процесс. Эти процессы используют динамический диапазон портов для взаимодействия с менеджером кластера и клиентами. По умолчанию это диапазон с 1560 по 1591.

Помимо основных компонентов, могут использоваться и другие службы, каждая со своими сетевыми портами :

- **Сервис удаленного администрирования (RAS):** Позволяет управлять кластером серверов удаленно.
- **Сервер хранилища конфигураций:** Используется для командной разработки и версионирования конфигураций.

На основе официальной документации и практического опыта можно составить следующую сводную таблицу используемых портов, которая станет основой для настройки межсетевого экрана.

Таблица 1: Стандартные порты компонентов сервера 1С:Предприятие

Компонент	Процесс	Порт(ы) по умолчанию	Протокол	Назначение
Агент сервера	ragent.exe	1540	TCP	Управление

				кластером, прием запросов от менеджеров
Менеджер кластера	rmngr.exe	1541	TCP	Основной порт для подключения клиентов
Рабочие процессы	rphost.exe	1560-1591	TCP	Динамический диапазон для сеансов клиентов
Сервис администрирования (RAS)	ras.exe	1545	TCP	Удаленное администрирование кластера
Сервер хранилища	crserver.exe	Зависит от версии	TCP	Хранилище конфигураций для разработки

Эта таблица является критически важным справочным материалом. Она консолидирует разрозненную информацию в единый, готовый к использованию формат и позволяет избежать ошибок при конфигурации правил безопасности.

2.2. Настройка Межсетевого Экрана: Практическое Руководство

Основной принцип сетевой безопасности — «запрещено все, что не разрешено явно» (deny by default). Межсетевой экран (файрвол), настроенный по этому принципу, должен блокировать весь входящий трафик, за исключением соединений на строго определенные порты, необходимые для работы легитимных служб. Настройка файрвола должна производиться непосредственно на сервере 1С (host-based firewall).

Для крупных организаций с высокими требованиями к безопасности, специализированные брандмауэры (отдельные устройства: роутер, сетевой брандмауэр) предлагают более надёжные и гибкие возможности.

Для небольших офисов роутера вполне достаточно. Крупным компаниям, обрабатывающим конфиденциальные данные, лучше инвестировать в специализированный брандмауэр, который обеспечивает многоуровневую защиту.

Реализация для Windows Server:

В операционных системах Windows Server рекомендуется использовать встроенный «Брандмауэр Защитника Windows в режиме повышенной безопасности».

1. Откройте оснастку wf.msc.
2. В свойствах брандмауэра для всех профилей (Доменный, Частный, Общий) установите для входящих соединений значение «Блокировать (по умолчанию)».
3. Перейдите в раздел «Правила для входящих подключений» и создайте новые правила:
    - **Правило для Агента сервера:**
        - Тип правила: Для порта.
        - Протокол: TCP.
        - Определенные локальные порты: 1540.
        - Действие: Разрешить подключение.
        - Профили: Все.
        - Имя: 1C Server Agent (TCP 1540).
    - **Правило для Менеджера кластера:**
        - Тип правила: Для порта.
        - Протокол: TCP.
        - Определенные локальные порты: 1541.
        - Действие: Разрешить подключение.
        - Профили: Все.
        - Имя: 1C Cluster Manager (TCP 1541).
    - **Правило для Рабочих процессов:**
        - Тип правила: Для порта.
        - Протокол: TCP.
        - Определенные локальные порты: 1560-1591.

- Действие: Разрешить подключение.
- Профили: Все.
- Имя: 1C Worker Processes (TCP 1560-1591).

Реализация для Linux (UFW - Uncomplicated Firewall для Ubuntu/Debian):

UFW — это простой и удобный интерфейс для управления iptables.[5]

1. **Проверка статуса и установка политик по умолчанию:**
   Bash
   ```
   sudo ufw status
   # Устанавливаем политику "запрещать все входящие" и "разрешать все исходящие"
   sudo ufw default deny incoming
   sudo ufw default allow outgoing
   ```

2. Создание разрешающих правил для 1С:
   Используя синтаксис для диапазонов портов 6, добавьте необходимые правила:
   Bash
   ```
   # Разрешаем SSH, чтобы не потерять доступ к серверу
   sudo ufw allow ssh
   # Разрешаем порты 1С
   sudo ufw allow 1540/tcp
   sudo ufw allow 1541/tcp
   sudo ufw allow 1560:1591/tcp
   ```

3. **Активация файрвола:**
   Bash
   ```
   sudo ufw enable
   ```

Реализация для Linux (Firewalld для CentOS/RHEL):

Firewalld использует концепцию зон для управления правилами.[8]

1. Добавление портов в нужную зону (например, internal или work):
   Предполагается, что серверы и рабочие станции находятся в доверенной зоне internal.
   Bash
   ```
   # Добавляем порты и делаем правила постоянными
   sudo firewall-cmd --zone=internal --add-port=1540/tcp --permanent
   ```

```
sudo firewall-cmd --zone=internal --add-port=1541/tcp --permanent
sudo firewall-cmd --zone=internal --add-port=1560-1591/tcp --permanent
```

2. **Применение изменений:**
   Bash
   ```
   sudo firewall-cmd --reload
   ```

Важно понимать, что возможность запускать несколько версий платформы 1С на одном сервере, используя разные наборы портов [4], создает операционную сложность. Статическая конфигурация файрвола может быстро устареть. Например, администратор устанавливает новую версию платформы для тестирования на портах 2540-2691, но забывает обновить правила файрвола. В результате сервис не работает, что приводит к простоям и путанице. Или, что еще хуже, для «быстрого решения» проблемы открывается слишком широкий диапазон портов, что ослабляет защиту.

Поэтому управление правилами межсетевого экрана для 1С не должно быть разовой задачей. Этот процесс должен быть интегрирован в формальную процедуру управления изменениями (Change Management). Любое изменение в конфигурации кластера серверов 1С (добавление/удаление версии, смена портов) должно автоматически инициировать пересмотр и обновление набора правил файрвола. Этот процедурный контроль не менее важен, чем сама техническая настройка.

2.3. Безопасная Публикация Веб-Сервисов через HTTPS

Любой доступ к данным 1С через веб-интерфейс (веб-клиент, веб-сервисы, HTTP-сервисы) должен быть в обязательном порядке зашифрован с использованием протокола TLS (Transport Layer Security), ранее известного как SSL. **Обращаем внимание, что речь не только о работе с публикацией 1С по внешнему каналу связи, но и в локальной сети организации.** Передача учетных данных и конфиденциальной бизнес-информации по открытому протоколу HTTP является грубейшей уязвимостью, позволяющей перехватить трафик и получить несанкционированный доступ к системе. Для шифрования трафика используется порт 443 (HTTPS).

Let's Encrypt — это некоммерческий центр сертификации, который предоставляет бесплатные SSL/TLS сертификаты. Их главная особенность — автоматизация процесса выпуска и обновления, что делает переход на безопасное HTTPS-соединение доступным для всех.

Общие требования (Обязательно!)

Прежде чем начать, убедитесь, что у вас есть следующее:

1. **Зарегистрированное доменное имя:** Например, `your-site.com`. Let's Encrypt не выдает сертификаты для IP-адресов.
2. **Доступ к серверу:** У вас должен быть полный административный доступ к серверу, где размещен ваш сайт (root- или sudo-доступ в Linux, права Администратора в Windows).
3. **Настроенная DNS A-запись:** Ваше доменное имя (и поддомен `www`, если планируете его использовать) должно указывать на публичный IP-адрес вашего сервера. Let's Encrypt проверит это, чтобы убедиться, что домен действительно принадлежит вам.

🐧 Инструкция для Linux (Ubuntu/Debian, CentOS)

На Linux мы будем использовать официальный и самый популярный инструмент — **Certbot**. Он умеет не только получать сертификат, но и автоматически настраивать веб-сервер (Apache или Nginx).

Шаг 1: Установка Certbot

Самый современный и универсальный способ — использовать `snap`. Он работает на большинстве дистрибутивов.

1. Установите snapd, если его еще нет (на Ubuntu он обычно уже есть):

```
None

sudo apt update

sudo apt install snapd
```

2. Установите сам Certbot:

```
None

sudo snap install --classic certbot
```

3. Создайте символическую ссылку для удобства запуска:

```
None

sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

Шаг 2: Получение и установка сертификата

Certbot все сделает за вас. Просто запустите команду, соответствующую вашему веб-серверу.

- **Если у вас веб-сервер Nginx:**

```
None

sudo certbot --nginx
```

- **Если у вас веб-сервер Apache:**

```
None

sudo certbot --apache
```

Что произойдет дальше:

1. Certbot попросит вас ввести email-адрес (для уведомлений об истечении срока действия сертификата).
2. Вам нужно будет согласиться с условиями использования.

3. Certbot проанализирует конфигурацию вашего веб-сервера и покажет список доменов, которые он нашел. Выберите тот, для которого нужен сертификат.
4. Он спросит, нужно ли настроить автоматическое перенаправление с HTTP на HTTPS. **Рекомендуется выбрать "Redirect" (Перенаправлять)**.

После этого Certbot получит сертификат, установит его в конфигурацию Nginx/Apache и перезапустит веб-сервер.

Шаг 3: Проверка автоматического обновления

Сертификаты Let's Encrypt действуют **90 дней**. Certbot автоматически настраивает системный таймер (cron job или systemd timer) для их обновления за 30 дней до истечения срока.

Вы можете проверить, что все работает, выполнив "сухой запуск":

```
None

sudo certbot renew --dry-run
```

Если команда завершилась без ошибок, значит, автоматическое обновление настроено правильно. Больше ничего делать не нужно!

Шаг 4: Настройка фаервола

Откройте порт 443 для входящего трафика.

```
None
# Для UFW
sudo ufw allow 443/tcp
# Для Firewalld
sudo firewall-cmd --zone=public --add-service=https
--permanent
sudo firewall-cmd --reload
```

Шаг 5: Бэкап каталога с корневыми сертификатами

Резервное копирование и хранение корневых сертификатов в Linux — это важная

задача для обеспечения безопасности и целостности системы. Вот как это сделать правильно.

Где находятся корневые сертификаты

В большинстве дистрибутивов Linux корневые сертификаты и связанные с ними файлы хранятся в нескольких ключевых каталогах. Важно понимать их назначение, чтобы скопировать всё необходимое.

- /etc/ssl/certs/: Это основной каталог, где система и приложения, такие как OpenSSL, ищут доверенные корневые сертификаты. Он часто содержит символические ссылки на сертификаты, хранящиеся в `/usr/share/ca-certificates/`.
- /usr/share/ca-certificates/: Здесь хранятся файлы сертификатов (`.crt`), поставляемые пакетами операционной системы (например, пакетом `ca-certificates`).
- /etc/ca-certificates.conf: Это конфигурационный файл, который определяет, какие сертификаты из `/usr/share/ca-certificates/` являются активными и должны быть включены в единый файл-бандл.
- /etc/ssl/certs/ca-certificates.crt: Это единый файл, объединяющий все доверенные корневые сертификаты в системе. Многие приложения используют именно его для проверки SSL-соединений.

Как правильно создать бэкап

Для полного и корректного резервного копирования необходимо сохранить как сами сертификаты, так и их структуру и права доступа. Рекомендуется использовать утилиту `tar`, так как она сохраняет символические ссылки и метаданные файлов.

Выполните следующую команду от имени суперпользователя (через `sudo`):

Bash

```
None
sudo tar -pczf ca-certificates-backup-$(date +%F).tar.gz
/etc/ssl/certs /usr/share/ca-certificates
/etc/ca-certificates.conf
```

Где и как хранить бэкап

Хранение резервной копии не менее важно, чем её создание. Следуйте этим рекомендациям:

1. **Внешний носитель**: Храните архив на **внешнем, изолированном носителе**, например, на USB-накопителе или внешнем жёстком диске. Не оставляйте бэкап на том же сервере, так как в случае компрометации системы он также может быть утерян или повреждён.
2. **Физическая безопасность**: Убедитесь, что носитель с бэкапом находится в **физически безопасном месте** (например, в сейфе), чтобы предотвратить несанкционированный доступ.
3. **Шифрование**: Для дополнительной защиты **зашифруйте архив** с помощью GPG или другого надёжного инструмента шифрования. Это защитит ваши сертификаты, даже если носитель попадёт в чужие руки. *Пример шифрования с помощью GPG:*

Bash

```
None
gpg -c ca-certificates-backup-2025-08-19.tar.gz
```

4. После выполнения этой команды будет создан зашифрованный файл `ca-certificates-backup-2025-08-19.tar.gz.gpg`. Для расшифровки потребуется пароль, который вы задали.
5. **Несколько копий**: Следуйте правилу "3-2-1": храните **три** копии данных на **двух** разных типах носителей, причём **одна** из копий должна находиться в другом географическом месте.
6. **Контроль доступа**: Ограничьте доступ к резервным копиям только авторизованному персоналу.

🪟 Инструкция для Windows (сервер с IIS)

Для Windows нет официального клиента Certbot, но есть отличные аналоги. Самый популярный и удобный — **win-acme**. Он работает с веб-сервером IIS (Internet Information Services), который является стандартом для Windows Server.

Шаг 1: Подготовка IIS и скачивание win-acme

1. **Настройте сайт в IIS:** Убедитесь, что ваш сайт уже создан в диспетчере IIS и для него настроена **привязка (binding)** к вашему доменному имени по порту 80 (HTTP).
2. **Скачайте win-acme:**
    - Перейдите на официальную страницу релизов: github.com/win-acme/win-acme/releases.
    - Скачайте последнюю версию архива с названием типа `win-acme.vX.X.X.XXXX.x64.pluggable.zip`.
3. **Распакуйте архив:** Создайте папку в надежном месте (например, `C:\win-acme\`) и распакуйте туда содержимое архива. Не стоит распаковывать на Рабочий стол или в папку Загрузок.

Шаг 2: Запуск и получение сертификата

1. Откройте папку, куда вы распаковали win-acme (`C:\win-acme\`).
2. Нажмите правой кнопкой мыши на файл `wacs.exe` и выберите **"Запуск от имени администратора"**.
3. Откроется консольное меню. Для первого раза самый простой путь:
    - Нажмите **`N`**, чтобы выбрать **"Create a new certificate (default settings)"** (Создать новый сертификат).
    - Программа просканирует ваши сайты в IIS и предложит список. Выберите нужный сайт, введя его номер.
    - Программа попросит ввести email для уведомлений. Введите его и нажмите Enter.
    - Согласитесь с условиями использования.

`win-acme` автоматически проведет валидацию, получит сертификат, создаст новую привязку для сайта в IIS по порту 443 (HTTPS) и применит к ней сертификат.

Шаг 3: Автоматическое обновление

Самое главное — `win-acme` самостоятельно создает задачу в **Планировщике заданий Windows** (Windows Task Scheduler). Эта задача будет автоматически запускаться каждый день, проверять срок действия сертификата и обновлять его при необходимости.

Шаг 4: Настройка фаервола

Убедитесь, что в «Брандмауэре Защитника Windows» создано разрешающее правило для входящего трафика по протоколу TCP на порт 443.

Внедрение HTTPS — это процесс, состоящий из трех взаимосвязанных слоев: **Сертификат -> Веб-сервер -> Файрвол**. Ошибка на любом из этих уровней (невалидный сертификат, неверная конфигурация веб-сервера, заблокированный порт) приведет либо к неработоспособности сервиса, либо к появлению у пользователей предупреждений безопасности. Такие предупреждения приучают игнорировать сигналы об опасности, что само по себе является риском. Поэтому после завершения настройки обязательна проверка: откройте адрес вашего веб-сервиса в браузере с внешнего компьютера и убедитесь, что соединение установлено по HTTPS и в адресной строке отображается значок замка без каких-либо ошибок.

Раздел 3. Укрепление Серверов и Рабочих Станций

После защиты сетевого периметра необходимо укрепить сами конечные точки — серверы и рабочие станции. Этот эшелон обороны предназначен для противодействия угрозам, которые смогли обойти сетевую защиту, а также внутренним угрозам.

3.1. Оптимальная Настройка Антивирусного ПО

Антивирусное программное обеспечение является обязательным компонентом защиты, однако его неправильная конфигурация на серверах с интенсивной дисковой нагрузкой, таких как серверы 1С и СУБД, может привести к серьезным проблемам с производительностью и даже к повреждению данных. Антивирусный сканер, проверяющий в реальном времени файлы баз данных, их журналы и резервные копии, может вызывать блокировки, замедлять операции ввода-вывода и конфликтовать с работой СУБД.

Поэтому ключевой задачей является нахождение баланса между безопасностью и производительностью путем создания точных исключений из сканирования. Перед развертыванием любого антивирусного решения необходимо провести тестирование производительности системы под полной нагрузкой до и после его установки, чтобы оценить влияние на быстродействие.[11]

Наиболее авторитетные рекомендации по настройке исключений для серверов баз данных предоставляет Microsoft для SQL Server.[11] Эти рекомендации полностью применимы к серверам 1С, работающим в клиент-серверном режиме с MS SQL.

Таблица 2: Рекомендуемые исключения антивируса для сервера 1С с СУБД MS SQL

Тип исключения	Путь / Процесс / Расширение	Обоснование
Процессы	sqlservr.exe	Основной процесс ядра СУБД. Исключение предотвращает вмешательство в его работу.
	sqlagent.exe	Процесс Агента SQL Server, отвечающий за выполнение заданий (в т.ч. бэкапов).
	sqlbrowser.exe	Служба обозревателя SQL Server.
Директории	%ProgramFiles%\Microsoft SQL Server\...\MSSQL\DATA\ ***Важно! Указан каталог по-умолчанию, в рабочей системе может отличаться***	Каталог с файлами данных и журналов транзакций. Сканирование может вызвать блокировки и повреждение.
	%ProgramFiles%\Microsoft SQL Server\...\MSSQL\Backup\ ***Важно! Указан каталог по-умолчанию, в рабочей системе может отличаться***	Каталог с файлами резервных копий. Сканирование во время создания бэкапа замедляет процесс.
	%ProgramFiles%\Microsoft SQL	Каталог файлов полнотекстового индекса.

	Server\...\MSSQL\FTDATA\ ***Важно! Указан каталог по-умолчанию, в рабочей системе может отличаться***	
	Каталог данных Filestream	Каталог для данных Filestream (если используется).
Расширения файлов	.mdf	Файлы данных SQL Server.
	.ldf	Файлы журнала транзакций SQL Server.
	.ndf	Вторичные файлы данных SQL Server.
	.bak	Файлы резервных копий.
	.trn	Файлы резервных копий журнала транзакций.
	.trc	Файлы трассировки SQL Server.
	.sqlaudit	Файлы аудита SQL Server.

Для настройки исключений в антивирусе для PostgreSQL необходимо добавить в исключения папки, в которых хранятся данные PostgreSQL, а также файлы, используемые PostgreSQL для работы, такие как файлы журналов и временные файлы. Конкретные шаги зависят от используемого антивирусного ПО.

Рекомендации по настройке исключений для PostgreSQL:

Тип исключения	Путь / Процесс / Расширение	Обоснование
Процессы	postgres.exe	Основной процесс ядра СУБД. Исключение предотвращает вмешательство в его работу.
	pg_ctl.exe	Утилита для запуска, остановки и перезагрузки сервера
	pg_walwriter.exe	Процесс, отвечающий за запись WAL-файлов (журналов транзакций)
	pg_stats.exe	Процесс, собирающий статистику
	pg_autovacuum.exe	Процесс для автоматической очистки
	postmaster.exe	Главный процесс PostgreSQL
Директории	/var/lib/postgresql/<версия>/main/log или C:\Program Files\PostgreSQL\<версия>\data\log. ***Важно! Указан каталог по-умолчанию, в рабочей системе может отличаться***	Каталог с файлами журналов PostgreSQL
	Это может быть каталог /tmp или /var/tmp	Временные каталоги, используемые PostgreSQL

	в Linux это может быть /var/lib/postgresql/<версия>/main/data или /var/lib/pgsql/<версия>/data, а в Windows - C:\Program Files\PostgreSQL\<версия>\data.	Каталог для данных
Расширения файлов	.dat	Файлы данных.
	.log	Файлы журнала транзакций.
	.wal	Журналы Write-Ahead Log, критически важные для целостности данных.
	.bak	Файлы резервных копий.
	.md	Метаданные файлов.
	.tbl	Таблицы данных.
	.idx	Файлы индексов, которые хранят структуру данных для ускорения запросов.

Добавьте исключения в антивирусе для сервера приложений 1С:

Тип исключения	Путь / Процесс / Расширение	Обоснование
Процессы	ragent.exe (агент сервера 1С)	Основные процессы сервера приложений 1С.

	rmngr.exe (менеджер кластера 1С) rphost.exe (рабочий процесс 1С)	Исключение предотвращает вмешательство в его работу.
	1cestart.exe (исполняемый файл платформы 1С) 1cv8.exe (исполняемый файл платформы 1С, толстый клиент) 1cv8s.exe (исполняемый файл платформы 1С) 1cv8c.exe (Тонкий клиент 1С)	Исполняемые файлы клиента 1С, запускаемые на стороне пользователя.
Директории	%ProgramFiles%*1cv8*\<*номер версии платформы*>*bin* ***Важно! Указан каталог по умолчанию, в рабочей системе может отличаться***	Каталог с рабочими файлами платформы 1С. Сканирование может вызвать блокировки и повреждение.
	%ProgramFiles%*1cv8**srvinfo*\ ***Важно! Указан каталог по умолчанию, в рабочей системе может отличаться***	Каталог данных кластера 1С. Сканирование во время создания бэкапа замедляет процесс.
	Папка с базами данных файловой версии 1С: Укажите путь к папке, где хранятся базы данных 1С (например, C:\1CV8\...)	Каталог базы файлового варианта работы 1С.
Расширения файлов	*.1CD, *.CDX, *.DBF	Файлы данных файлового варианта работы 1С.
	*.1CD	Для файлового режима работы необходимо добавить в исключения

		расширение .1CD также на всех клиентских рабочих станциях.

3.2. Блокировка Несанкционированных USB-Накопителей

Съемные USB-накопители (флешки, внешние диски) представляют собой двойную угрозу:

1. **Вектор заражения:** Они являются одним из классических способов доставки вредоносного ПО в изолированную или защищенную корпоративную сеть.
2. **Канал утечки данных:** Неконтролируемое использование USB-накопителей позволяет сотрудникам легко выносить за пределы компании большие объемы конфиденциальной информации, включая выгрузки из баз данных 1С.

Контроль за использованием съемных носителей является критически важной мерой по укреплению конечных точек.

Реализация для Windows:

Наиболее эффективным способом управления доступом к USB-устройствам в доменной среде является использование групповых политик (GPO).

1. Откройте редактор управления групповыми политиками (gpmc.msc).
2. Создайте или отредактируйте объект GPO, который применяется к нужным компьютерам.
3. Перейдите по пути: Конфигурация компьютера -> Политики -> Административные шаблоны -> Система -> Доступ к съемным запоминающим устройствам.
4. Здесь находится набор политик, позволяющих гибко управлять доступом. Основная политика — «Все классы съемных запоминающих устройств: Запретить любой доступ». Установите ее в состояние «Включена». Это полностью заблокирует использование любых USB-накопителей.

Часто возникает необходимость разрешить использование конкретных, одобренных службой безопасности устройств (например, зашифрованных флешек или токенов). Такой подход является более зрелым, так как он балансирует безопасность и бизнес-потребности. Для этого можно использовать

более гранулярные политики, которые позволяют разрешать или запрещать устройства по их ID оборудования (Hardware ID). Это позволяет реализовать политику «запрещено все, кроме разрешенного списка».

Реализация для Linux:

В Linux контроль над USB-устройствами можно осуществлять с помощью правил udev. udev — это подсистема, которая управляет устройствами в каталоге /dev и позволяет выполнять определенные действия при подключении или отключении устройства.

1. Создайте файл правил, например, /etc/udev/rules.d/99-block-usb-storage.rules.
2. Добавьте в него правило, которое будет блокировать новые USB-накопители. Пример простого правила, которое запрещает авторизацию новых устройств класса usb-storage:
   `SUBSYSTEM=="usb", DRIVERS=="usb-storage", ATTR{authorized}="0"`
3. Для более сложного сценария (например, разрешить только определенные устройства) можно написать правило, которое будет проверять ID вендора и продукта (idVendor, idProduct) и разрешать авторизацию только для них, а для всех остальных — запрещать.

Рекомендуемый подход к внедрению — поэтапный. Начать следует с полного запрета, чтобы немедленно закрыть основной вектор угрозы. Затем, в сотрудничестве с бизнес-подразделениями, необходимо выявить легитимные сценарии использования USB-накопителей, составить список одобренных устройств и создать точечные исключения в политиках.

3.3. Защита Файлового Режима Работы

Файловый режим работы 1С, несмотря на свою простоту в развертывании, несет в себе специфические и весьма серьезные риски безопасности и стабильности. В этом режиме все клиенты напрямую обращаются к одному файлу базы данных (.1CD), расположенному в общей сетевой папке.

Ключевые меры защиты:

1. **Настройка прав доступа к сетевой папке:** Это самый важный элемент защиты. Доступ к каталогу, где лежит база данных, должен быть настроен с

максимальной строгостью.

- **На сервере Windows (NTFS + SMB):**
  - Создайте в Active Directory специальную группу безопасности, например, 1C_File_Users.
  - Включите в эту группу только тех пользователей, которым действительно нужен доступ к этой базе.
  - На уровне разрешений общего доступа (Share Permissions) предоставьте этой группе права «Изменение».
  - На уровне разрешений файловой системы (NTFS Permissions) также предоставьте этой группе права «Изменение», но не «Полный доступ».
  - Явно запретите доступ для встроенных групп «Все» (Everyone) и «Прошедшие проверку» (Authenticated Users).
- **На сервере Linux (Samba):**
  - В файле конфигурации Samba (smb.conf) для общей папки используйте директивы valid users = @groupname, чтобы ограничить доступ только членами определенной группы.
  - Установите правильные маски создания файлов и каталогов (create mask = 0660, directory mask = 0770), чтобы новые файлы не получали избыточных прав.

2. **Исключения антивируса:** Как уже упоминалось, файл .1CD должен быть добавлен в исключения антивирусного сканирования как на файловом сервере, так и на всех без исключения клиентских рабочих станциях, которые с ним работают.

Необходимо четко осознавать, что файловый режим работы по своей природе уязвим. Производительность и целостность данных в этом режиме крайне чувствительны к качеству сети. Кратковременный сбой сети или аварийное завершение работы одного из клиентов в момент записи в базу может легко привести к повреждению всего файла .1CD.

С точки зрения безопасности, этот режим еще более опасен. Если программа-шифровальщик попадет на любую из клиентских рабочих станций, имеющих доступ к общей папке, она сможет зашифровать центральный файл базы данных через подключенный сетевой диск. Это мгновенно парализует работу всех пользователей системы.

Исходя из этих рисков, файловый режим работы можно считать приемлемым

только для очень ограниченного круга сценариев: не более 3-5 пользователей, работающих в пределах одной высоконадежной, проводной локальной сети. Для всех остальных случаев настоятельно рекомендуется переход на клиент-серверную архитектуру. Преимущества клиент-серверного режима в плане надежности, производительности и, главное, безопасности многократно окупают затраты на его внедрение.

Заключение: Построение Эшелонированной и Эффективной Защиты

В данном руководстве были рассмотрены ключевые меры по обеспечению безопасности платформы 1С:Предприятие. Цель состояла не в том, чтобы описать все возможные механизмы защиты, а в том, чтобы сконцентрировать внимание и ресурсы на тех из них, которые дают максимальный вклад в снижение рисков. Комплексное внедрение этих рекомендаций позволяет построить надежную и глубоко эшелонированную оборону, способную противостоять подавляющему большинству современных киберугроз.

Краткое изложение ключевых рекомендаций:

1. **Резервное копирование по правилу «3-2-1»:** Внедрение стратегии с тремя копиями данных на двух разных носителях и одной обязательной изолированной (air-gapped или immutable) копией является последним и самым надежным рубежом защиты от программ-вымогателей и сбоев.
2. **Межсетевой экран с политикой «запрещено по умолчанию»:** Жесткий контроль сетевого трафика на уровне хоста, разрешающий доступ только к строго определенным портам, необходимым для работы 1С, кардинально сокращает поверхность атаки.
3. **Обязательное использование HTTPS:** Любая публикация веб-клиентов или веб-сервисов 1С во внешней сети или даже внутри корпоративной сети должна осуществляться исключительно по зашифрованному протоколу HTTPS для защиты учетных данных и передаваемой информации.
4. **Точная настройка антивирусного ПО:** Создание выверенного списка исключений для процессов, каталогов и файлов 1С и СУБД позволяет избежать проблем с производительностью и стабильностью, не жертвуя при этом безопасностью.
5. **Строгий контроль доступа:** Реализация принципа наименьших привилегий на всех уровнях — от ролей в приложении 1С до прав в операционной

системе и СУБД — является фундаментальным барьером на пути злоумышленника.

Эти меры не являются изолированными. Они формируют систему «защиты в глубину» (Defense in Depth), где каждый слой дополняет и страхует предыдущий. Злоумышленник, которому удастся обойти один рубеж обороны, с высокой вероятностью будет остановлен на следующем.

В заключение необходимо подчеркнуть, что информационная безопасность — это не единовременный проект, а непрерывный процесс. Ландшафт угроз постоянно меняется, появляются новые уязвимости, развивается IT-инфраструктура компании. Поэтому внедренные меры защиты требуют постоянного контроля, пересмотра и адаптации. Регулярный аудит, тестирование на проникновение, своевременное обновление всех компонентов системы и, что не менее важно, повышение осведомленности пользователей в вопросах кибербезопасности должны стать неотъемлемой частью корпоративной культуры. Только такой комплексный и динамичный подход позволит обеспечить долгосрочную и эффективную защиту информационных активов, сосредоточенных в системе 1С:Предприятие.

Источники

1. 1С-ARCH Базовая защита 1С от шифровальщиков, accessed August 5, 2025, https://dc1.su/uslugi/uskorenie-i-zashchita-1s/1c-arch-bazovaya-zashchita-1s-ot-shifrovalshchikov/
2. Правило 3-2-1 - стандарт для безопасного резервного копирования., accessed August 5, 2025, https://serverpart.kz/a46492-pravilo-standart-dlya.html
3. Хранение настроек кластера серверов 1С:Предприятия 8.1 ..., accessed August 5, 2025, https://its.1c.ru/db/content/metod8dev/src/platform81/administration/i8101570.htm
4. Установка серверной части 1С в Linux среде (сентябрь 2021), accessed August 5, 2025, https://rarus.ru/publications/20210927-ot-ekspertov-ustanovka-1c-linux-496320/
5. Using UFW Firewall in Ubuntu Linux [Beginner's Guide] - It's FOSS, accessed August 5, 2025, https://itsfoss.com/ufw-ubuntu/
6. How to Set Up a Firewall with UFW on Ubuntu - DigitalOcean, accessed August 5, 2025, https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu

7. UFW allow port range - How we do it? - Bobcares, accessed August 5, 2025, https://bobcares.com/blog/ufw-allow-port-range/
8. Создание высокодоступной фермы рабочих серверов OneScript ..., accessed August 5, 2025, https://infostart.ru/1c/articles/1057169/
9. Установка SSL-сертификата на IIS • Hostpro Wiki, accessed August 5, 2025, https://hostpro.ua/wiki/ssl/installing-ssl-certificate-on-iis/
10. Установка SSL сертификата на Apache / Oblako.kz в Казахстане, accessed August 5, 2025, https://oblako.kz/help/ssl/install-ssl-na-apache
11. Configure antivirus software to work with SQL Server - Microsoft Learn, accessed August 5, 2025, https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/security/antivirus-and-sql-server
12. Antivirus software for APS - Parallel Data Warehouse | Microsoft Learn, accessed August 5, 2025, https://learn.microsoft.com/en-us/sql/analytics-platform-system/antivirus-software?view=aps-pdw-2016-au7