Реализация мер обеспечения безопасности информации средствами «1С:Предприятие 8»

Марк Суарес
Руководитель направления
suam@1c.ru

Информация ограниченного доступа

Статья 9 Закона «Об информации…» № 149-ФЗ

ГОСТАЙНА

Указ Президента РФ от 30.11.1995 № 1203

Конфиденциальная информация

- Закон 152-ФЗ — Персональные данные → У всех. Самые жесткие требования у медиков
- Закон 98-ФЗ — Коммерческая тайна → Повсеместно
- Служебная тайна. Постановление № 1233 от 1994г → Органы власти. Предприятия оборонно-промышленного комплекса
- Служебная тайна в области обороны статья 3.1 Закона «Об обороне» → Органы власти. Предприятия оборонно-промышленного комплекса
- Сведения о сущности изобретения, полезной модели или промышленного образца → Предприятия оборонно-промышленного комплекса
- Закон «О Связи» ст.63 — Тайна связи → Почта России

Гриф «Для служебного пользования»

Указ Президента РФ от 06.03.1997 № 188

Приказы ФСТЭК России и вопросам ОБИ

- Приказ ФСТЭК от 28.02.2017 № 31 дсп «Требования к обеспечению защиты информации содержащейся в информационных системах управления производством, используемых предприятиями ОПК»

- Приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

- Приказ ФСТЭК России № 239 от 25.12.2017 «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры»

Методический документ «Меры защиты информации в государственных информационных системах»

Фундаментальные нормативные акты

- Руководящий документ «Защита от несанкционированного доступа. Термины и определения»
- Приказ ФСТЭК России № 76 от 2020г «Требования доверия по безопасности информации» (Требования доверия)
- Руководящий документ «Защита от несанкционированного доступа» (РД СВТ)
- Руководящий документ «Контроль отсутствия недекларируемых возможностей» (РД НДВ) ➔**В настоящее время отменен ФСТЭК, но действует в Минобороны**
- Руководящий документ «Классификация автоматизированных систем» (РД АС)➔**Частично отменен Приказом ФСТЭК № 025 от 2016г**
- Приказ ФСТЭК России № 55 от 2018г «Положение о системе сертификации средств защиты информации» (Положение по сертификации)

Дополнительные требования

ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций»

- Постановление Правительства РФ от 15.01.2018 № 10
  ~«Освобождение от раскрытия информации»
  предприятия имеют полное право не публиковать информацию по крупным сделкам:

  - выполненным по гособоронзаказу;

  - в рамках военно-технического сотрудничества;

  - любых сделок с предприятиями и лицами, попавшими под санкции;

- Постановление Правительства РФ от 12.01.2018 № 5
  ~«О запрете размещения информации в Интернет»

  Если предприятие находится под санкциями, то публикация финансовой отчетности запрещается

Законодательство в области обороны

- **Статья 3.1 Закона «Об обороне»**
  Введено новое понятие «Служебная тайна в области обороны»

- Постановление Правительства РФ от 26.11.2021 № 2052

"Об утверждении Правил обращения со сведениями, составляющими служебную тайну в области обороны«

- Приказ Министра обороны РФ от 17.01.2022 № 22

"Об утверждении Перечня сведений Вооруженных Сил Российской Федерации, подлежащих отнесению к служебной тайне в области обороны"

Нормативные акты по безопасности персональных данных

Нормативный акт	Что устанавливает
Федеральный закон № 152-ФЗ «О персональных данных»	Общие требования к обеспечению безопасности персональных данных
Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	Уровни защищенности ПДн в зависимости от объема, категории и типа угроз
Приказ ФСТЭК России от 18.02.2013 № 21 «Состав и содержание мер обеспечения безопасности ПДн»	Конкретный перечень мер обеспечения безопасности ПДн в зависимости от уровня защищенности

Обработка персональных данных не является лицензируемым видом деятельности. Ни вам, ни вашим клиентам не требуется получать лицензию ФСТЭК, если речь идет о персональных данных ваших сотрудников, пациентов, клиентов ит.п.

Разъяснение ФСТЭК № 240/13/2549 от 06.06.2018

КАК ВСЁ ЭТО СООТНОСИТСЯ К 1С:ПРЕДПРИЯТИЮ?

Соотнесение требований к 1С:Предприятию

Тип предприятий ОПК	Требования законодательства	Что требуется	В каких прикладных решениях «1С:Предприятие 8»
Предприятия, находящиеся под санкциями	Постановление Правительства РФ от 05.01.2018 № 5	Следует ограничить доступ к инструментам формирования финансовой отчетности	1С:Бухгалтерия 8; 1С:ERP; 1С:УПП; иные учетные системы
Оборонные предприятия	**Приказ ФСТЭК России № 31 дсп от 28.02.2017**	Доп. настройки; разнесение по разным ИС в отдельные сегменты	**1С:ERP; 1С:УПП; 1С:PDM; 1С:Управление холдингом 8**
Иные предприятия, выполняющие работы по ГОЗ и/или ВТС	Постановление Правительства РФ от 15.01.2018 № 10	Следует ограничить доступ и обеспечить контроль за формированием отчетности	1С:Бухгалтерия 8; 1С:ERP; 1С:УПП; иные учетные системы
Предприятия КИИ	Приказ ФСТЭК России № 239 от 2017г	Настройки по требованиям Приказа	Все решения, если они относятся к объектам КИИ

СОГЛАШЕНИЯ И ОГРАНИЧЕНИЯ

Прикладные решения «1С:Предприятие 8» представляют собой совокупность настроек и скриптов, интерпретатором которых является технологическая платформа «1С:Предприятие 8» и самостоятельно никакой код не выполняют

«1С:Предприятие 8» не реализует функции контроля печати
- регистрация выдачи печатных (графических) выходных документов [по РД АС];
- маркировка документов [п. 2.4.5 РД СВТ]

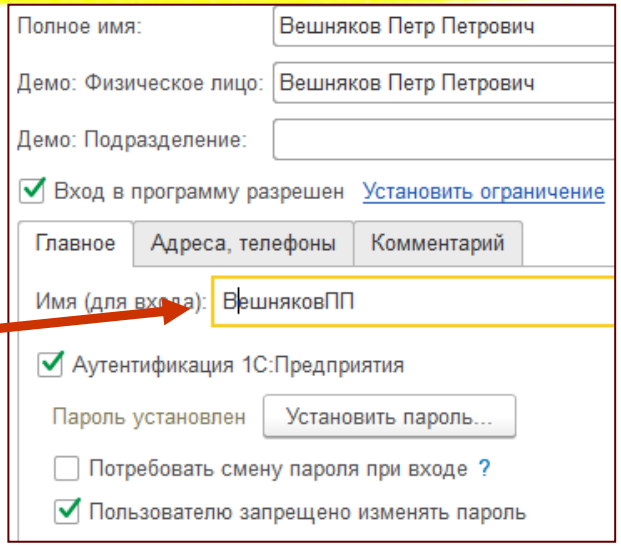
«1С:Предприятие 8» обращается к СУБД как один пользователь
- такова особенность всех серверов приложений;
- доступ иными средствами к БД 1С:Предприятия **запрещен** (см. лицензионное соглашение) «запрещается осуществлять доступ к информационной базе изделия и построение систем на основе изделия с помощью средств и технологических решений, не предусмотренных документацией»

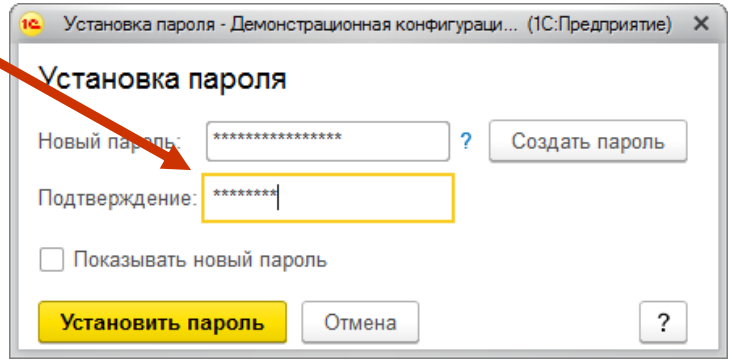
«1С:Предприятие 8» никак не влияет на работу наложенных СЗИ

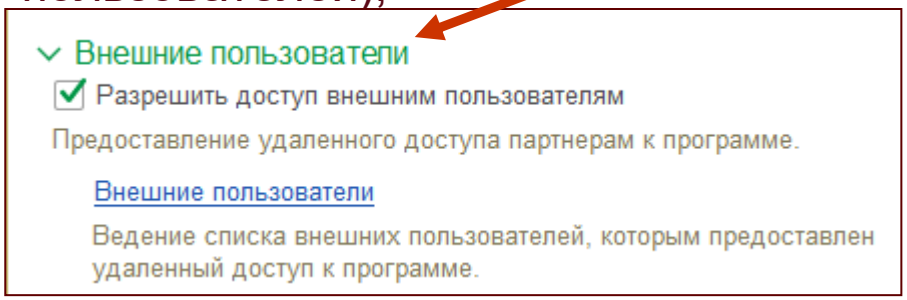
«1С:Предприятие 8» не является средством криптографической защиты информации

Меры идентификации и аутентификации

- **ИАФ.1** - Идентификация и аутентификация пользователей, являющихся работниками оператора;
- **ИАФ.3** - Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- **ИАФ.5** - Защита обратной связи при вводе аутентификационной информации;
- **ИАФ.6** - Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);







Документация https://its.1c.ru/db/v8317doc#bookmark:adm:TI000000122

Управление правами доступа

Средствами «1С:Предприятие 8» реализованы меры группы УПД:

- **УПД.1** - Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- **УПД.2** - Реализация необходимых методов (ролевой метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- **УПД.4** - Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- **УПД.5** - Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- **УПД.6** – Ограничение неуспешных попыток входа в информационную систему
- **УПД.9** - Ограничение числа параллельных сеансов доступа;
- **УПД.10** - Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
- **УПД.11** - Запрет действий пользователей, разрешенных до идентификации и аутентификации;

Основы управления доступом в 1С:Предприятии

Роль - это минимальная единица, описывающая **Права** пользователя на выполнение неких действий, как общесистемных (запуск тонкого/толстого клиента), так и функциональных (чтение, добавление, использование, редактирование неких объектов конфигурации).

Меры УПД.2, УПД.5

Права назначаются **Ролями** ==>
Роли входят в **Профили групп доступа** ==>
в **Профилях групп доступа** могут назначаться определенные ограничения по **Видам доступа** ==>
Профиль группы доступа соответствует только одной **Группе доступа** ==>
Группа доступа включает в себя **Пользователей** ==>
в **Группах доступа** также могут назначаться определенные ограничения по **Видам доступа**

Один пользователь может входить в несколько **Групп доступа**.

Документация https://its.1c.ru/db/bsp311doc#content:1911:hdoc

Описание прав доступа https://its.1c.ru/db/v8317doc#bookmark:dev:TI000001241

ПРИМЕР

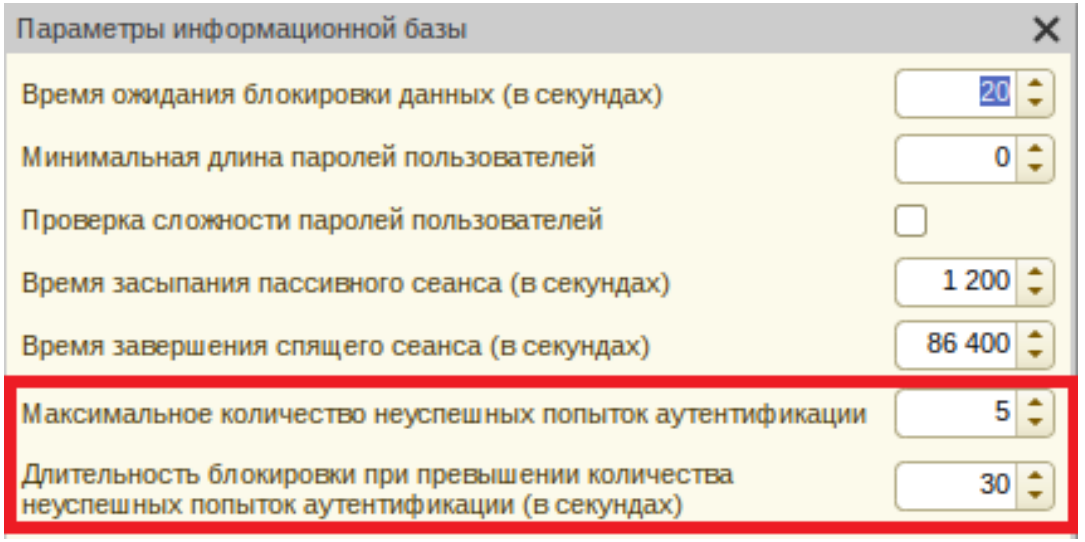
Соотнесение пользователя определенным группам доступа представляет собой **совокупность полномочий пользователя**

Пользователь	Группа доступа	Профиль группы доступа	Роль	Право
Совокупность полномочий	Базовые полномочия	Профиль «Базовые полномочия»	Базовые права	Чтение видов контактной информации
			Запуск Тонкого Клиента	Запуск тонкого клиента
	Функциональные полномочия	Профиль «Функциональные полномочия»	Добавление и изменение договоров	Чтение, Добавление и Изменение документа «Акт выполненных работ»
			Настройка договоров	Чтение и Изменение справочника «Договоры»
	Специальные полномочия	Профиль «Специальные полномочия»	Выполнение обмена электронными документами	Использование и Просмотр обработки «Обмен с банками»

Итого, **Пользователю** доступно пять **Ролей**, разрешающих (!) ему: Запускать тонкий клиент; Читать справочник «Виды контактной информации», полноценно работать с документом «Акт выполненных работ», читать и изменять справочник «Договоры», а также использовать и просматривать результаты работы обработки «Обмен с банками».

Меры УПД.6 и УПД.10

Начиная с версии 8.3.16 реализовано требование «Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)»



Документация:

- Блокировка установки сеансов пользователям
  https://its.1c.ru/db/v8317doc#bookmark:cs:TI000000186
- Максимальное количество попыток аутентификации и длительность блокировки
  https://its.1c.ru/db/v8317doc#bookmark:adm:TI000000136

Мера УПД.9

Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы

Реализуется посредством механизма внешнего управления сеансами
«доступно только для версии КОРП»

Документация:

- Описание механизма внешнего управления сеансами
  https://its.1c.ru/db/v8317doc#bookmark:cs:TI000000186
- Описание примера реализации
  https://its.1c.ru/db/v8317doc#bookmark:cs:TI000000188

Регистрация событий безопасности

Средствами «1С:Предприятие 8» реализованы меры группы РСБ:

- **РСБ.1** - Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- **РСБ.2** - Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
- **РСБ.3** - Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- **РСБ.5** - Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- **РСБ.7** - Защита информации о событиях безопасности;

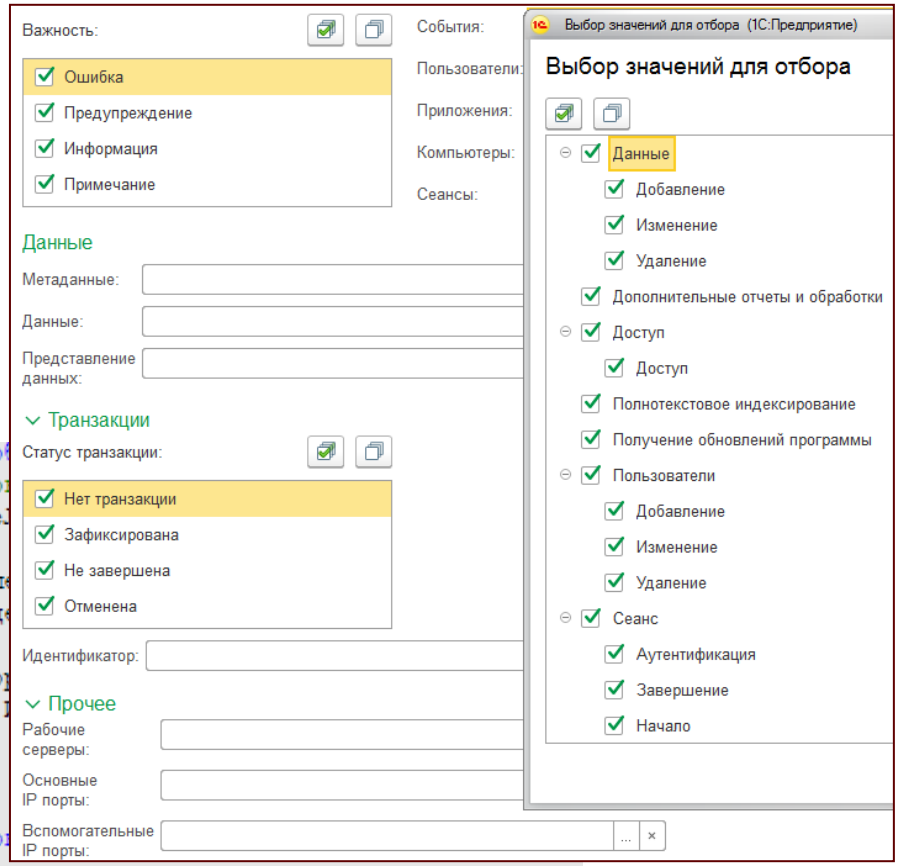
Настройка отбора событий безопасности

Меры РСБ.1 и РСБ.2 настраиваются в Конфигураторе

и реализуются в Журнале регистрации

- Реализована настройка отбора зарегистрированных событий по большому количеству критериев
- Необходимость регистрации события и перечень объектов метаданных по событиям настраиваются администратором

```
НастройкаСправочника = Новый ОписаниеИспользованияСо
// Укажем объект, доступ к которому будет регистриро
НастройкаСправочника.Объект = "Справочник.Физические
// Укажем поля доступа
НастройкаСправочника.ПоляДоступа.Добавить("Паспортны
НастройкаСправочника.ПоляДоступа.Добавить("Дети.Свид
// Укажем поля регистрации
НастройкаСправочника.ПоляРегистрации.Добавить("Паспо
НастройкаСправочника.ПоляРегистрации.Добавить("Дети.
АльтернативыПолей = Новый Массив();
АльтернативыПолей.Добавить("Фамилия");
АльтернативыПолей.Добавить("Имя");
НастройкаСправочника.ПоляРегистрации.Добавить(Альтер
НастройкаОбъектовМетаданных = Новый Массив();
НастройкаОбъектовМетаданных.Добавить(НастройкаСправочника);
```



Документация https://its.1c.ru/db/v8317doc#bookmark:dev:TI000000826

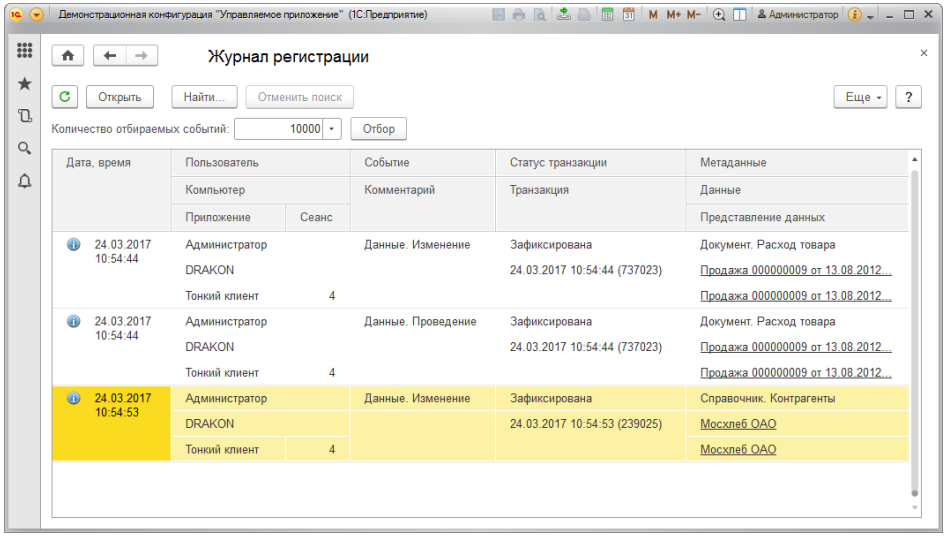
Регистрация событий в информационной базе

Меры РСБ.3 и РСБ.5 реализованы в Журнале регистрации

- Журнал регистрации содержит информацию о том, какие события происходили в информационной базе в определенный момент времени или какие действия выполнял тот или иной пользователь

- Журнал регистрации по событию Доступ регистрирует факты доступа пользователей системы к тем или иным данным

- По событию Отказ в доступе регистрирует факты отказа в доступе к тем или иным данным пользователям системы



Документация https://its.1c.ru/db/v8317doc#bookmark:adm:TI000000145

Регистрация управляющих воздействий администратора кластера серверов

Усиление меры РСБ.3

```
<?xml version="1.0" encoding="utf-8"?>
<config xmlns="http://v8.1c.ru/v8/tech-log">
    <log location ="/home/v8logs" history="384">
        <event> <eq property="name" value="ADMIN"/> </event>
        <property name="all" />
    </log>
</config>
```

По группе событий ADMIN технологического журнала

- аутентификация ИБ; в кластере; удаленного сервера;
- добавление/удаление кластера; ИБ; пользователя; рабочего сервера;
- создание/изменение записей в профилях безопасности; добавление/удаление профиля безопасности;
- изменение параметров ИБ; изменения параметров кластера;
- чтение параметров кластера серверов;
- регистрация удачных и неудачных попыток создания/изменения/удаления

Документация https://its.1c.ru/db/v8317doc#bookmark:adm:TI000000149

Обеспечение целостности информационной системы и персональных данных

Меры ОЦЛ.1 и ОЦЛ.2 реализуются утилитой контроля целостности ci

Утилита контроля целостности (ci) предназначена для контроля состояния объектов файловой системы и базы данных, используемых при работе «1С:Предприятие», и обнаружения ситуации изменения этих объектов.

```
Контроль целостности файловой информационной базы:
/opt/1C/v8.3/x86_64/ci check --in /home/user/CI/konf.txt --etalon /home/user/CI/etalonkonf.txt --report /home/user/CI/reportkonf.txt
Контроль целостности клиент-серверной информационной базы:
/opt/1C/v8.3/x86_64/ci check --in /home/user/CI/serv.txt --etalon /home/user/CI/etalonserv.txt --report /home/user/CI/reportserv.txt
Контроль целостности платформы «1С:Предприятие 8»:
/opt/1C/v8.3/x86_64/ci check --in /home/user/CI/plat.txt --etalon /home/user/CI/etalonplat.txt --report /home/user/CI/reporplat.txt
```

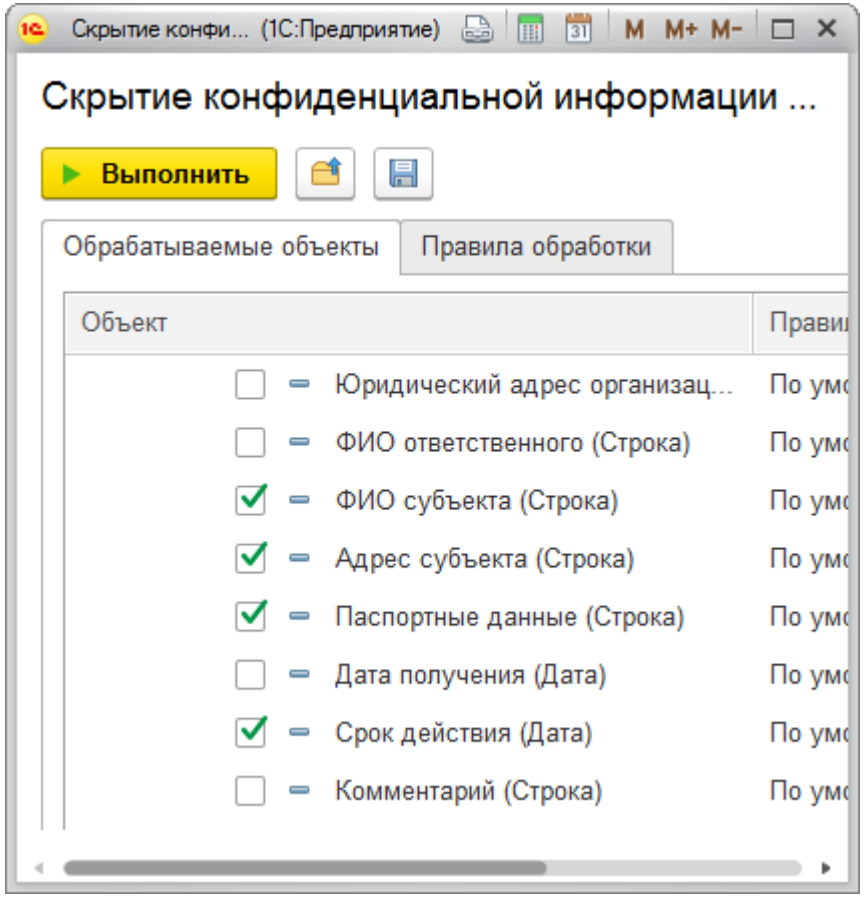
```
Отчет по изменениям в файловой информационной базе:
[dbe:///home/user/1C/infobase1/?users]
users = M
Отчет по изменениям в клиент-серверной информационной базе:
[postgre://127.0.0.1:5432/db1/?config,users]
config = M
users = M
Отчет по изменениям в платформе «1С:Предприятие 8»:
[rdir:///opt/1C/v8.3/x86_64/?*]
1ctest.so = A
1cv8_az.hbk = M
xml2.so = D
```

Документация https://its.1c.ru/db/v8317doc#bookmark:adm:TI000000510

Скрываем конфиденциальную информацию

ЗНИ.8 – Уничтожение (стирание) информации и обезличивание персональных данных

- После окончания действия соглашения об обработке персональных данных необходимо их очищать.
- Реализован программный интерфейс для уничтожения персональных данных по переданному отбору.
- Регламентное задание для автоматического уничтожения данных по истечению срока согласия на предоставление персональных данных.



Мера ЗИС.21

Очистка внешней памяти

только в ЗПК «1С:Предприятие 8.3z»

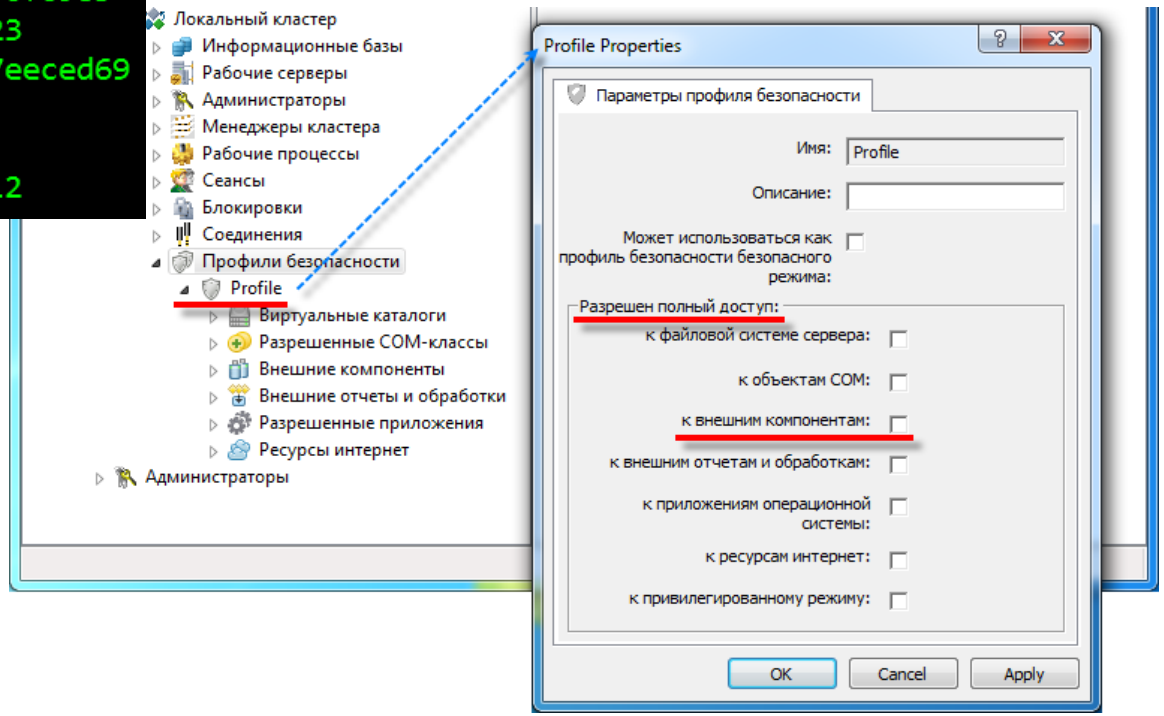
Средства ограничения программной среды

ОПС.1 - Управление запуском (обращениями) компонентов программного обеспечения

Профили безопасности - набор явно заданных разрешений использования теми или иными внешними ресурсами (с указанием перечня таких ресурсов), которые могут назначаться информационным базам, зарегистрированным в кластере

```
/opt/1C/v8.3/x86_64/rac infobase update
--cluster=9481fdc2-c689-11e6-d58d-0800270f6985
--cluster-user=newadmin --cluster-pwd=123
--infobase=9d2fa99a-448e-11e3-0d94-d43d7eeced69
--descr=NewInfoBaseProfil
--security-profile-name=profil1
--safe-mode-security-profile-name=profil2
```

Пример добавления профиля безопасности информационной базы



Документация: https://its.1c.ru/db/v8317doc#bookmark:cs:TI000000053

Защищенный программный комплекс «1С:Предприятие 8.3z»

Класс АС	Уровень доверия	Класс защищенности СВТ	Гриф секретности
1Г	УД-4	5-СВТ	Конфиденциально

Astra Linux Special Edition; РЕД ОС;

Альт 8 СП, PostgresPro Enterprise Certified

ЗПК «1С:Предприятие 8.3z» сертифицирован
по четвертому уровню доверия
и пятому классу защищенности от несанкционированного доступа

- ЗПК может использоваться в автоматизированных системах до класса 1Г включительно — **РД АС**
- При создании государственных информационных систем до первого класса защищенности — **Приказ ФСТЭК от 2013г № 17**
- В информационных системах персональных данных до первого уровня защищенности персональных данных включительно — **Приказ ФСТЭК от 2013г № 21**
- На объектах критической информационной инфраструктуры до первой категории значимости включительно — **Приказ ФСТЭК от 2017г № 239**

Информация http://1c.ru/news/info.jsp?id=21439

Текущая версия 8.3.21.1676 https://1c.ru/news/info.jsp?id=30166

Продление и переоформление сертификата соответствия

Сертификат продлен до 02.09.2023

переоформлен по 4 уровню доверия в 2021 году

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 3442

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
2 сентября 2015 г.

Выдан: 2 сентября 2015 г. Переоформлен: 12 мая 2021 г.
Действителен до: 2 сентября 2018 г.
Срок действия продлён до: 2 сентября 2023 г.

Настоящий сертификат удостоверяет, что **защищенный программный комплекс «1С:Предприятие, версия 8.3z»** (партия из 10000 (десяти тысяч) экземпляров продукции с серийными номерами с 801695000 по 801699999, с 801705000 по 801709999, маркированных знаками соответствия с № К605432 по № К615431), разработанный и производимый ООО «Научно-производственный центр «1С», является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 5 классу защищенности при выполнении указаний по эксплуатации, приведенных в формуляре 46.1С.506190-83-01 30 01.

https://static.1c.ru/rus/products/serts/sert83.jpg

Признаётся в системе сертификации МО РФ (для «несекретного» ПО)

Информация о выпуске https://1c.ru/news/info.jsp?id=28391

Неявные меры обеспечения безопасности информации

Очистка внешней памяти только в ЗПК «1С:Предприятие 8.3z»

- **ЗИС.21** - очистка внешней памяти методом перезаписи уничтожаемых (стираемых) файлов случайной битовой последовательностью;
- **АНЗ.5** - Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе;
- **ОПС.2** - Управление установкой (инсталляцией) компонентов программного обеспечения;

Реализуются только средствами операционной системы и/или наложенных СЗИ

- УПД.13 - Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
- ЗИС.15 - Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных

Рекомендации по взаимодействию с СЗИ

При реализации мер АВЗ.1, УПД.3 и ЗИС.17 в части предоставления доступа к объектам информационной системы следует учитывать

Порты процессов «1С:Предприятия» по умолчанию:

- порты клиента тестирования (**1cv8**) – 1538:1539
- порт агента кластера (**ragent**) - 1540
- порт главного менеджера кластера (**rmngr**) – 1541;
- рабочий порт сервера хранилища конфигурации (**crserver**) – 1542;
- порт агента конфигуратора (**1cv8**) – 1543;
- диапазон сетевых портов динамического выбора (**rphost**) – 1560:1591;
- порт, по которому утилита администрирования (**rac**) будет взаимодействовать с сервером администрирования (**ras**) - 1545
- при запуске в отладочном режиме с использованием протокола HTTP, сервер отладки использует порт 1550
- порт автономного сервера (**ibsrv**) – 8314
- порт автономного сервера при доступе по SSH - 8282
- пользователь, от имени которого выполняется сервис сервера «1С:Предприятия» (в среде ОС Linux), – usr1cv8
- а также порт PostgreSQL - 5432

Документация: https://its.1c.ru/db/v8317doc#bookmark:cs:TI000000116
https://its.1c.ru/db/v8317doc#bookmark:adm:TI000000360

Поиск уязвимостей

ВНИМАНИЕ!

При реализации меры АН3.1 «Выявление и анализ уязвимостей» следует учитывать:

- Не ищите уязвимости в коде конфигураций сторонними средствами!
- Средств поиска уязвимостей, умеющих анализировать встроенный язык «1С:Предприятия» в природе не существует
- Имеющиеся на рынке программные продукты, «умеющие» искать уязвимости в конфигурациях Фирмой «1С» не поддерживаются
- Продукт «1С:Автоматизированная проверка конфигураций» Предназначен для проверок *на соответствие стандартам и иным требованиям технического характера* *https://v8.1c.ru/acc/*

Работа со сведениями, составляющими государственную тайну

Сертификация в системе сертификации ФСТЭК России

Фирмой «1С» успешно завершены сертификационные испытания Защищенного программного комплекса «1С:Предприятие 8s»

(ЗПК «1С:Предприятие 8s»)
по требованиям безопасности информации

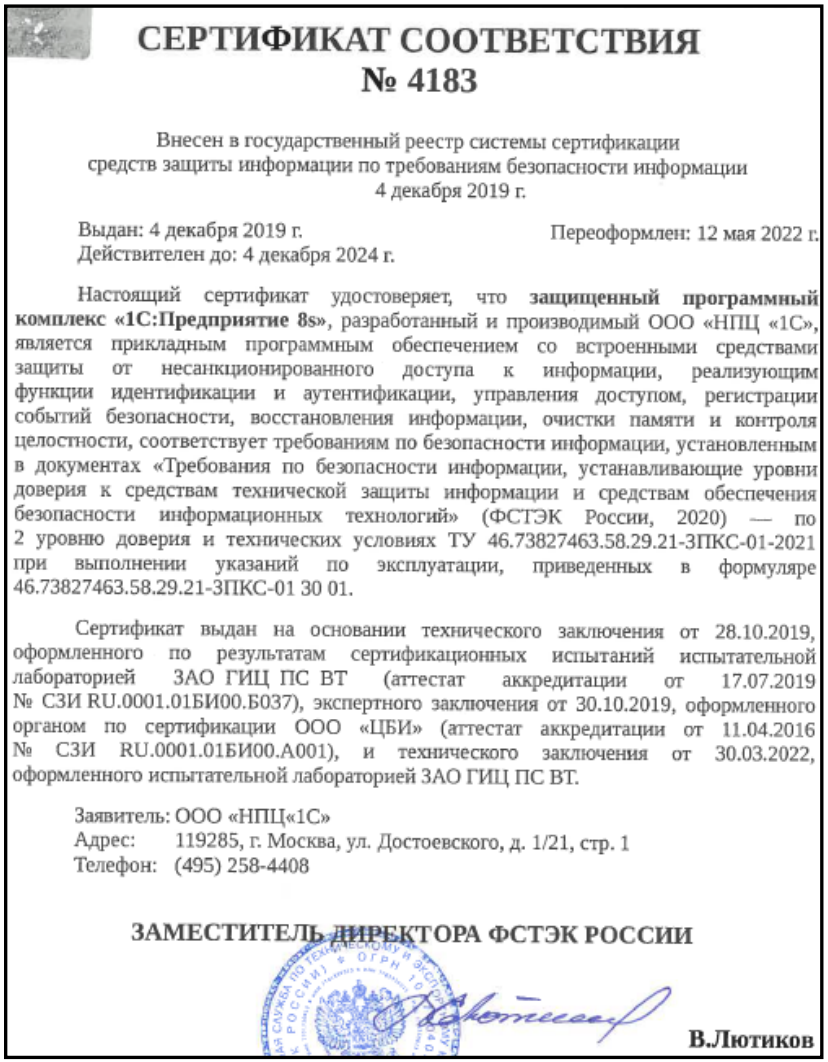
- Сертификат соответствия ФСТЭК России от 04.12.2019 № 4183
- переоформлен 12.05.2022
- 2 уровень уровень доверия
- Технические условия в части требований 3 класса защищенности от несанкционированного доступа
- Может использоваться в автоматизированных системах, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну и имеющие степень секретности не выше «совершенно секретно»
- Среда исполнения – ОС СН Astra Linux Special Edition 1.6
- Используемая СУБД – PostgreSQL 9.6 из состава ОС СН Astra Linux Special Edition 1.6

Информационное письмо № 26662 https://1c.ru/news/info.jsp?id=26662

Требования защищенности от НСД

ТУ 46.73827463.58.29.21-ЗПКС-01-2017

- **Мандатный принцип контроля доступа**
- Ролевой принцип контроля доступа
- Очистка памяти в части очистки внешней памяти
- Идентификация и аутентификация
- Регистрация
- Надежное восстановление
- Контроли целостности КСЗ



СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4183

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
4 декабря 2019 г.

Выдан: 4 декабря 2019 г. Переоформлен: 12 мая 2022 г.
Действителен до: 4 декабря 2024 г.

Настоящий сертификат удостоверяет, что **защищенный программный комплекс «1С:Предприятие 8s»**, разработанный и производимый ООО «НПЦ «1С», является прикладным программным обеспечением со встроенными средствами защиты от несанкционированного доступа к информации, реализующим функции идентификации и аутентификации, управления доступом, регистрации событий безопасности, восстановления информации, очистки памяти и контроля целостности, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) — по 2 уровню доверия и технических условиях ТУ 46.73827463.58.29.21-ЗПКС-01-2021 при выполнении указаний по эксплуатации, приведенных в формуляре 46.73827463.58.29.21-ЗПКС-01 30 01.

Сертификат выдан на основании технического заключения от 28.10.2019, оформленного по результатам сертификационных испытаний испытательной лабораторией ЗАО ГИЦ ПС ВТ (аттестат аккредитации от 17.07.2019 № СЗИ RU.0001.01БИ00.Б037), экспертного заключения от 30.10.2019, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001), и технического заключения от 30.03.2022, оформленного испытательной лабораторией ЗАО ГИЦ ПС ВТ.

Заявитель: ООО «НПЦ«1С»
Адрес: 119285, г. Москва, ул. Достоевского, д. 1/21, стр. 1
Телефон: (495) 258-4408

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Текущая версия 8.3.19.1405 http://1c.ru/news/info.jsp?id=29493

Сертификация в системе МО РФ. Технологическая платформа

Фирмой «1С» успешно завершены сертификационные испытания Комплекта компонент технологической платформы «1С:Предприятие 8»

(ККТП «1С:Предприятие 8» ШАРД.10002-02) по требованиям безопасности информации

- Сертификат соответствия МО РФ от 16.09.2019 № 4448
- 2-НДВ и 3-СВТ в части касающейся
- Может использоваться в автоматизированных системах, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну и имеющие степень секретности не выше «совершенно секретно»
- Среда исполнения – ОС СН Astra Linux Special Edition 1.6
- Используемая СУБД – PostgreSQL 9.6 из состава ОС СН Astra Linux Special Edition 1.6

Информация о сертификате по письменному запросу

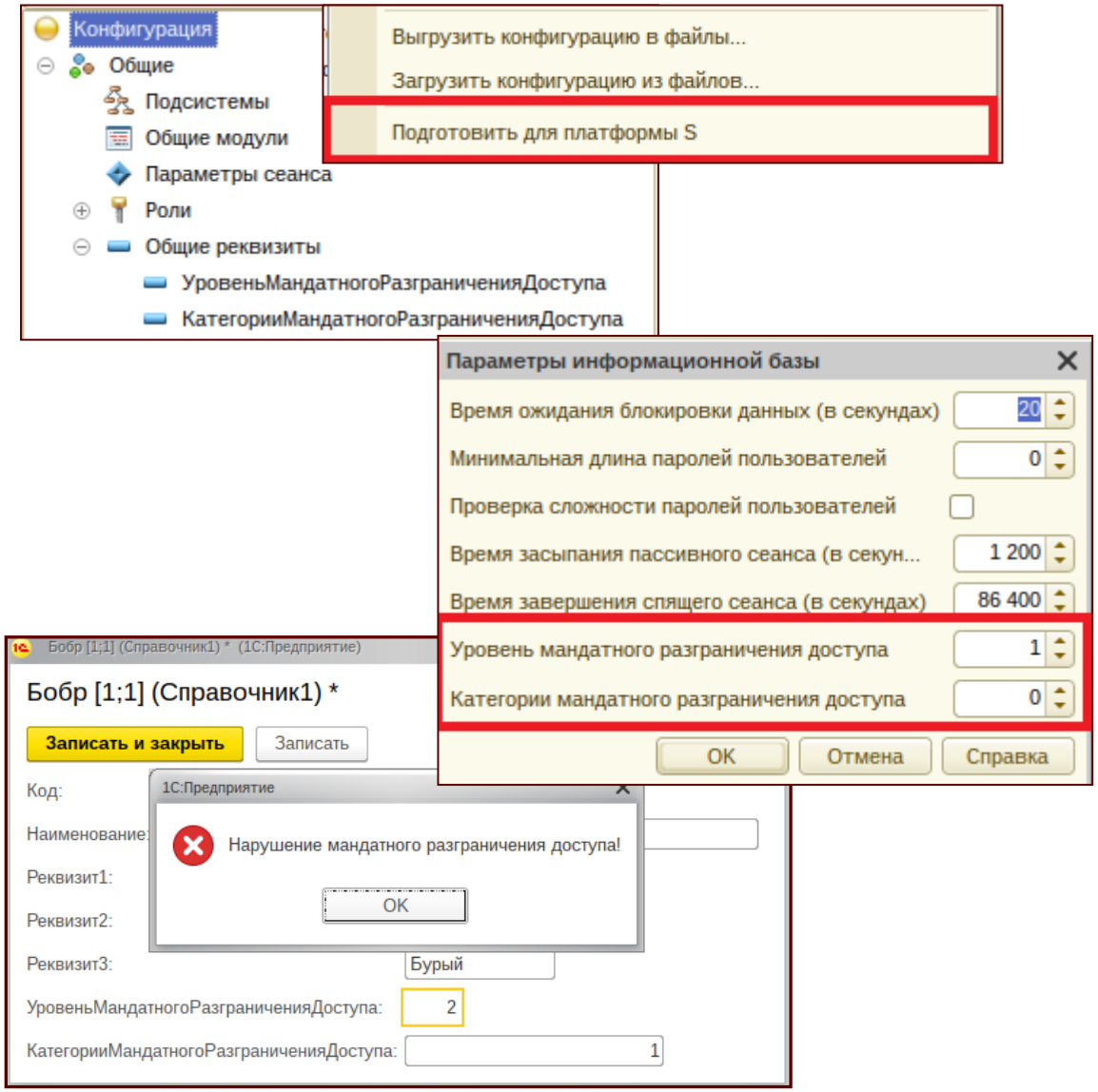
Системные особенности и соответствие требованиям нормативных актов

- Мандатное разграничение доступа по модели системы военных сообщений
- Соответствует требованиям пункта 2.4.2 ➔2.5.2 РД СВТ
- НЕ модель Белла – Лападулы
- НЕ модель Биба
- НЕ ИСПОЛЬЗУЕТ мандатные механизмы PostgreSQL из состава Astra Linux Special Edition, но требует «включения» PostgreSQL в мандатный режим
- Взаимодействует с мандатными механизмами Astra Linux Special Edition

класс защищенности 2А по приказу № 025 = класс защищенности 1Б по РД АС

Функциональные отличия

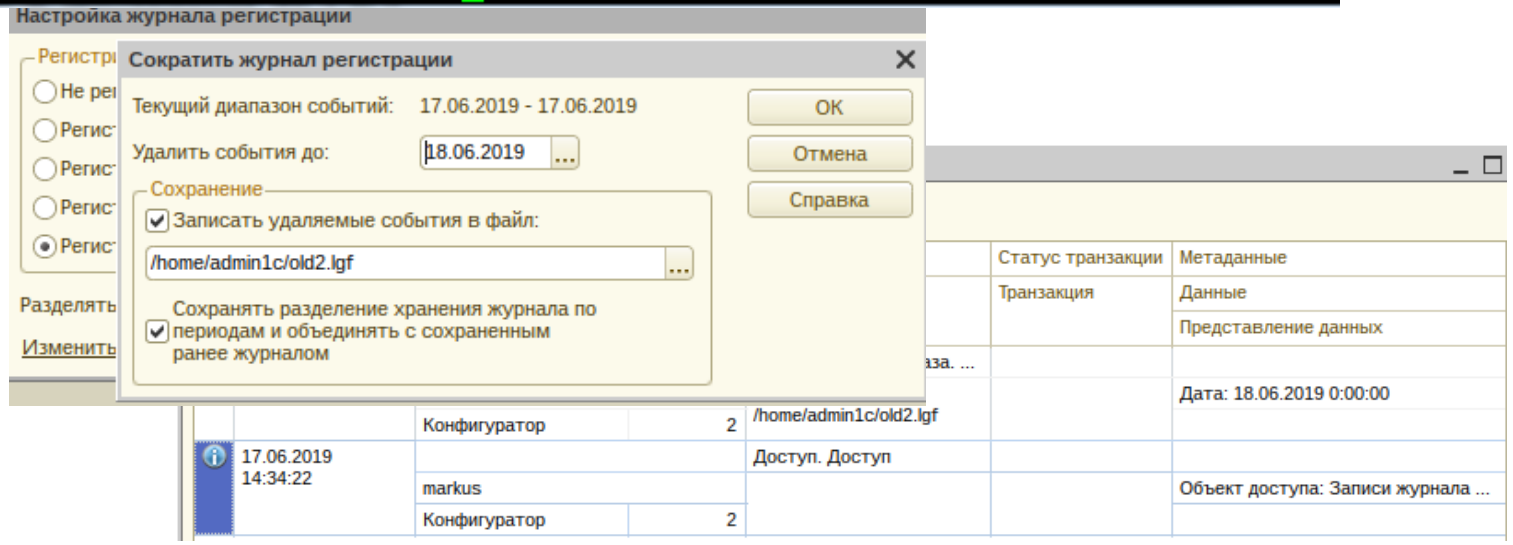
- Наличие обязательных общих реквизитов
- Новые параметры информационной базы
- Запрет толстого клиента для пользователей (разрешено только администратору)
- «Нет чтения вверх, нет записи вниз».



Очистка внешней памяти

Требование: Очистка внешней памяти должна производиться путем записи маскирующей информации в память при ее освобождении (перераспределении)

```
root@markus:/home/markus#grep -a -R "T.r.a.v.o.y.a.d" testpam2
root@markus:/home/markus#grep -a -R "Frog" testpam2
{"R",21:138c080027b98c6111e990f04b294e1c},"Frog",0,0,0,4,0,
{"R",21:138c080027b98c6111e990f04b294e1c},"Frog",0,0,0,2,0,
{"R",21:138c080027b98c6111e990f04b294e1c},"Frog",0,0,0,2,0,
root@markus:/home/markus#grep -a -R "F.r.o.g" testpam2
root@markus:/home/markus#
```

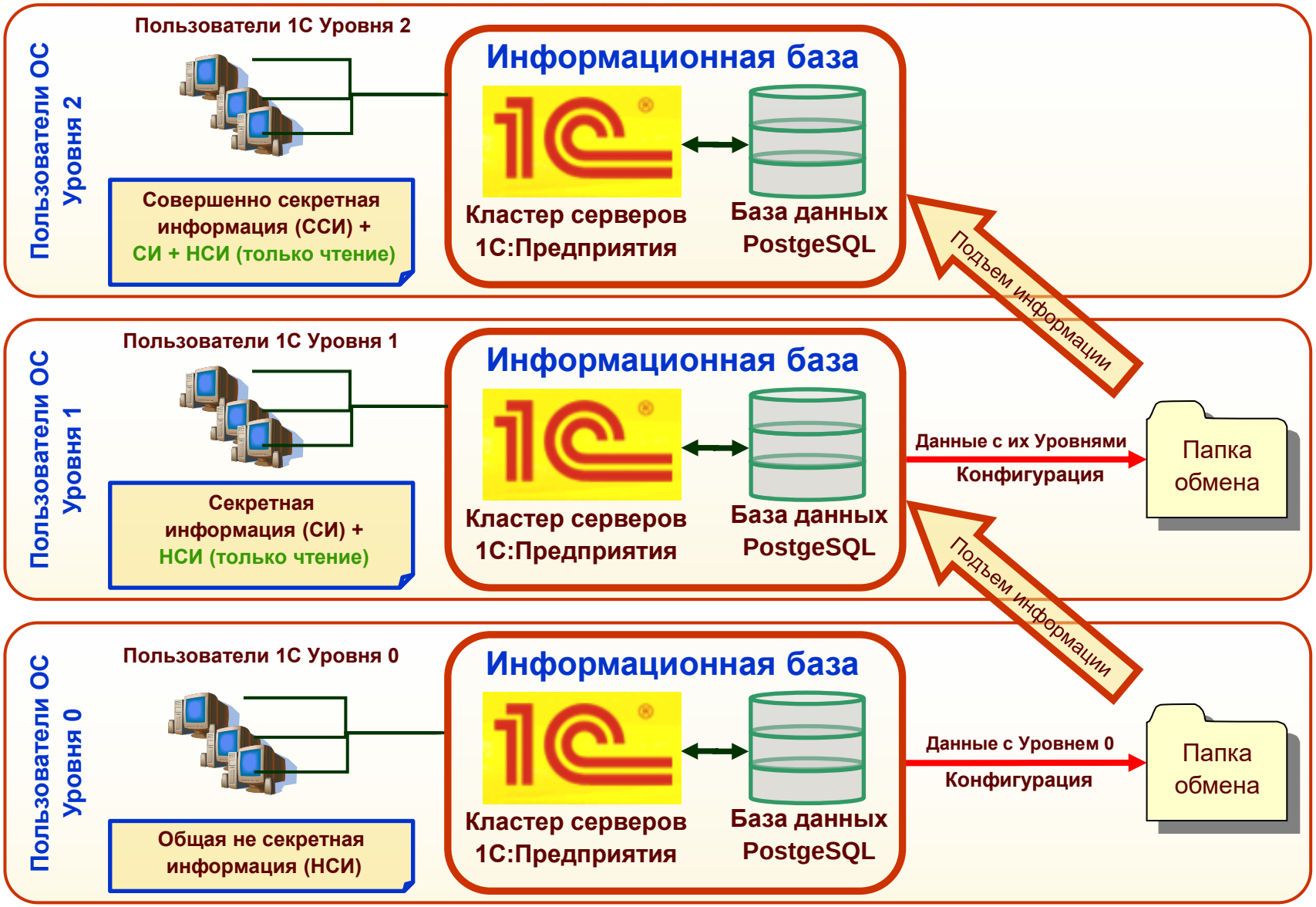


Реализация: При удалении область на жестком диске забивается нулями.
Усиление: Факты принудительной очистки памяти регистрируются

Как работает

ЗПК «1С:Предприятие 8s»

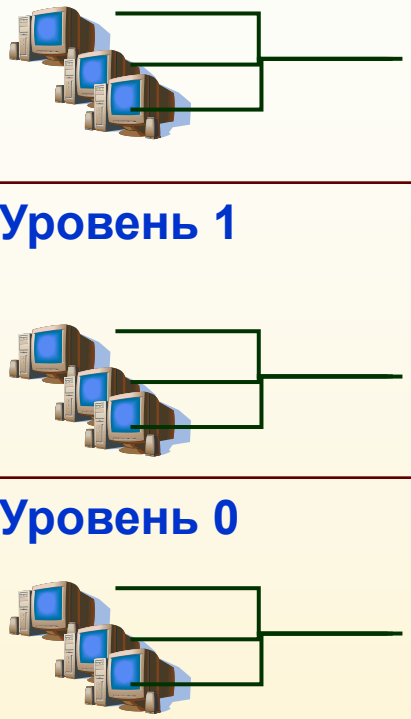
Разделение информации по уровням конфиденциальности



Реализация мандатной матрицы доступа

Операционная система Astra Linux Special Edition

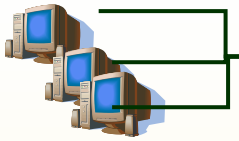
Уровни доступа	Категория 1	Категория 2	Категория 1+2
Уровень 2	ИБ 2.1	ИБ 2.2	
Уровень 1	ИБ 1.1	ИБ 1.2	ИБ 1.(1+2)
Уровень 0	ИБ 0.1	ИБ 0.2	



Изменение уровня конфиденциальности

Пользователи ОС Уровня 2

Пользователи 1С Уровня 2



Совершенно секретная информация (ССИ) + СИ + НСИ (только чтение)

Информационная база

Кластер серверов 1С:Предприятия

База данных PostgeSQL

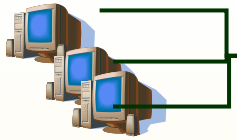
Операция понижения уровня доступа

XML

В выгружаемых данных сохраняются их уникальные идентификаторы и принудительно понижается уровень доступа

Пользователи ОС Уровня 1

Пользователи 1С Уровня 1



Секретная информация (СИ) + НСИ (только чтение)

Информационная база

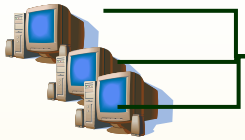
Кластер серверов 1С:Предприятия

База данных PostgeSQL

При загрузке данных с уже существующим уникальным идентификатором, уровень доступа меняется на значение из загружаемых данных снизу.

Пользователи ОС Уровня 0

Пользователи 1С Уровня 0



Общая не секретная информация (НСИ)

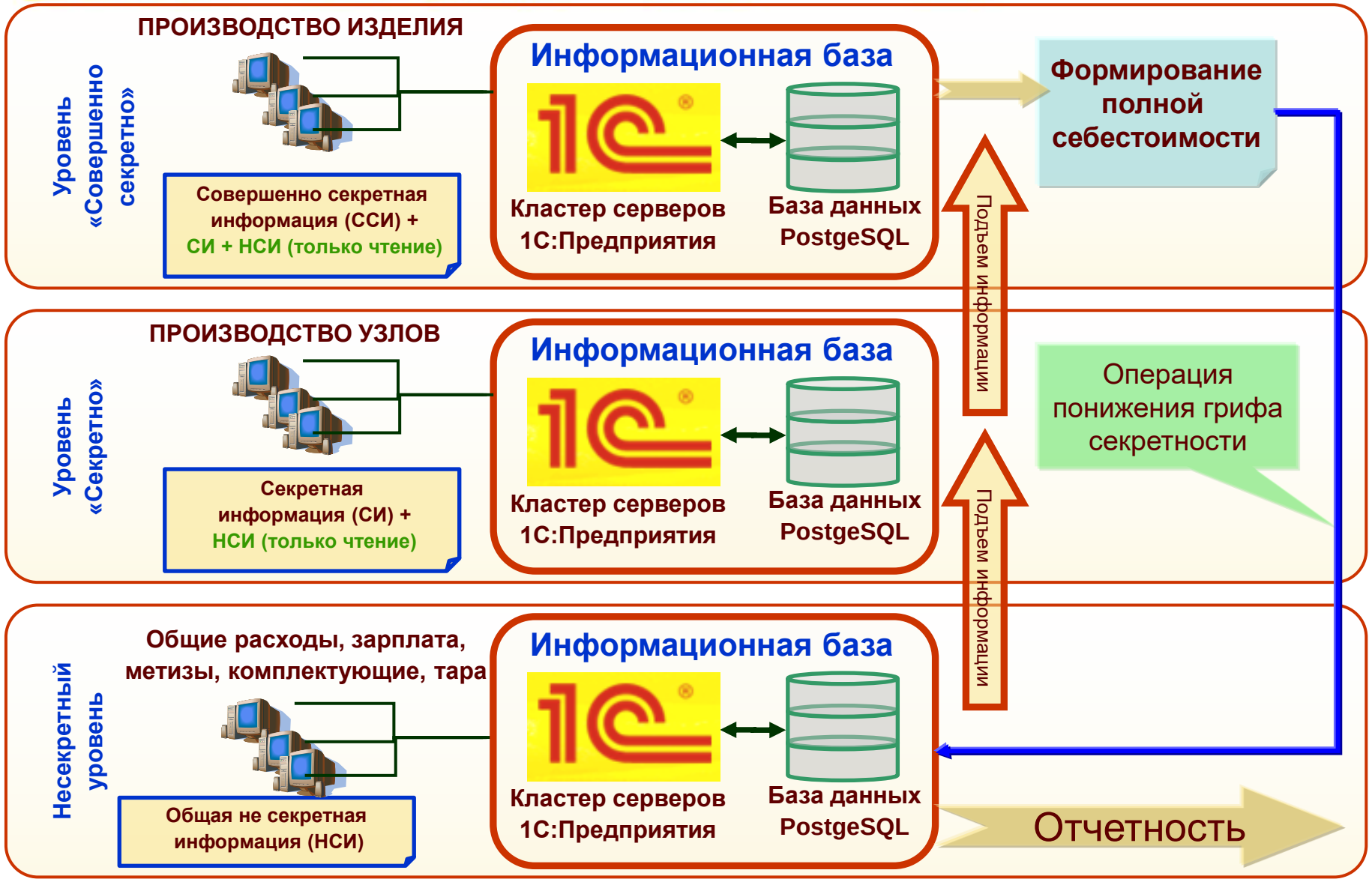
Информационная база

Кластер серверов 1С:Предприятия

База данных PostgeSQL

При изменении уровня вверх, данные принудительно удаляются после проведенного обмена

Пример машиностроительного предприятия



Что делать

- Настраивать строго по Руководству администратора и по Руководству по КСЗ
- Разработку вести изначально в Linux, а лучше в NFR-версии продукта и на Astra Linux Special Edition
- Рекомендуется предварительно договориться о встрече на Селезневской 21 и посмотреть, как работает продукт

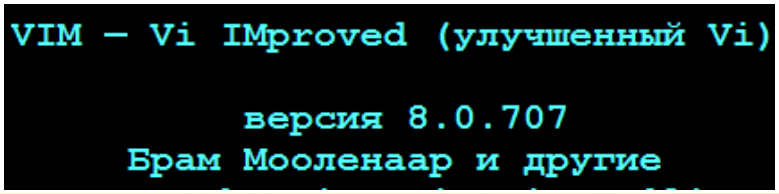
ВАЖНО!

Конфигурация открытого (несекретного) контура

может быть НЕ РАВНА конфигурации закрытого (секретного) контура

Это надо учитывать при проектировании информационной системы

Надо изучать Linux и Vim пророк его ☺



Что делать нельзя

ВНИМАНИЕ!

Нельзя работать на красном экране. Экран должен быть синим

- Нельзя работать в закрытых контурах не имея соответствующих лицензий, допусков и договоров
- Нельзя добавлять запрещенную функциональность ➔ Java, сторонние deb-пакеты не из Astra Linux Special Edition
- Нельзя настраивать ЗПК «1С:Предприятие 8s» в обход требований формуляра и Руководства по КСЗ ➔ применять аппаратную защиту от нелегального копирования; публиковать на веб-серверах; вносить изменения нештатными средствами.
- Нельзя применять режим привилегированного сокета!

Всё вышеуказанное делать запрещено даже по требованиям заказчика

Работа с иностранными компаниями

GDPR
великий и ужасный

- Общий регламент по защите данных (англ. General Data Protection Regulation, GDPR) (Постановление (Европейский союз) 2016/679) — это Постановление, с помощью которого Европейский парламент, Совет Европейского союза и Европейская комиссия усиливают и унифицируют защиту персональных данных всех лиц в Европейском союзе (ЕС). Постановление также направлено на экспорт данных из ЕС.
- Вступил в силу с 25.05.2018
- **Требований к программному обеспечению не предъявляет**

Требования GDPR к российским предприятиям

- GDPR действует только на территории ЕС
- Если персональные данные гражданина ЕС обрабатываются в ИСПДн российских предприятий, то руководстоваться необходимо требования российского законодательства
- Если российское предприятие имеет филиал в ЕС, то под действия GDPR в большинстве случаев попадает
- Если российское предприятие обслуживает информационные системы предприятий ЕС на территории ЕС, то однозначно попадает под требования GDPR (на территории ЕС)
- Бытует страшилка о праве на забвение – но даже по законодательству ЕС данное право не всегда применимо, а в случаях, когда применимо, то не по первому звонку

ПОМНИТЕ!

Ни одно программное средство не может реализовать все требования обеспечения безопасности информации!

- Средства разграничения доступа
- Средства контроля съемных носителей;
- Средства доверенной загрузки;
- Средства антивирусной защиты;
- Средства межсетевого экранирования;
- Средства обнаружения вторжений;
- Средства защиты среды виртуализации;
- Средства анализа защищенности;
- И выполнение организационных мер!

Только комплексное применение организационных и технических мер ОБИ может гарантировать конфиденциальность, доступность и целостность защищаемой информации

Реализация мер обеспечения безопасности информации средствами «1С:Предприятие 8»

Спасибо за внимание!

Марк Суарес
Руководитель направления
suam@1c.ru