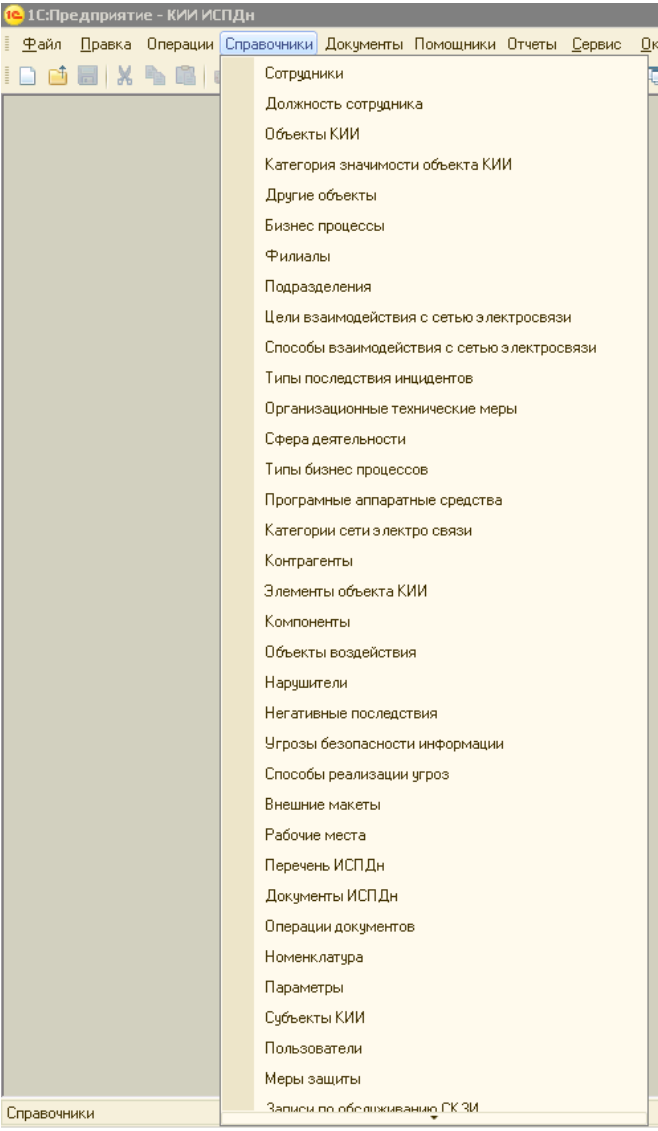
Рабочее место специалиста по информационной безопасности. КИИ ИСПДн

На базе 1С:Предприятие

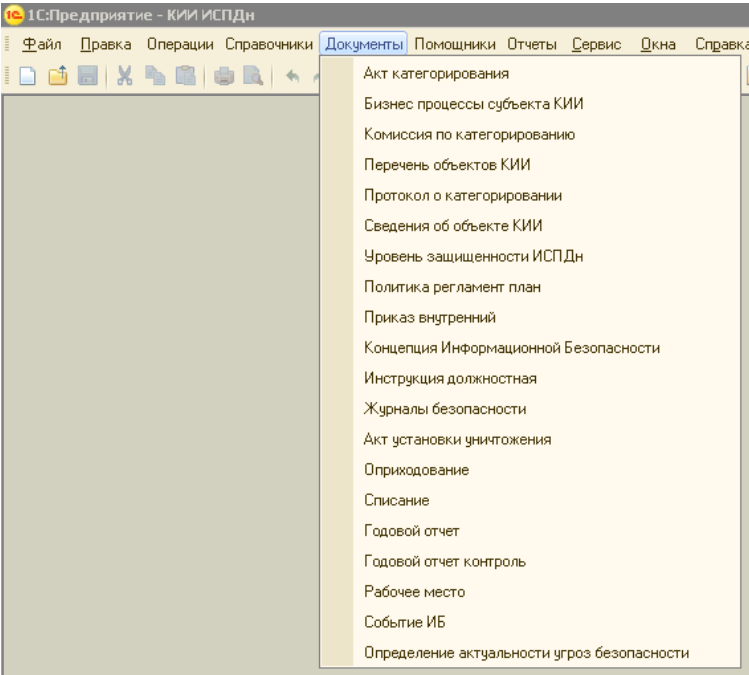
Функции программы



Хранение, подготовка, анализ информации, в том числе

- нормативная, справочная
- документы ИСПДн, КИИ
- о сотрудниках, любых лицах, имеющих доступ к ИСПДн
- об ЭЦП
- об объектах КИИ
- о бизнес процессах
- о рабочих местах
- о печатных формах, шаблонах
- о нарушителях, инцидентах
- об угрозах безопасности, способах реализации
- о негативных последствиях
- о мерах противодействия
- о сфере деятельности
- о программных, аппаратных средствах у Субъекта КИИ

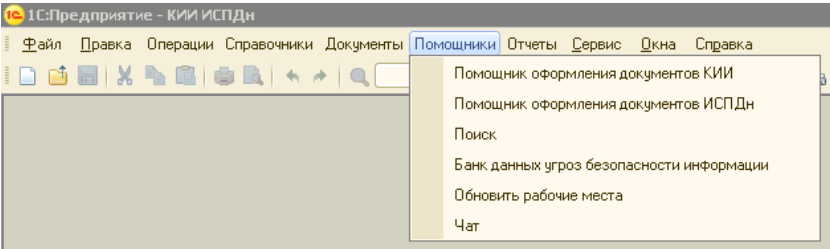
Функции программы



Создавайте на основе шаблонов документы, в том числе

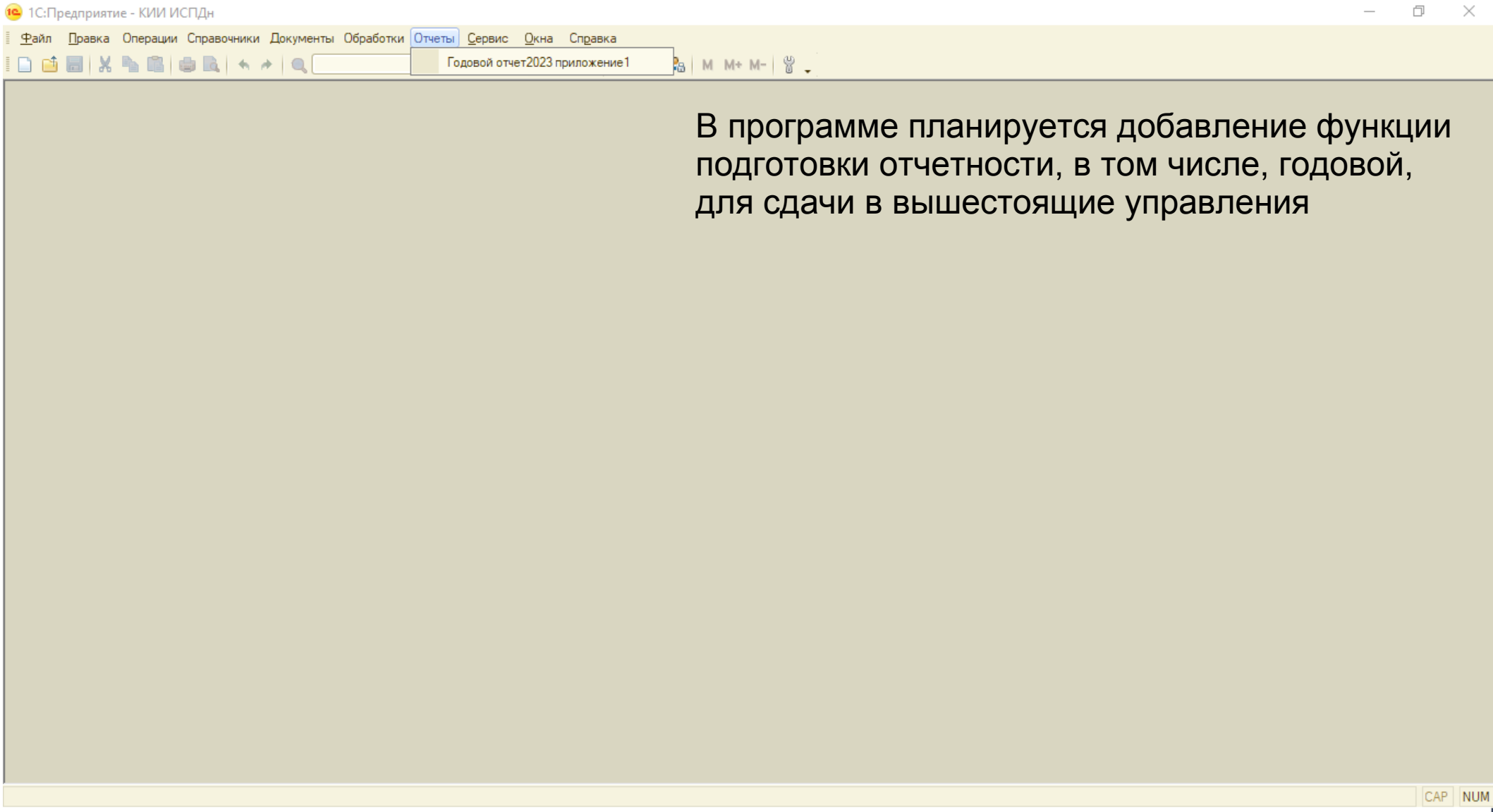
- Концепция информационной безопасности
- Приказы, инструкции в сфере ИБ
- Политики парольной защиты, управлением доступом
- Сведения об объектах КИИ
- Расчет уровня защищенности
- Протоколы, Акты категорирования
- Уровень защищенности ПДн
- Перечень объектов КИИ
- Информация о комиссии по категорированию
- Бизнес процессы субъекта КИИ
- Акты ввода в эксплуатацию СЗИ, СКЗИ
- Акты списания СЗИ, СКЗИ
- Журналы безопасности
- Приход, расход средств СЗИ

Функции программы



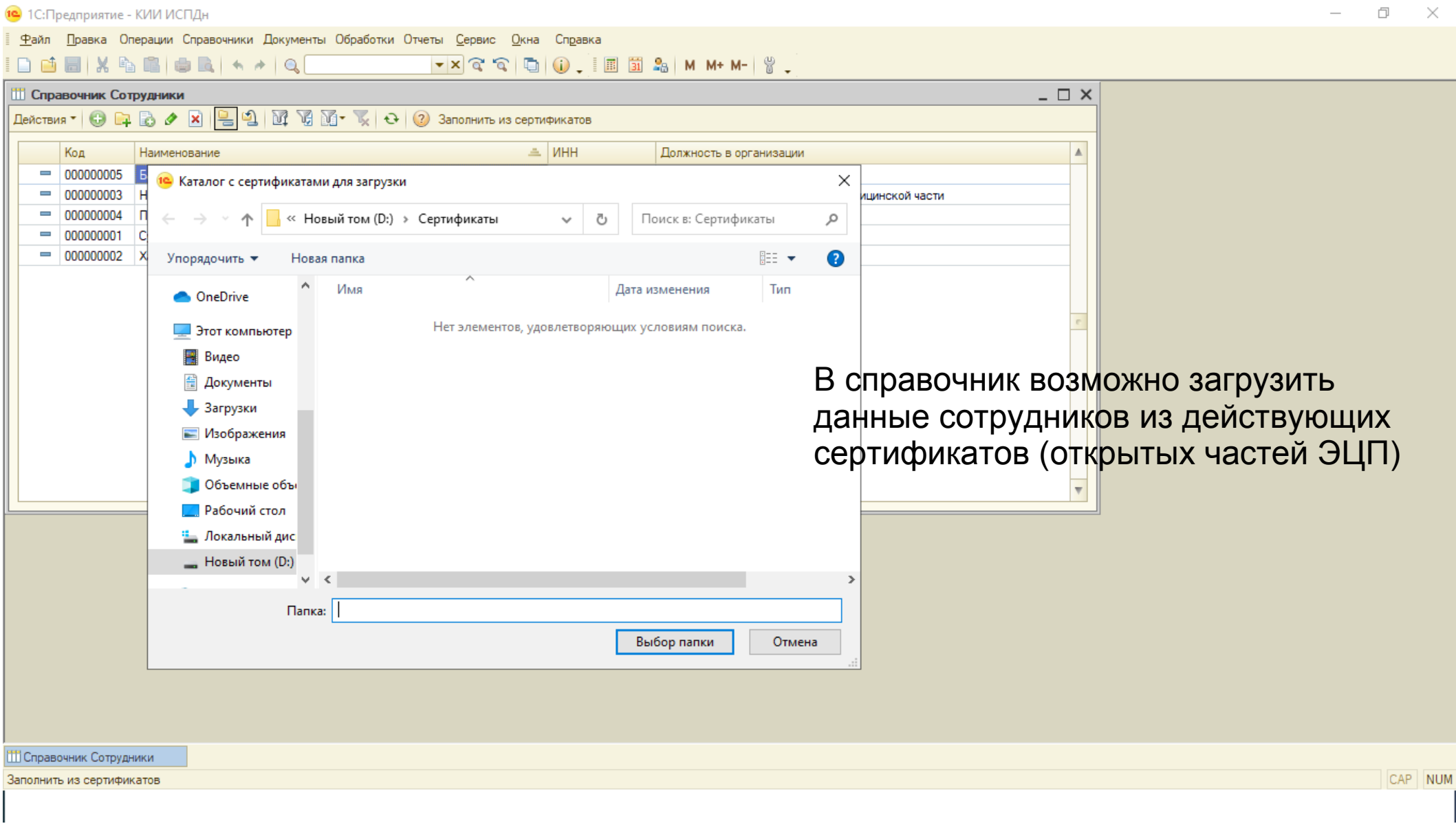
- Для подготовки пакета документов по ИСПДн и категорированию КИИ существуют помощники, которые помогают пользователю создавать документы.
- Для поиска информации в базе существует соответствующий помощник
- С сайта ФСТЕК возможно скачать Угрозы безопасности информации и загрузить их в базу
- Помощник Обновить рабочие места позволяет собирать с рабочих мест пользователей информацию об установленных ЭЦП и программных продуктах
- Чат необходим для общения между пользователями базы

Функции программы



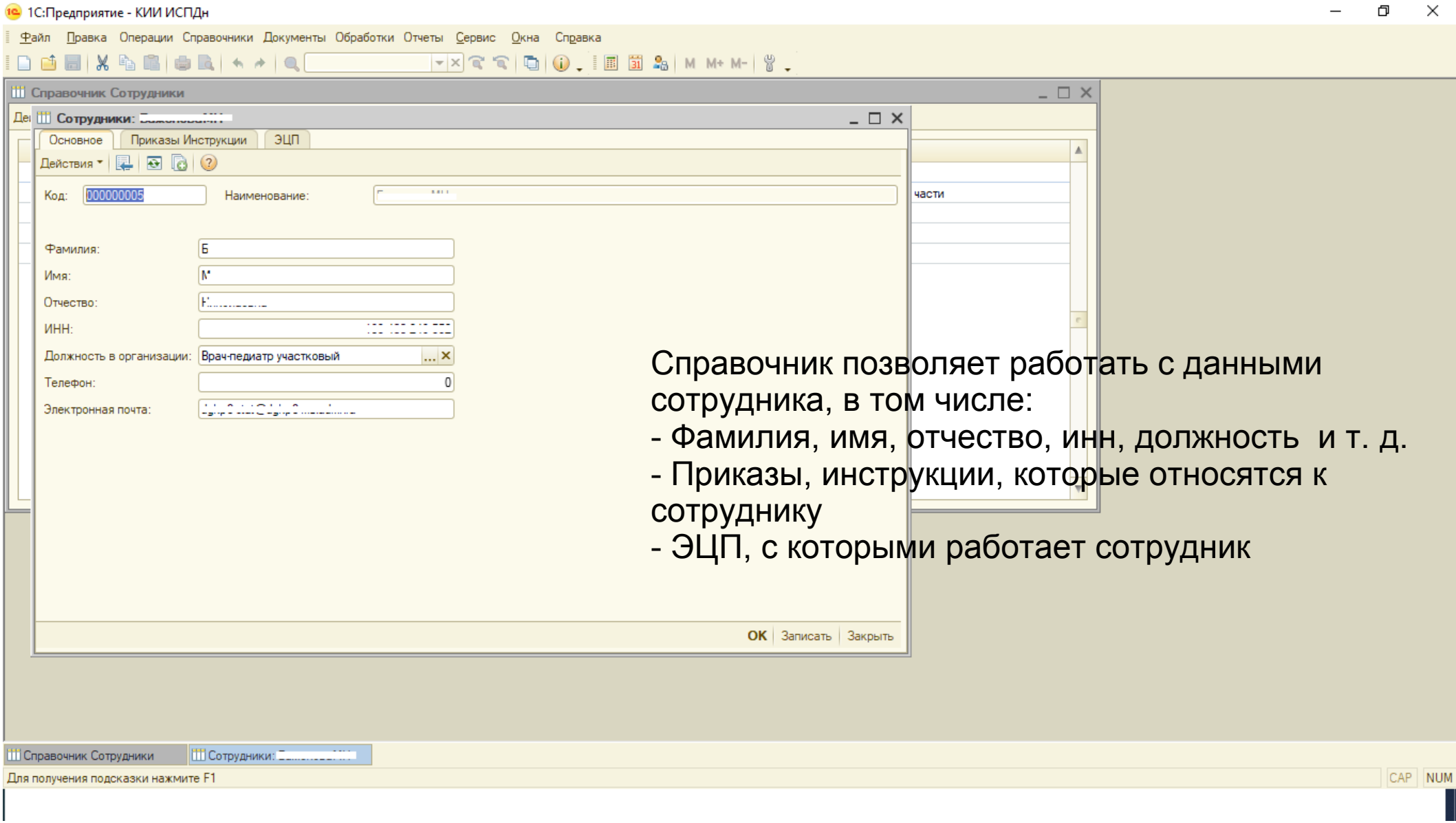
В программе планируется добавление функции подготовки отчетности, в том числе, годовой, для сдачи в вышестоящие управления

Справочник. Сотрудники



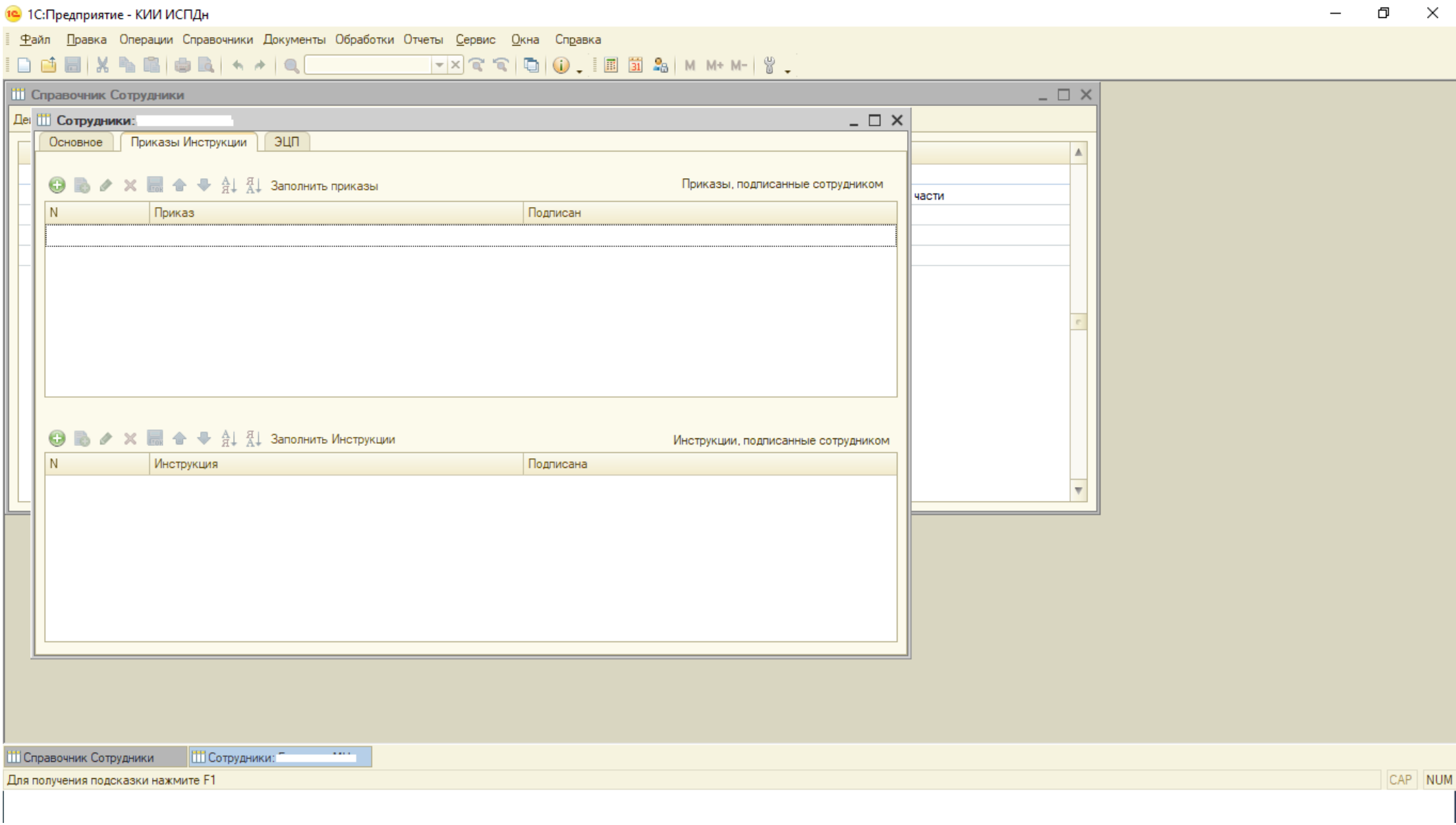
В справочник возможно загрузить данные сотрудников из действующих сертификатов (открытых частей ЭЦП)

Справочник. Сотрудники

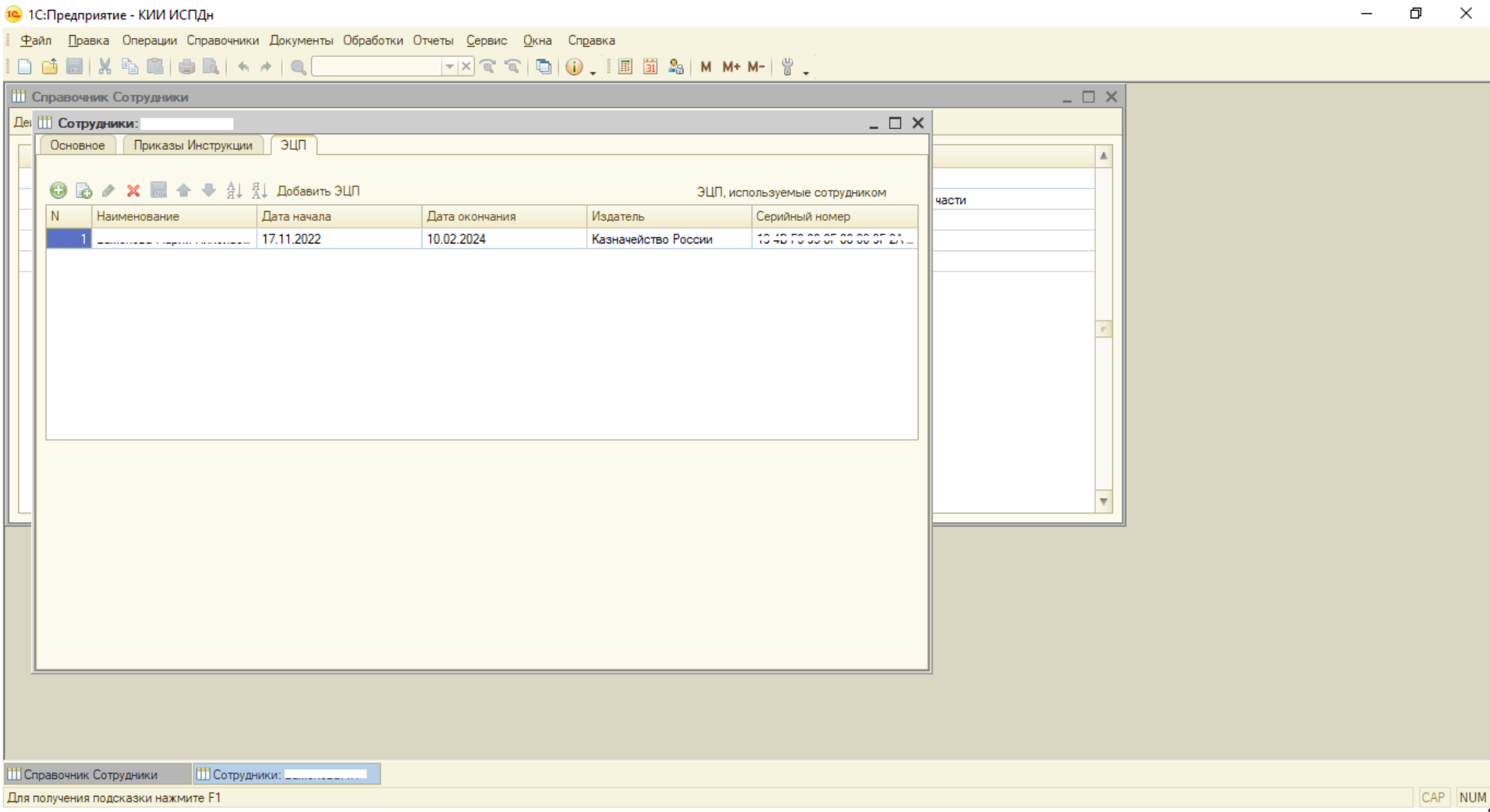


Справочник позволяет работать с данными сотрудника, в том числе:
- Фамилия, имя, отчество, инн, должность и т. д.
- Приказы, инструкции, которые относятся к сотруднику
- ЭЦП, с которыми работает сотрудник

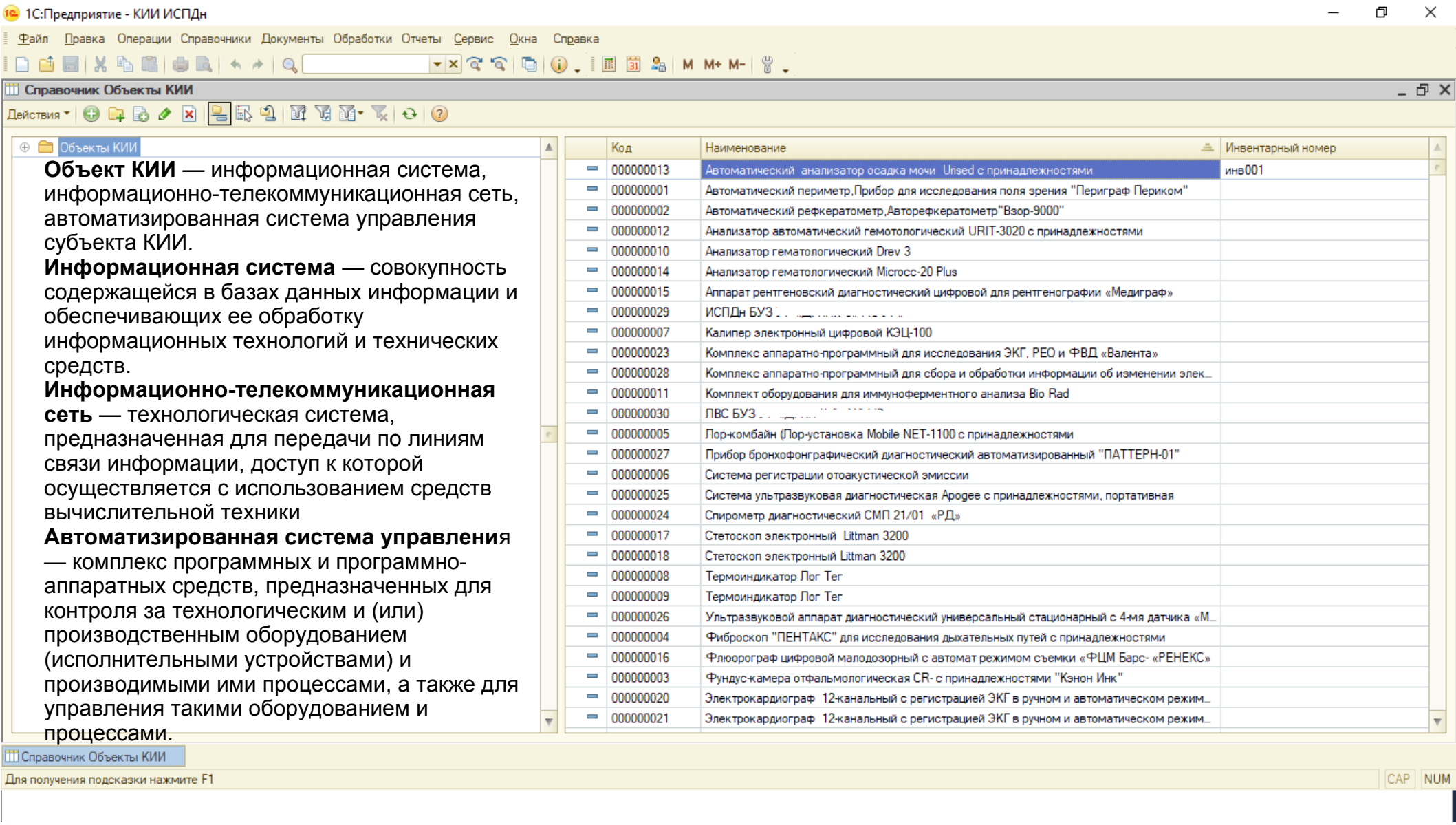
Справочник. Сотрудники



Справочник. Сотрудники



Справочник.ОбъектыКИИ



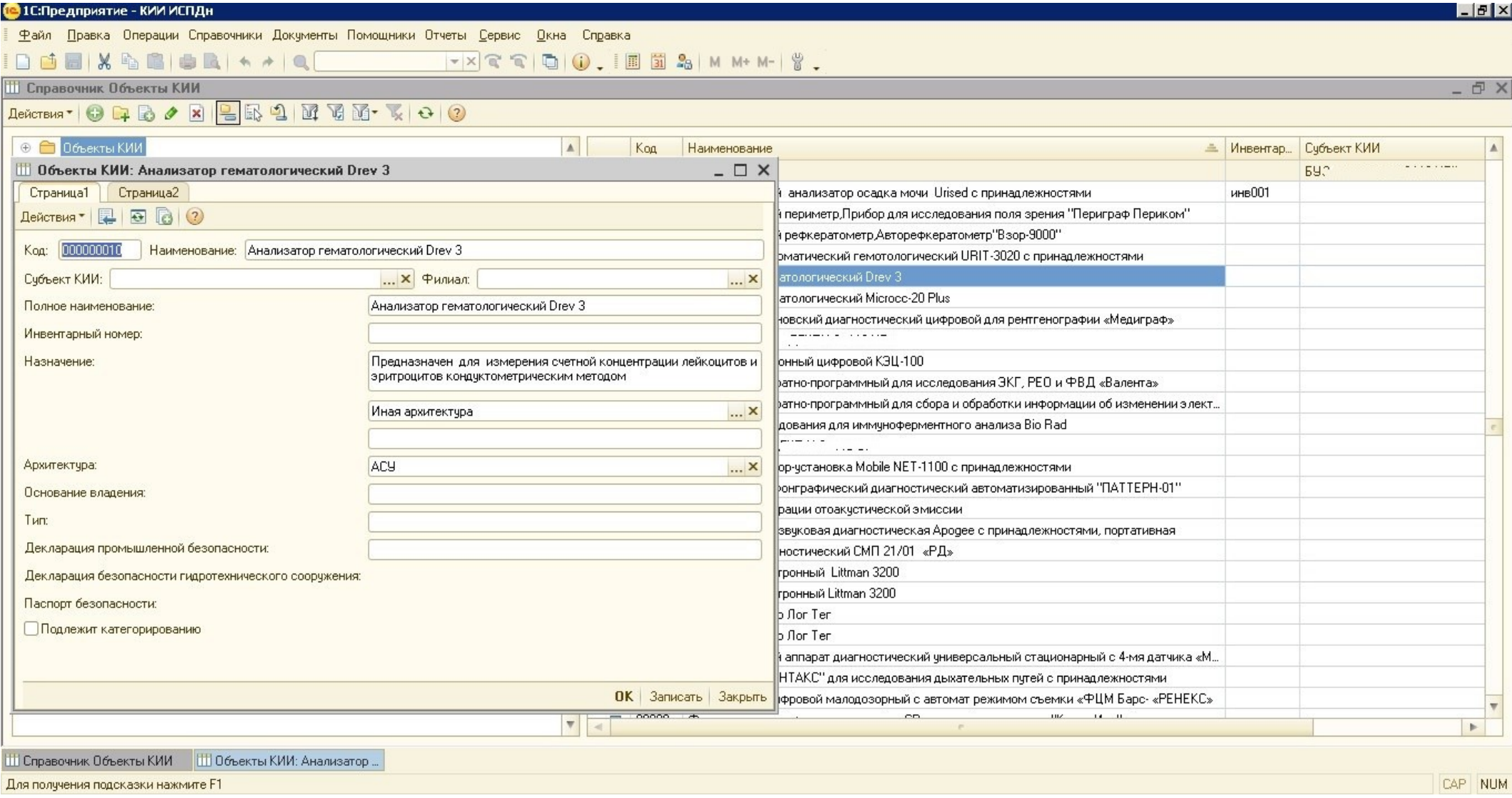
Объект КИИ — информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта КИИ.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

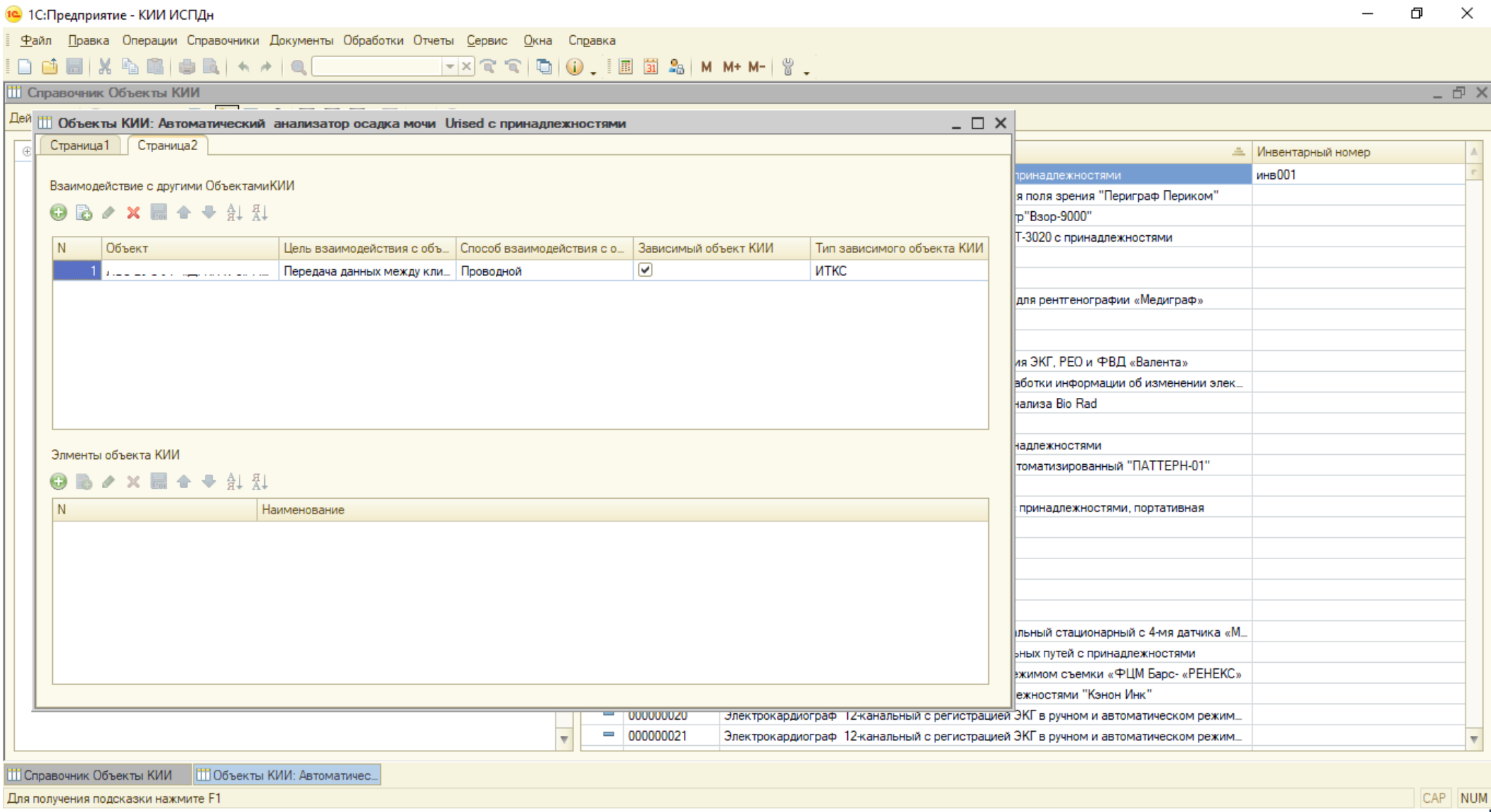
Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

Автоматизированная система управления — комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами.

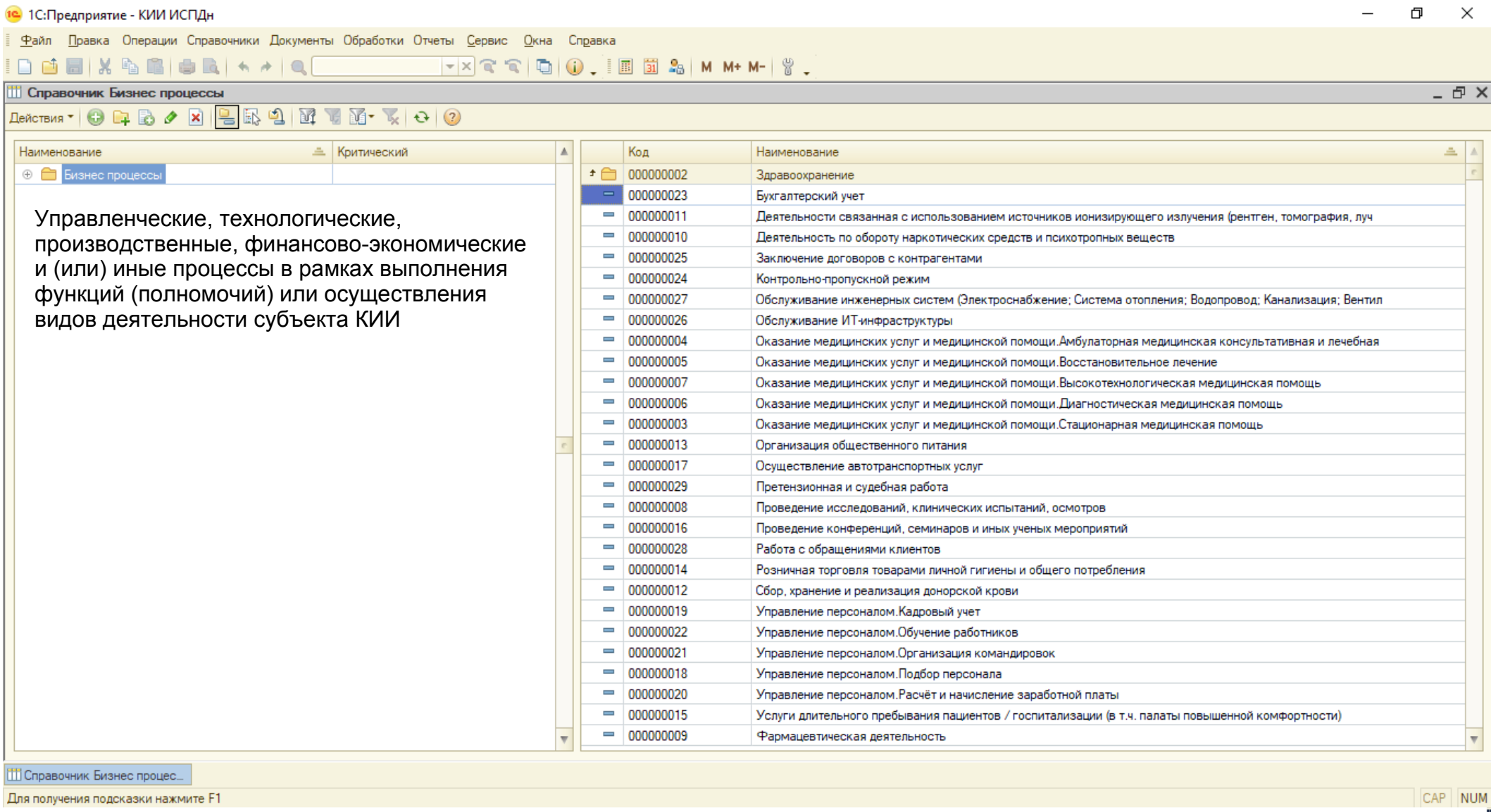
Справочник.ОбъектыКИИ



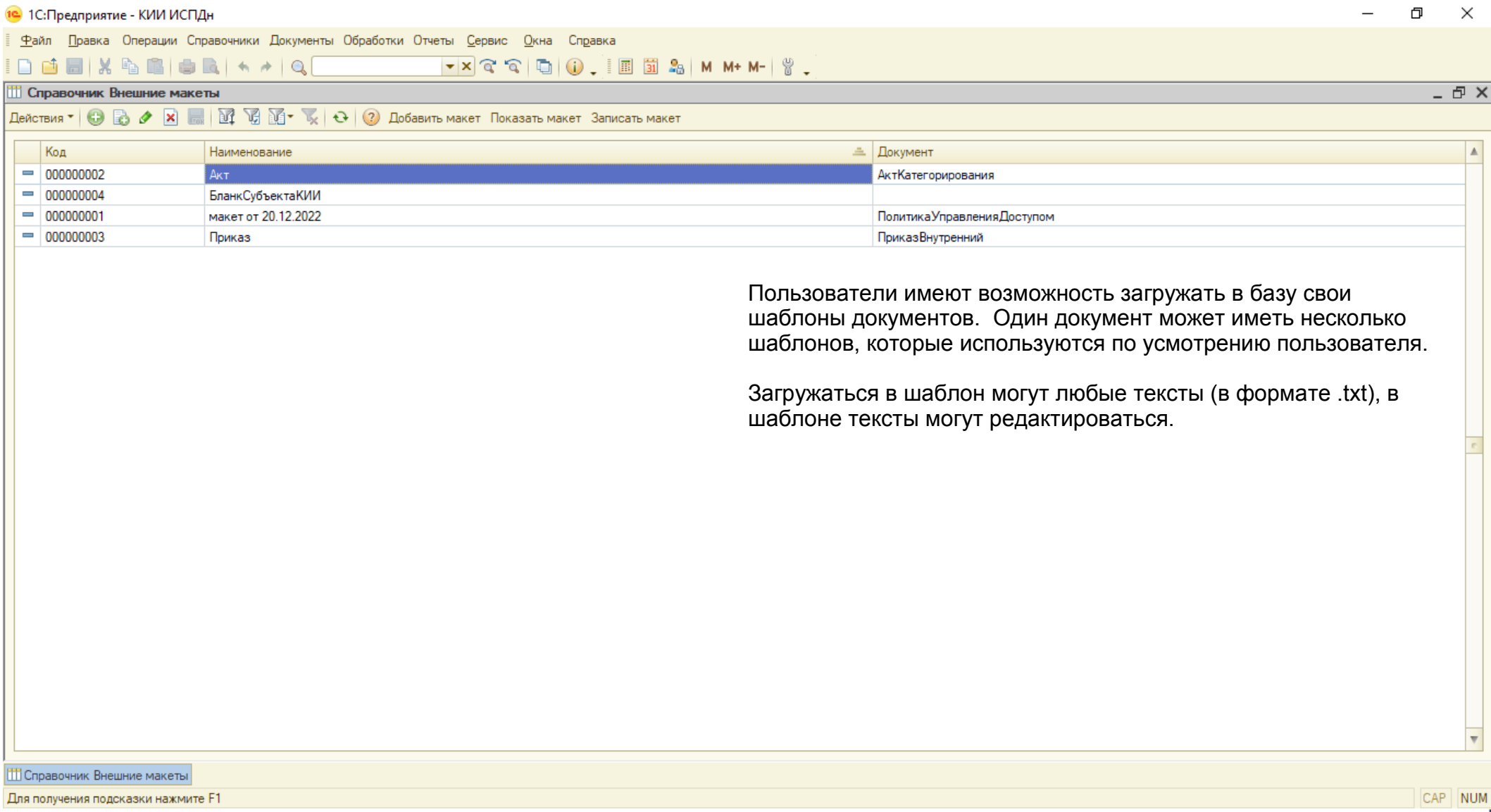
Справочник.ОбъектыКИИ



Справочник.БизнесПроцессы



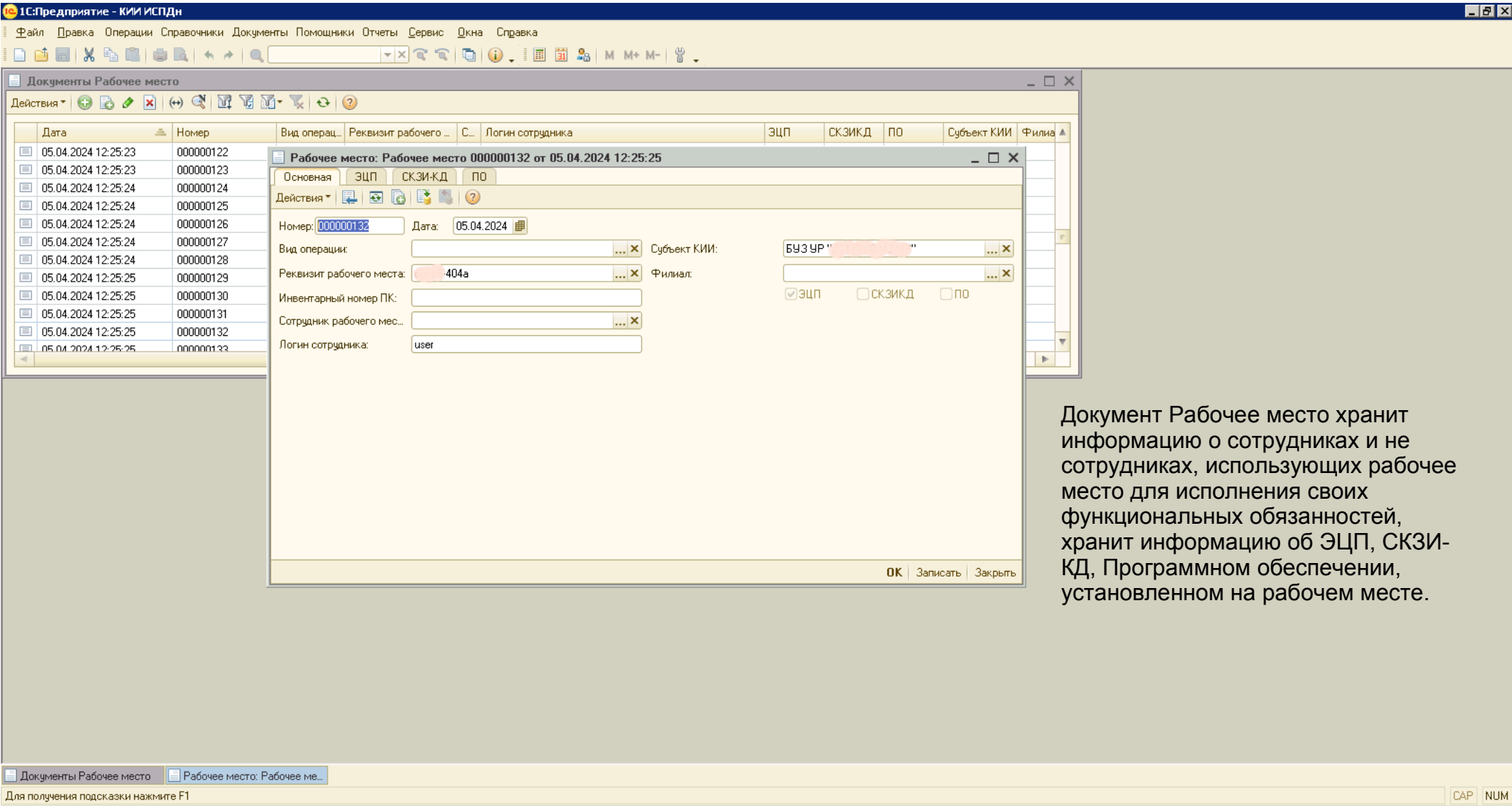
Справочник.ВнешниеМакеты



Пользователи имеют возможность загружать в базу свои шаблоны документов. Один документ может иметь несколько шаблонов, которые используются по усмотрению пользователя.

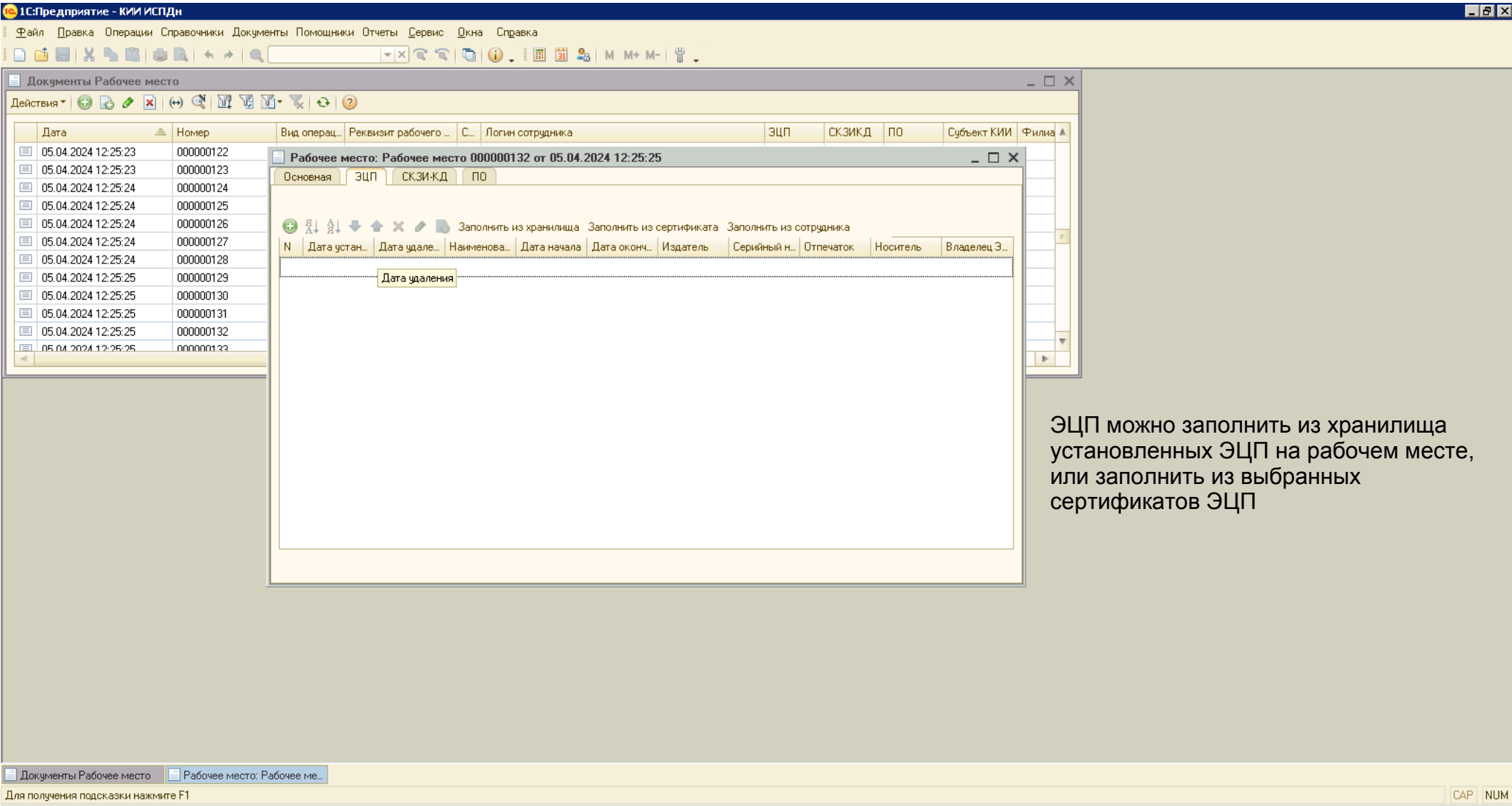
Загружаться в шаблон могут любые тексты (в формате .txt), в шаблоне тексты могут редактироваться.

Документ.РабочееМесто



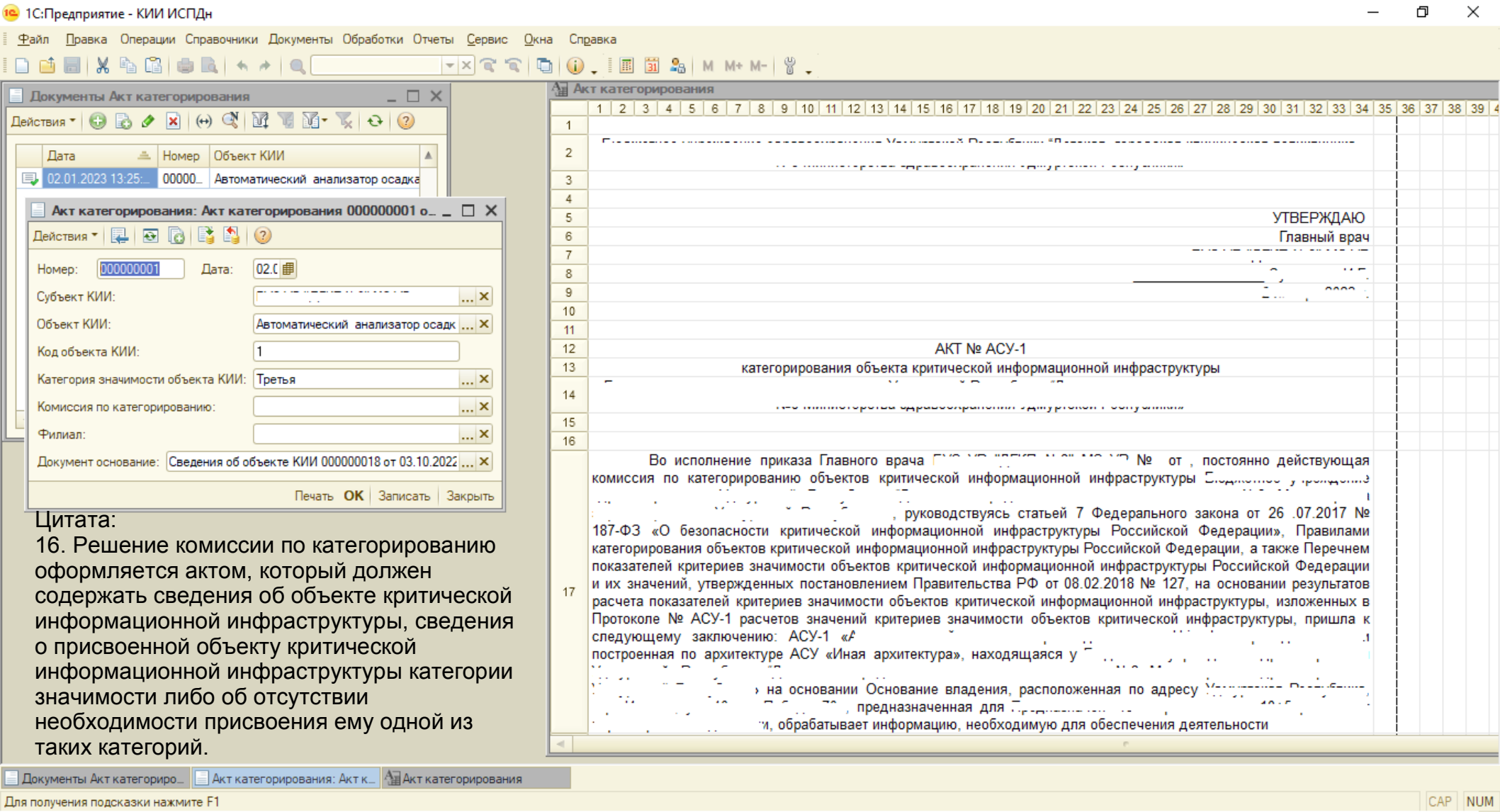
Документ Рабочее место хранит информацию о сотрудниках и не сотрудниках, использующих рабочее место для исполнения своих функциональных обязанностей, хранит информацию об ЭЦП, СКЗИ-КД, Программном обеспечении, установленном на рабочем месте.

Документ.РабочееМесто



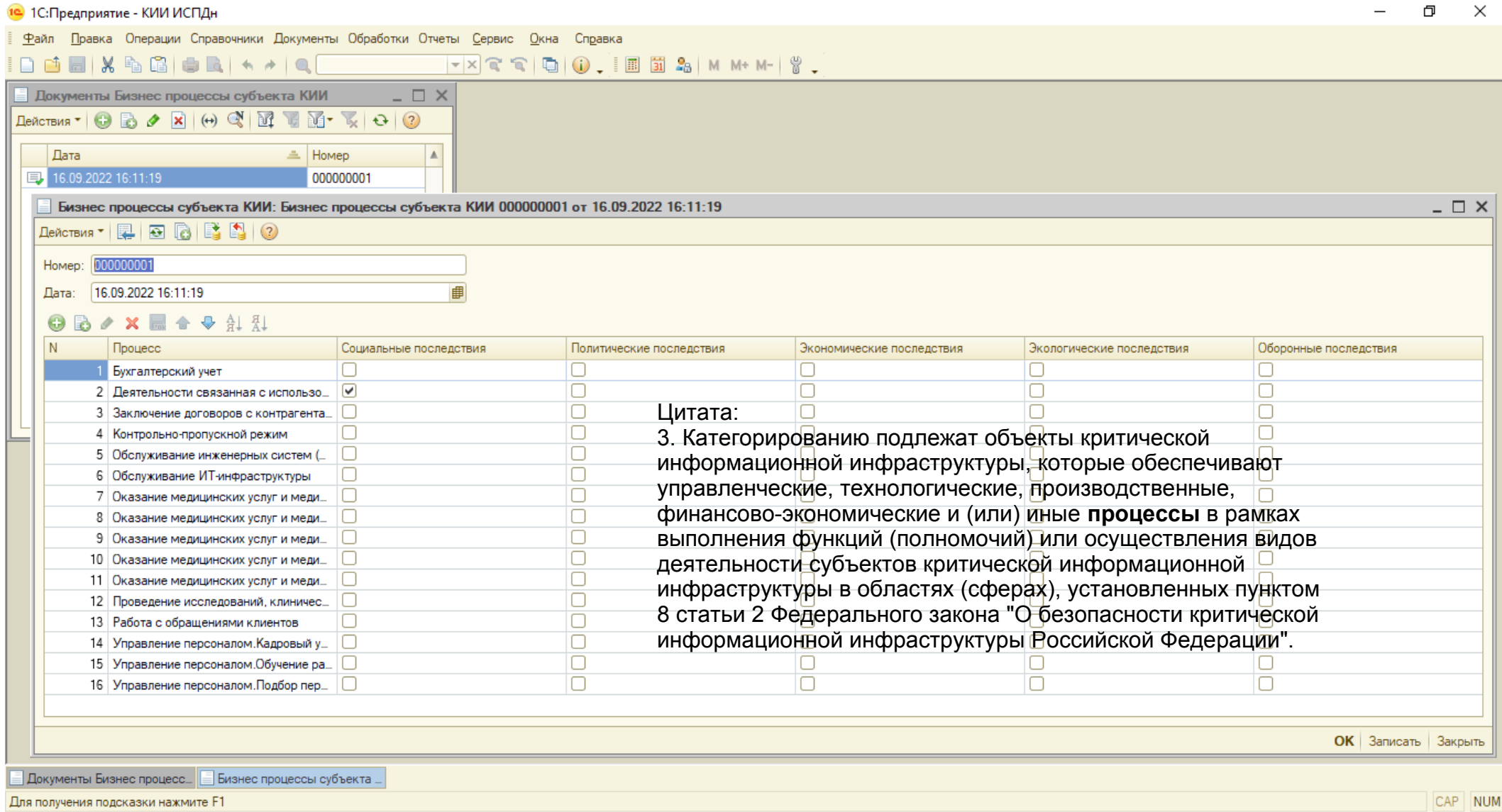
ЭЦП можно заполнить из хранилища установленных ЭЦП на рабочем месте, или заполнить из выбранных сертификатов ЭЦП

Документ.АктКатегорирования



Цитата:
16. Решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

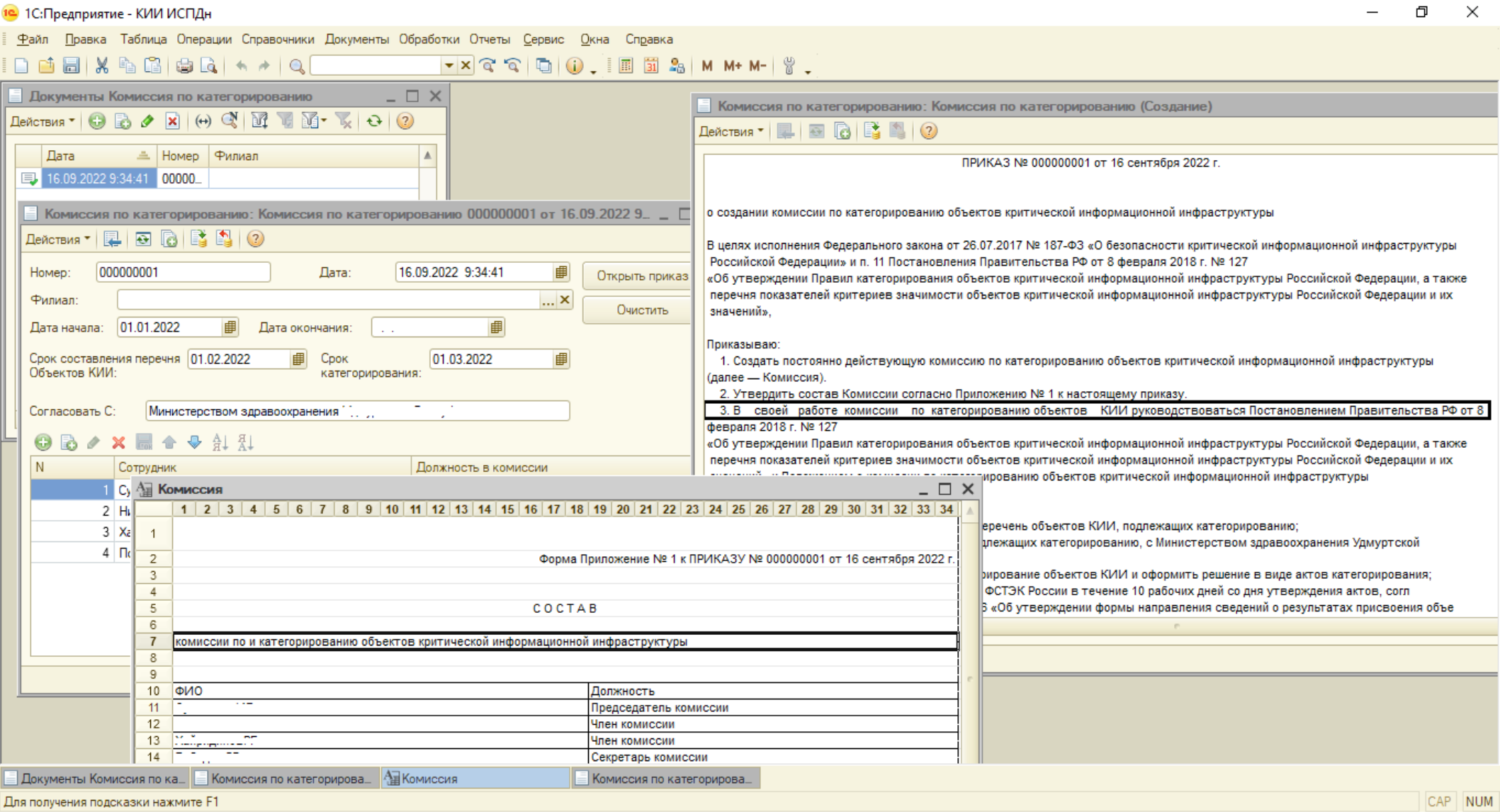
Документ.БизнесПроцессы



Цитата:

3. Категорированию подлежат объекты критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные **процессы** в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

Документ.КомиссияПоКатегорированию

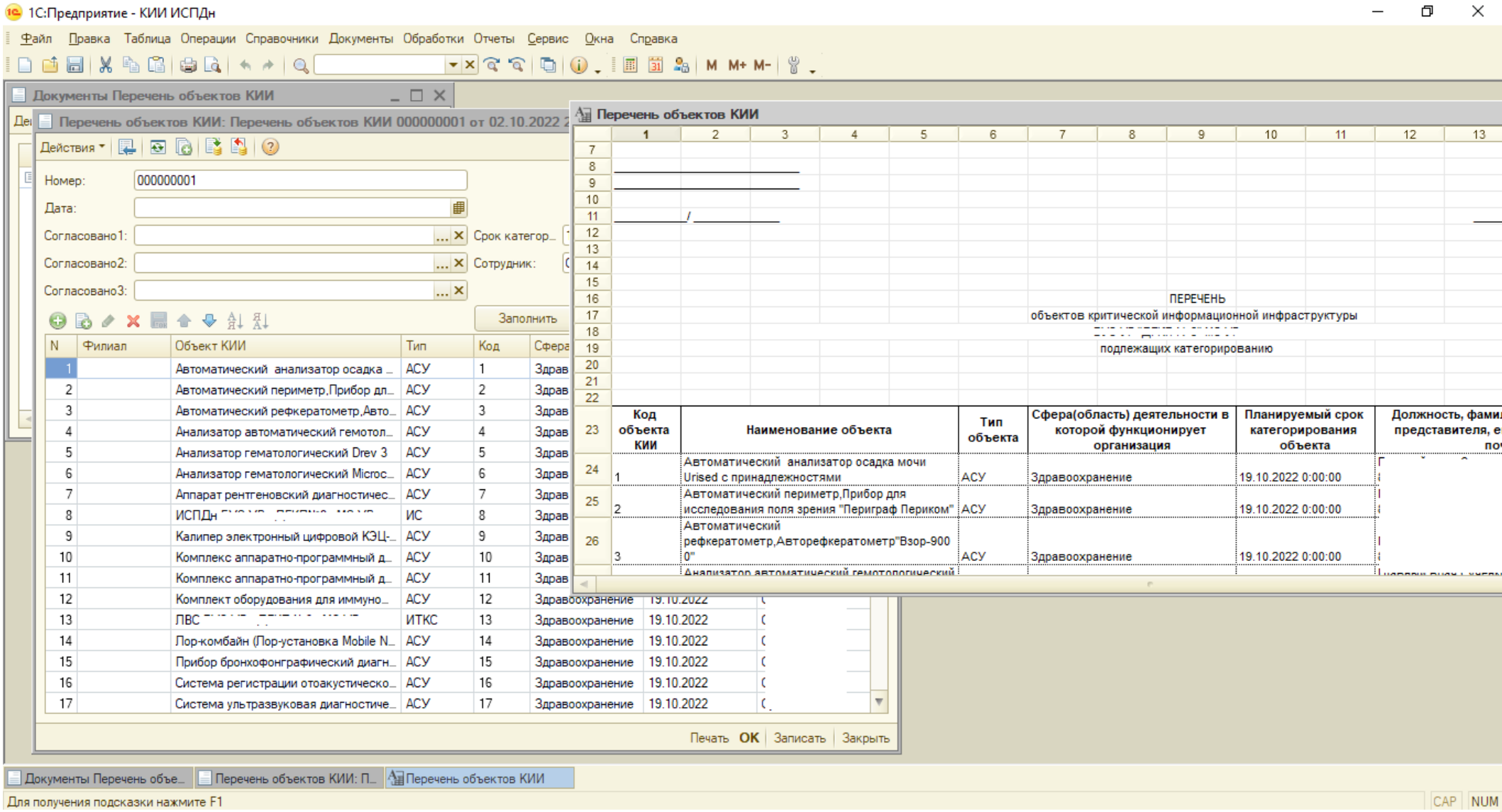


Документ.КомиссияПоКатегорированию

14. Комиссия по категорированию в ходе своей работы:

- а) определяет процессы, указанные в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;
- б) выявляет наличие критических процессов у субъекта критической информационной инфраструктуры;
- в) выявляет объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, готовит предложения для включения в перечень объектов, а также оценивает необходимость категорирования вновь создаваемых информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей;
- г) рассматривает возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;
- д) анализирует угрозы безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;
- е) оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры, определяет значения каждого из показателей критериев значимости или обосновывает их неприменимость;
- ж) устанавливает каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости.
-

Документ.ПереченьОбъектовКИИ



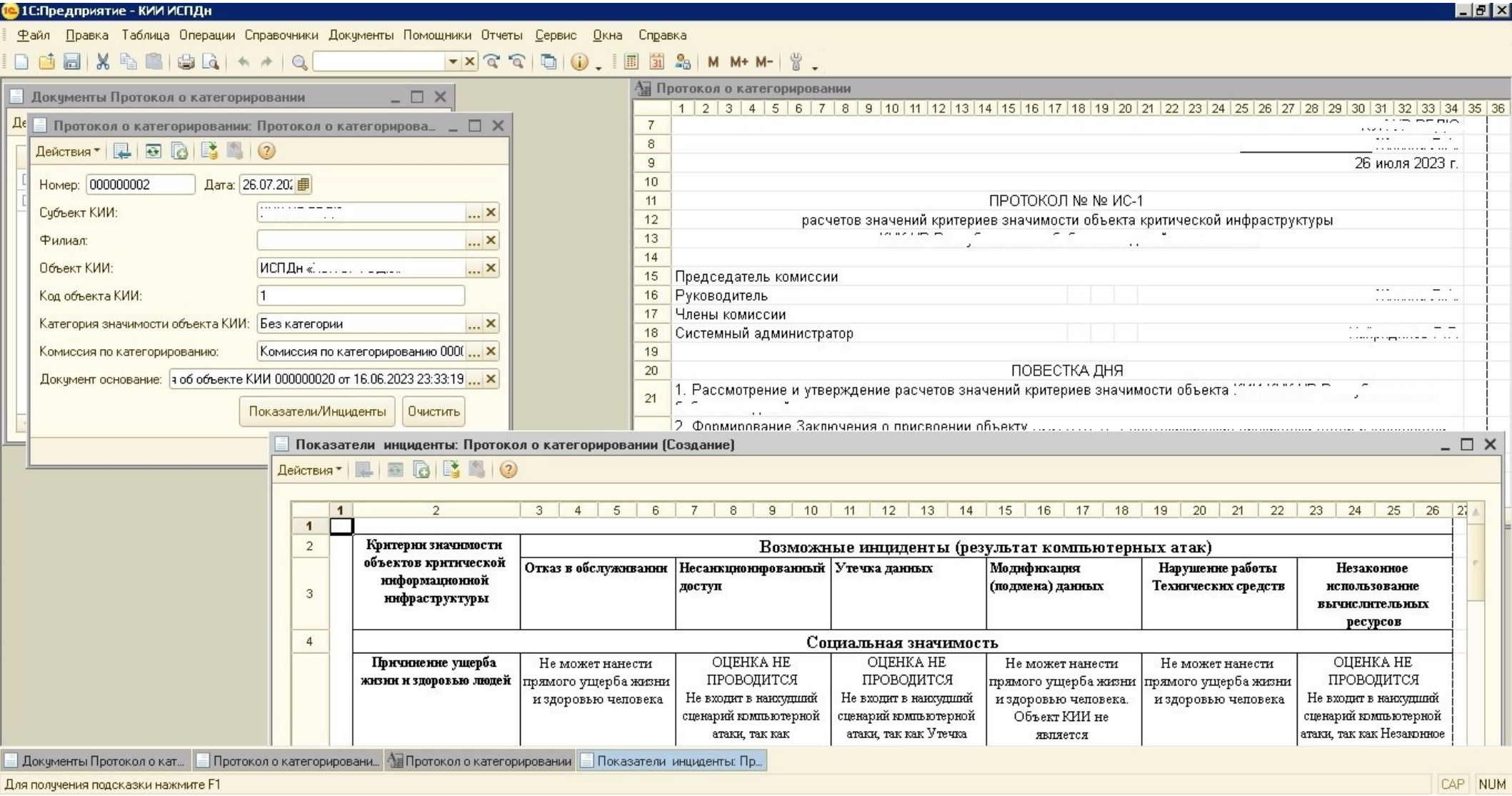
Документ.ПереченьОбъектовКИИ

Цитата:
в) определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
г) формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию (далее - перечень объектов);

В перечень объектов в том числе включаются объекты критической информационной инфраструктуры филиалов, представительств субъекта критической информационной инфраструктуры.

Перечень объектов критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

Документ.ПротоколОКатегорировании



Критерии значимости объектов критической информационной инфраструктуры	Возможные инциденты (результат компьютерных атак)					
	Отказ в обслуживании	Несанкционированный доступ	Утечка данных	Модификация (подмена) данных	Нарушение работы Технических средств	Незаконное использование вычислительных ресурсов
Социальная значимость						
Причинение ущерба жизни и здоровью людей	Не может нанести прямого ущерба жизни и здоровью человека	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Утечка	Не может нанести прямого ущерба жизни и здоровью человека. Объект КИИ не является	Не может нанести прямого ущерба жизни и здоровью человека	ОЦЕНКА НЕ ПРОВОДИТСЯ Не входит в наихудший сценарий компьютерной атаки, так как Незаконное

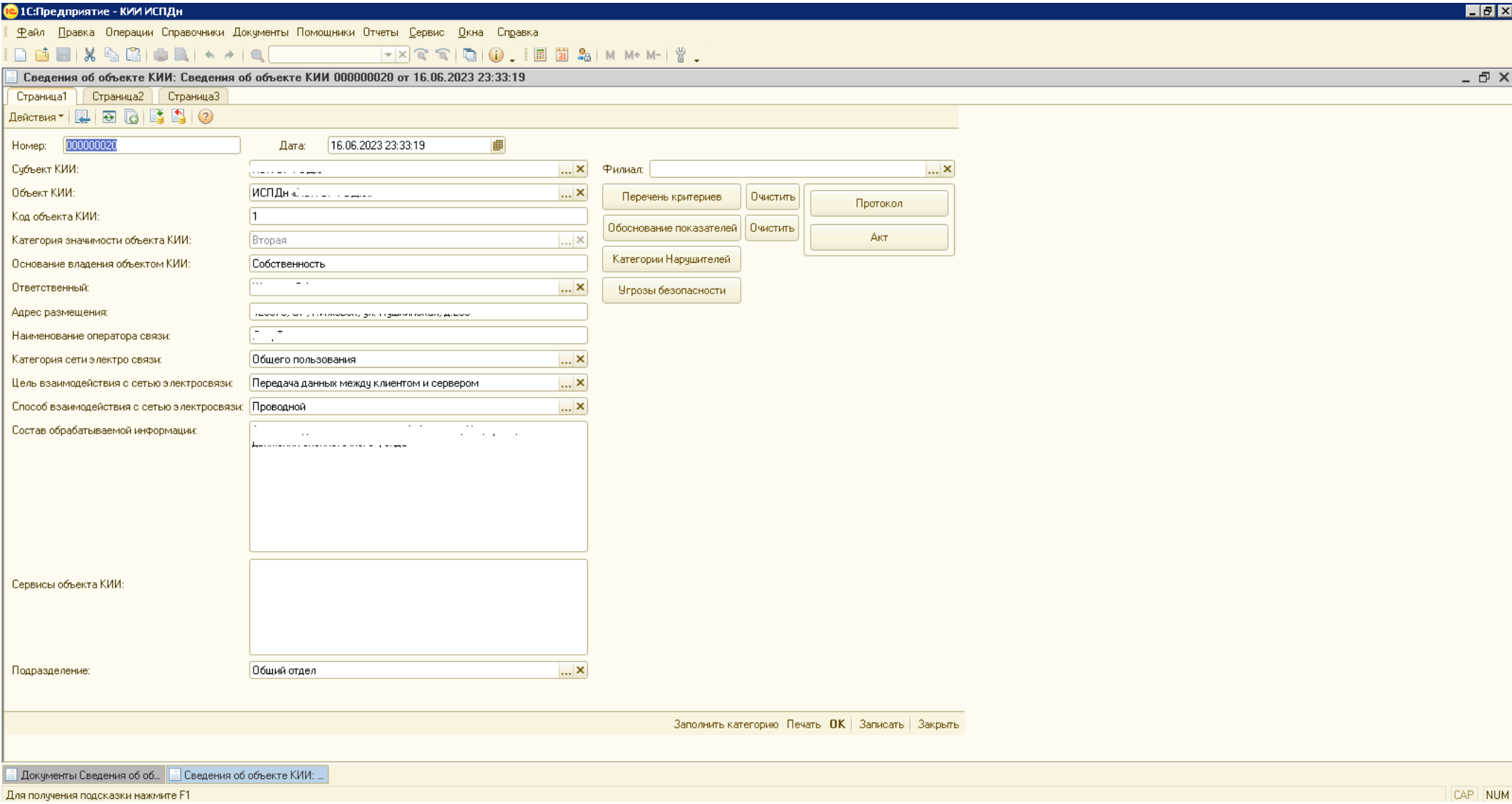
Документ.ПротоколОКатегорировании

Результаты расчета значений показателей критериев значимости объектов КИИ организации сферы здравоохранения для каждой ИС, ИТКС, АСУ организации сферы здравоохранения фиксируются в Протоколе расчетов значений критериев значимости.

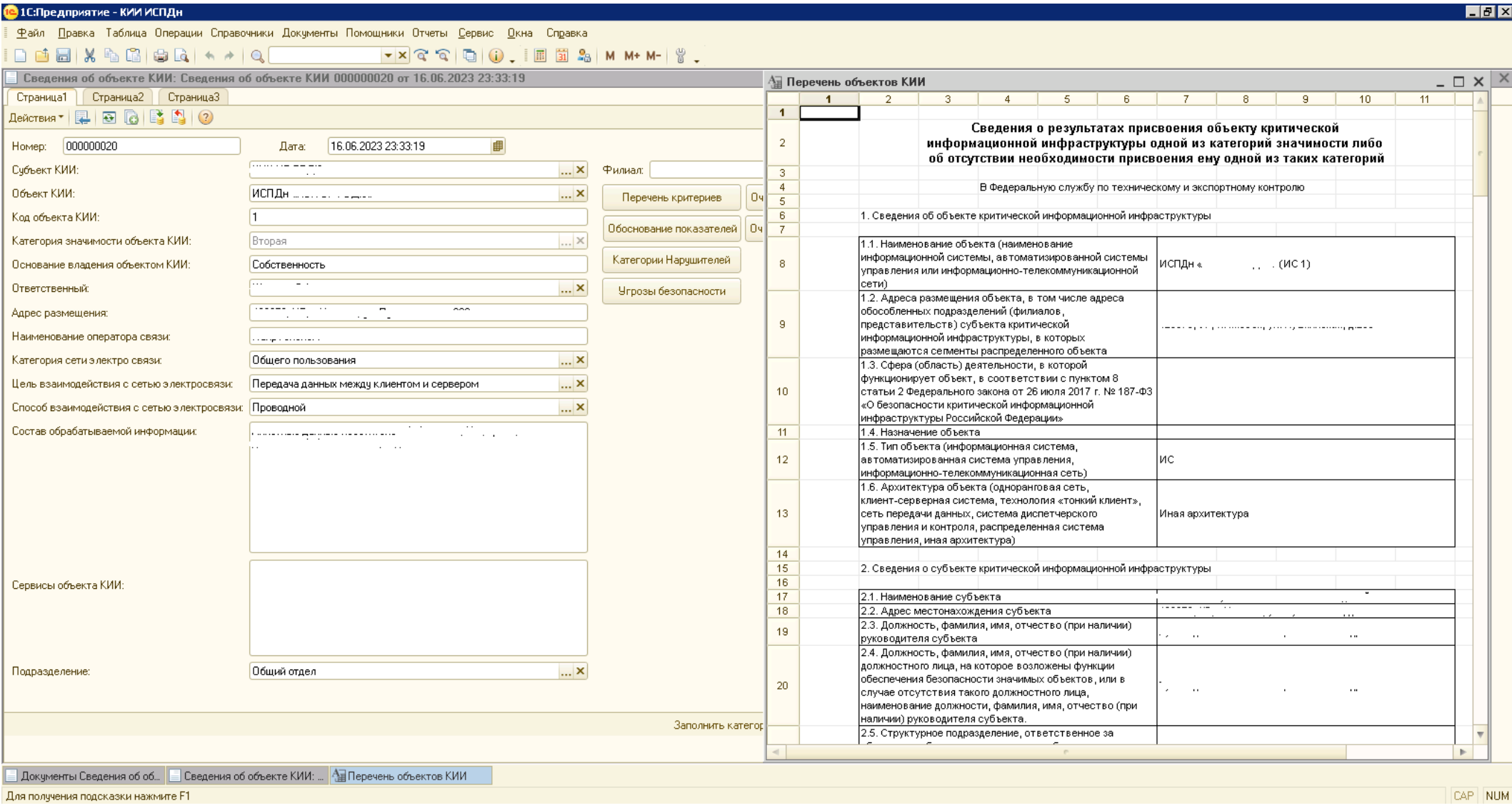
Протокол расчетов значений критериев значимости объектов КИИ организации сферы здравоохранения оформляется для каждой ИС, ИТКС, АСУ, включенной в Перечень объектов КИИ организации сферы здравоохранения, подлежащих категорированию. Общие сведения об ИС, ИТКС, АСУ, подлежащей категорированию, вносятся в разделы I–III Протокола расчетов значений критериев значимости объектов КИИ.

В разделе IV Протокола расчетов значений критериев значимости объектов КИИ в каждой графе, для которой определена неприменимость критериев значимости, установленных постановлением Правительства РФ от 08.02.2018 № 127, указывается обоснование неприменимости критерия.

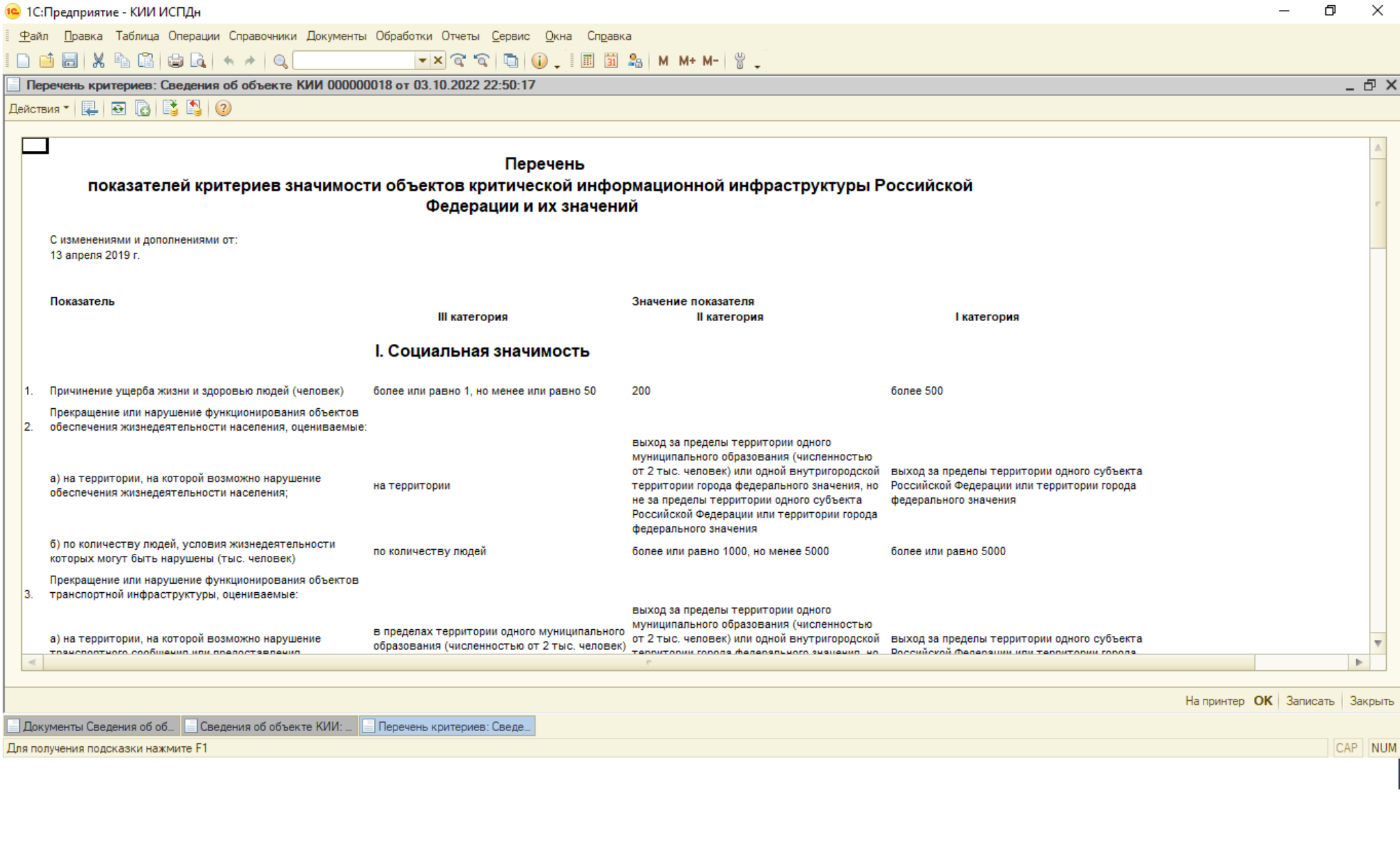
Документ.СведенияОбОбъектеКИИ



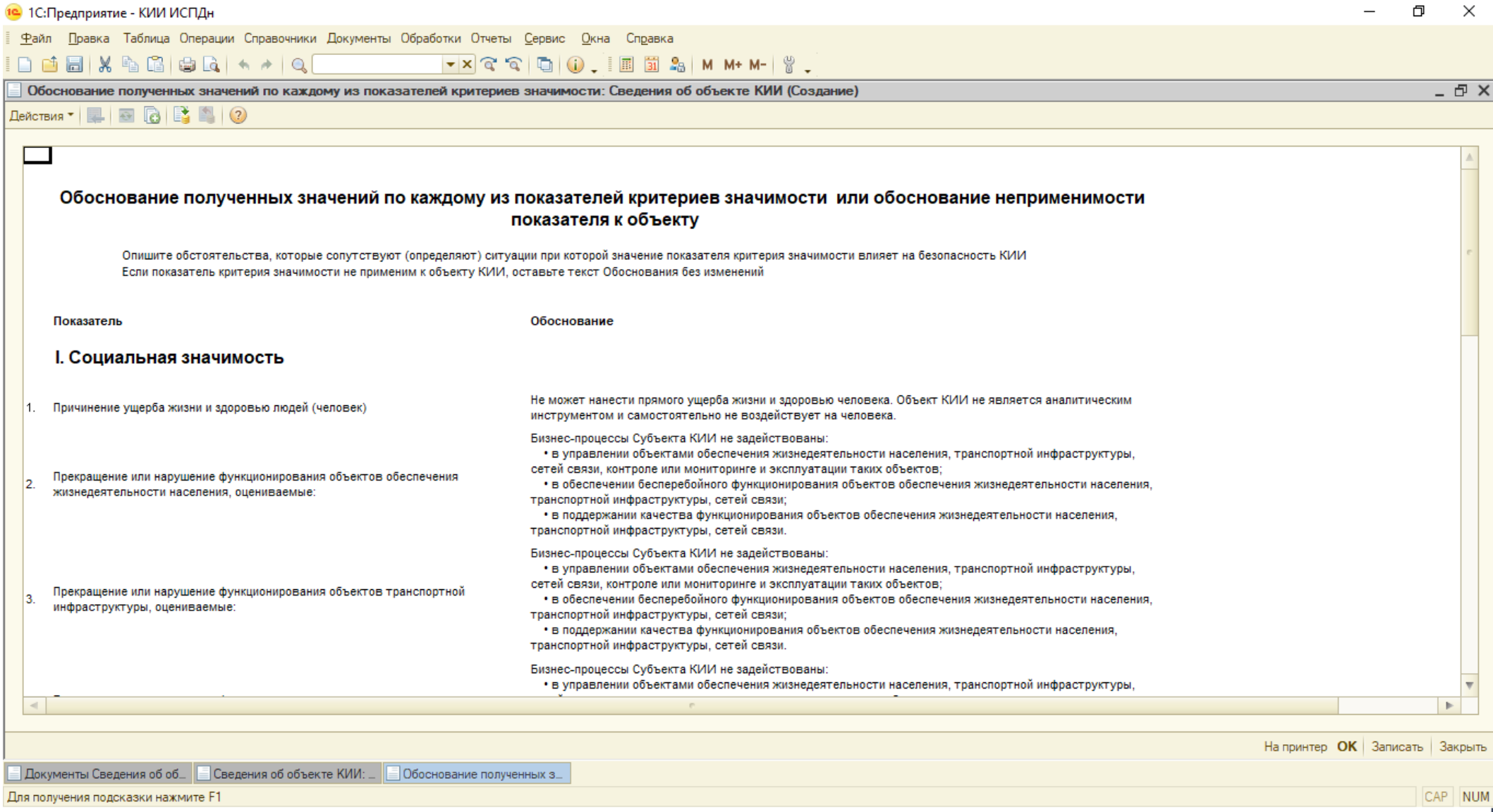
Документ.СведенияОбОбъектеКИИ



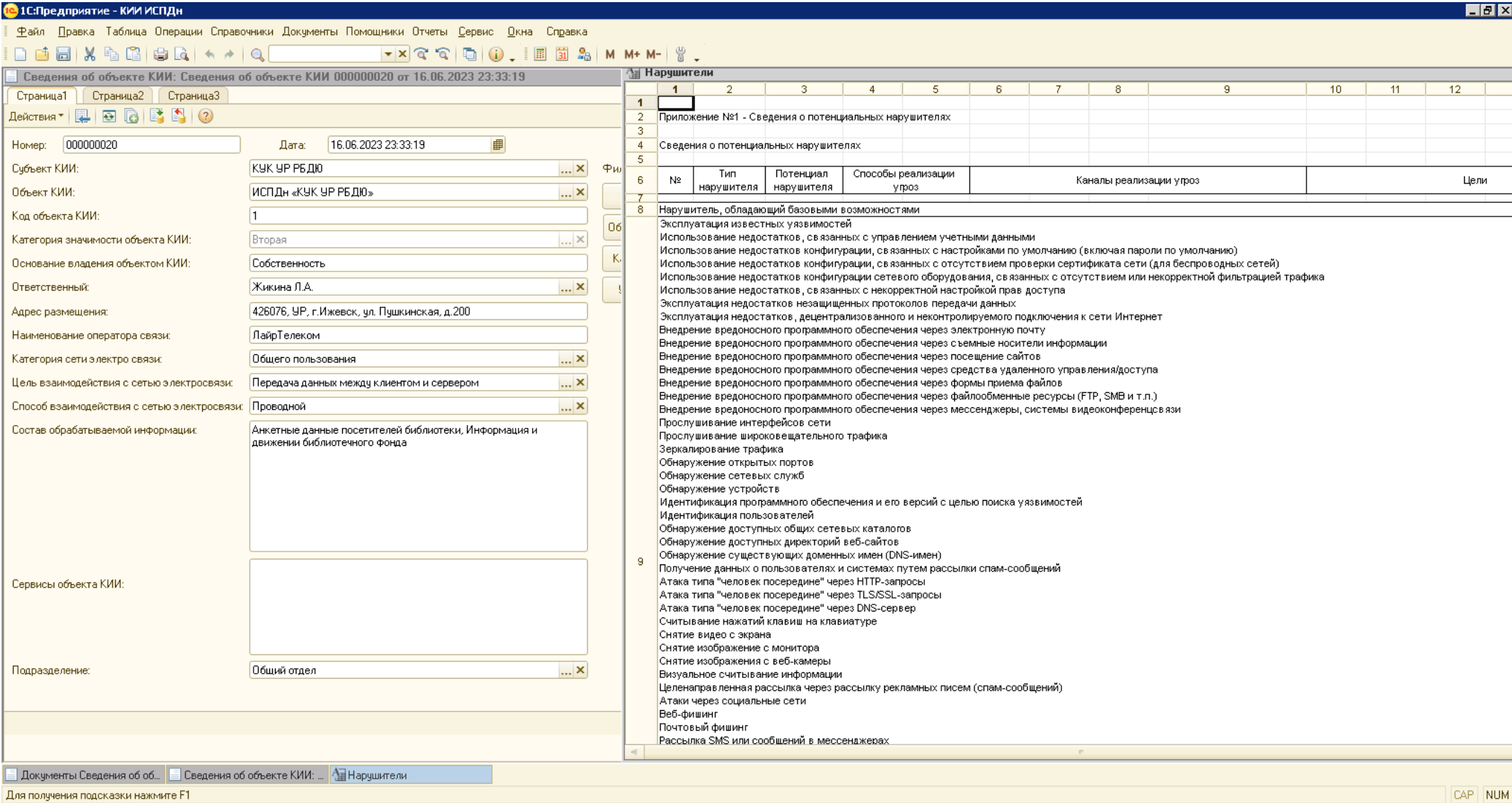
Документ.СведенияОбОбъектеКИИ



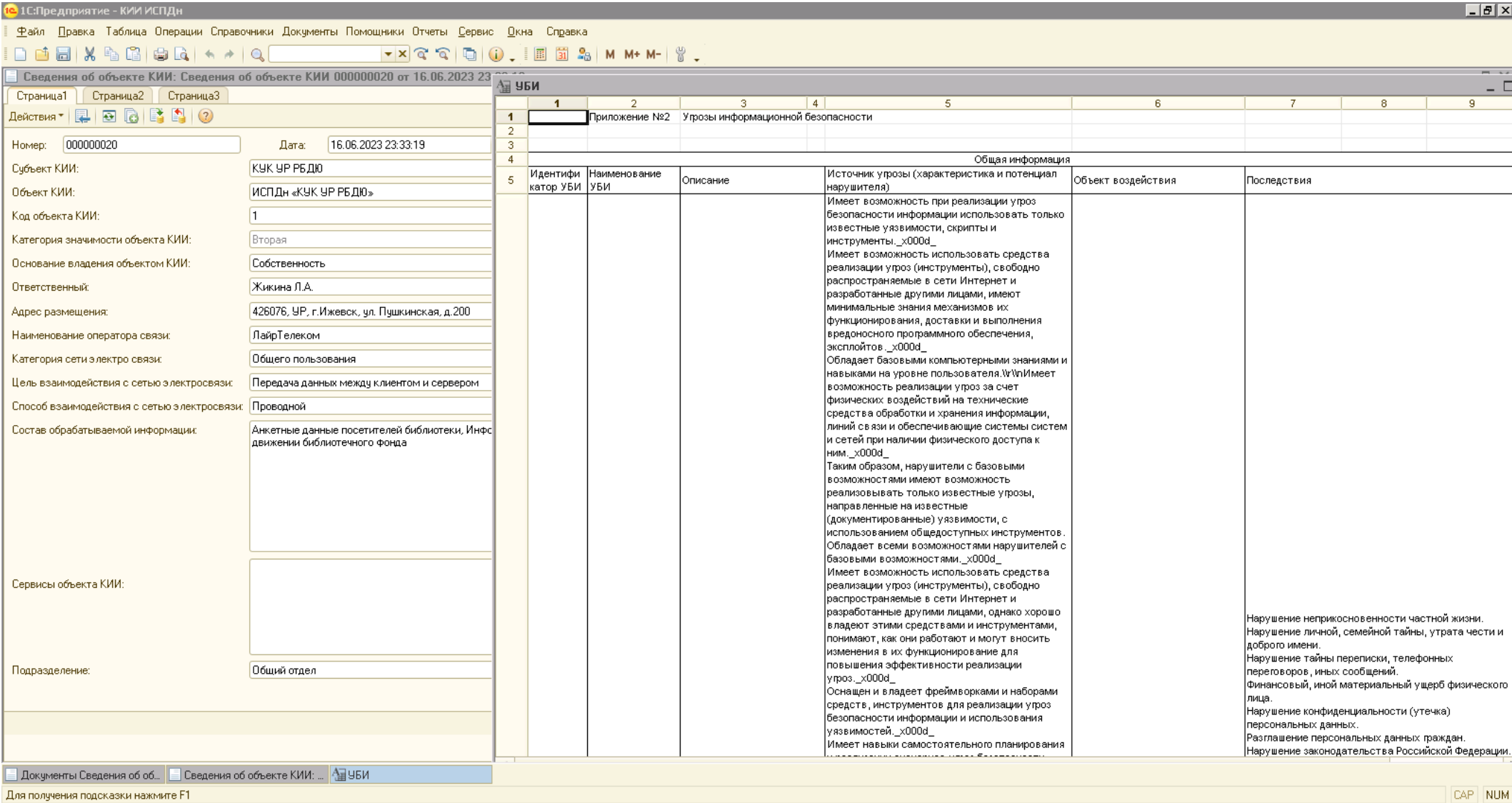
Документ.СведенияОбОбъектеКИИ



Документ.СведенияОбОбъектеКИИ



Документ.СведенияОбОбъектеКИИ

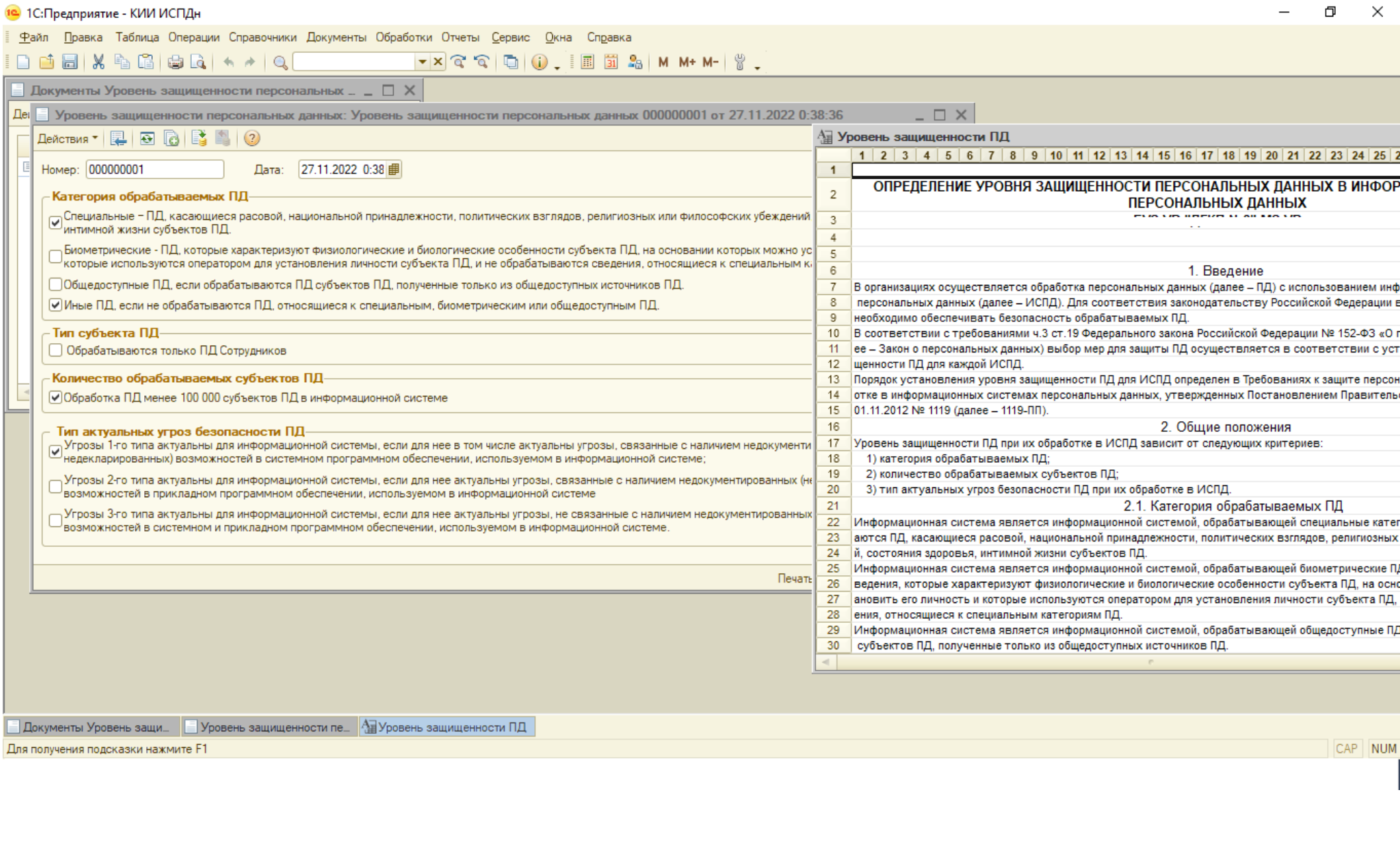


Документ.СведенияОбОбъектеКИИ

д) оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;
е) присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.
6. Объекту критической информационной инфраструктуры по результатам категорирования присваивается в соответствии с перечнем показателей критериев значимости категория значимости с наивысшим значением.
Для каждого показателя критериев значимости, для которого установлено более одного значения такого показателя (территория, количество людей), оценка производится по каждому из значений показателя критериев значимости, а категория значимости присваивается по наивысшему значению такого показателя.
В случае если объект критической информационной инфраструктуры по одному из показателей критериев значимости отнесен к первой категории, расчет по остальным показателям критериев значимости не проводится.
В случае если ни один из показателей критериев значимости неприменим для объекта критической информационной инфраструктуры или объект критической информационной инфраструктуры не соответствует ни одному показателю критериев значимости и их значениям, категория значимости не присваивается.

17. Субъект критической информационной инфраструктуры в течение 10 рабочих дней со дня утверждения акта, указанного в пункте 16 настоящих Правил, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Указанные сведения включают:
а) сведения об объекте критической информационной инфраструктуры;
б) сведения о субъекте критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежит объект критической информационной инфраструктуры;
в) сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи;
г) сведения о лице, эксплуатирующем объект критической информационной инфраструктуры;
д) сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры, в том числе средствах, используемых для обеспечения безопасности объекта критической информационной инфраструктуры и их сертификатах соответствия требованиям по безопасности информации (при наличии);
е) сведения об угрозах безопасности информации и о категориях нарушителей в отношении объекта критической информационной инфраструктуры либо об отсутствии таких угроз;
ж) возможные последствия в случае возникновения компьютерных инцидентов на объекте критической информационной инфраструктуры либо сведения об отсутствии таких последствий;
з) категорию значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости, содержащие полученные значения по каждому из рассчитываемых показателей критериев значимости с обоснованием

Документ.УровеньЗащищенностиПДн



Документ.УровеньЗащищенностиПДн

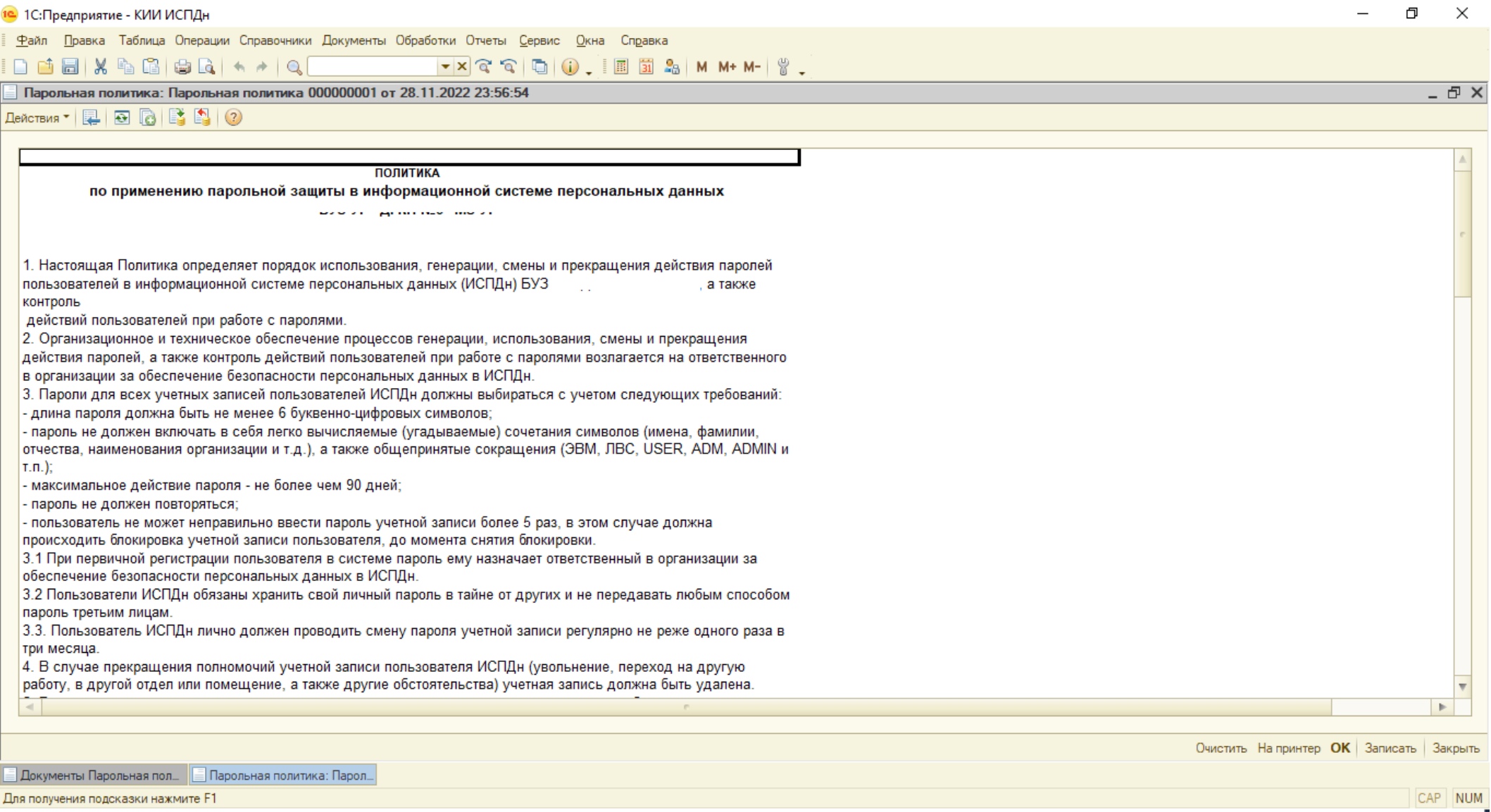
В организациях осуществляется обработка персональных данных (далее – ПД) с использованием информационных систем персональных данных (далее – ИСПД). Для соответствия законодательству Российской Федерации в области защиты ПД необходимо обеспечивать безопасность обрабатываемых ПД

В соответствии с требованиями ч.3 ст.19 Федерального закона Российской Федерации № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) выбор мер для защиты ПД осуществляется в соответствии с устанавливаемым уровнем защищенности ПД для каждой ИСПД.
Порядок установления уровня защищенности ПД для ИСПД определен в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (далее – 1119-ПП)

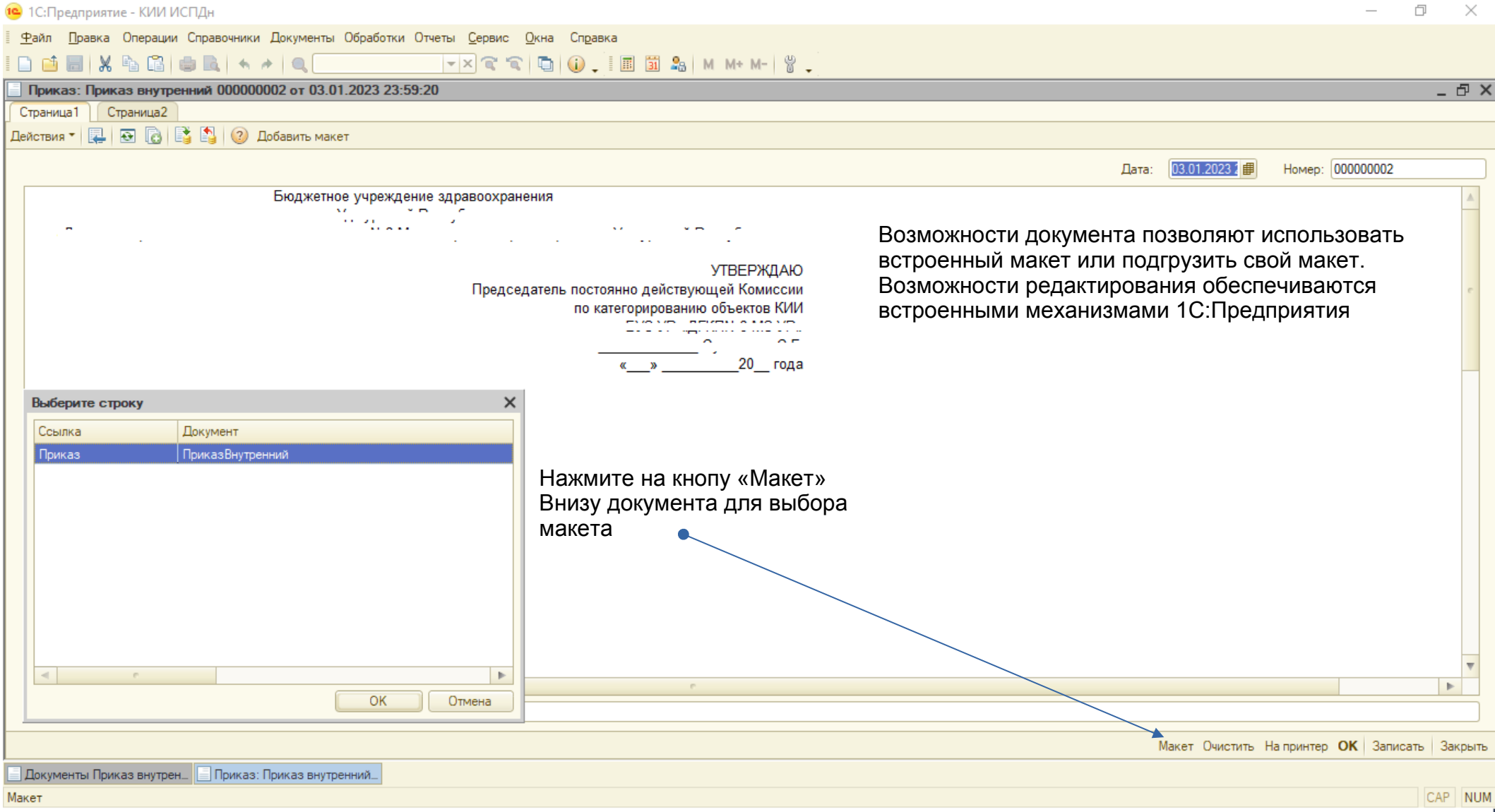
Уровень защищенности ПД при их обработке в ИСПД зависит от следующих критериев:

1) категория обрабатываемых ПД;
2) количество обрабатываемых субъектов ПД;
3) тип актуальных угроз безопасности ПД при их обработке в ИСПД.

Документ.ПарольнаяПолитика



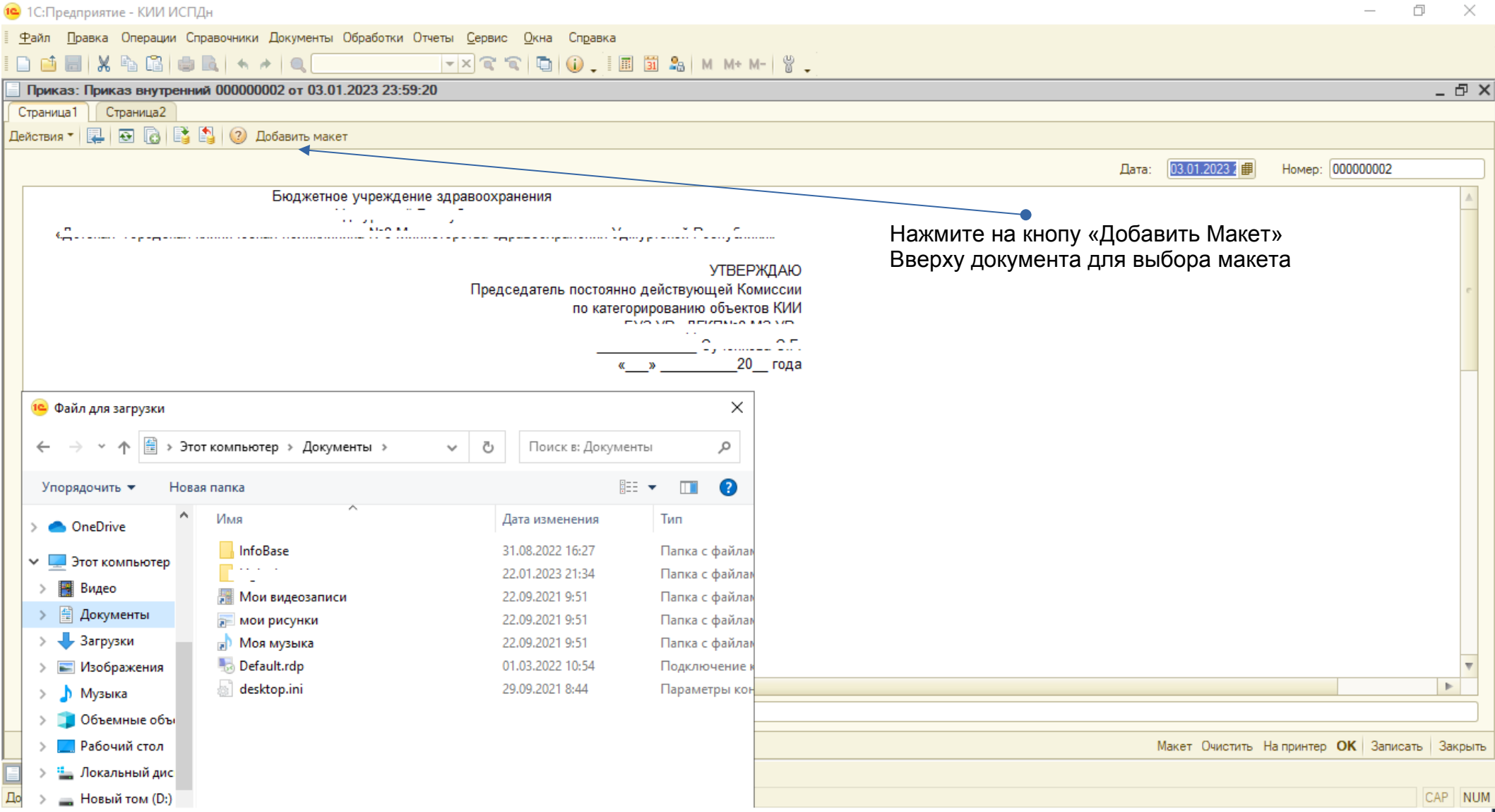
Документ.ПриказВнутренний



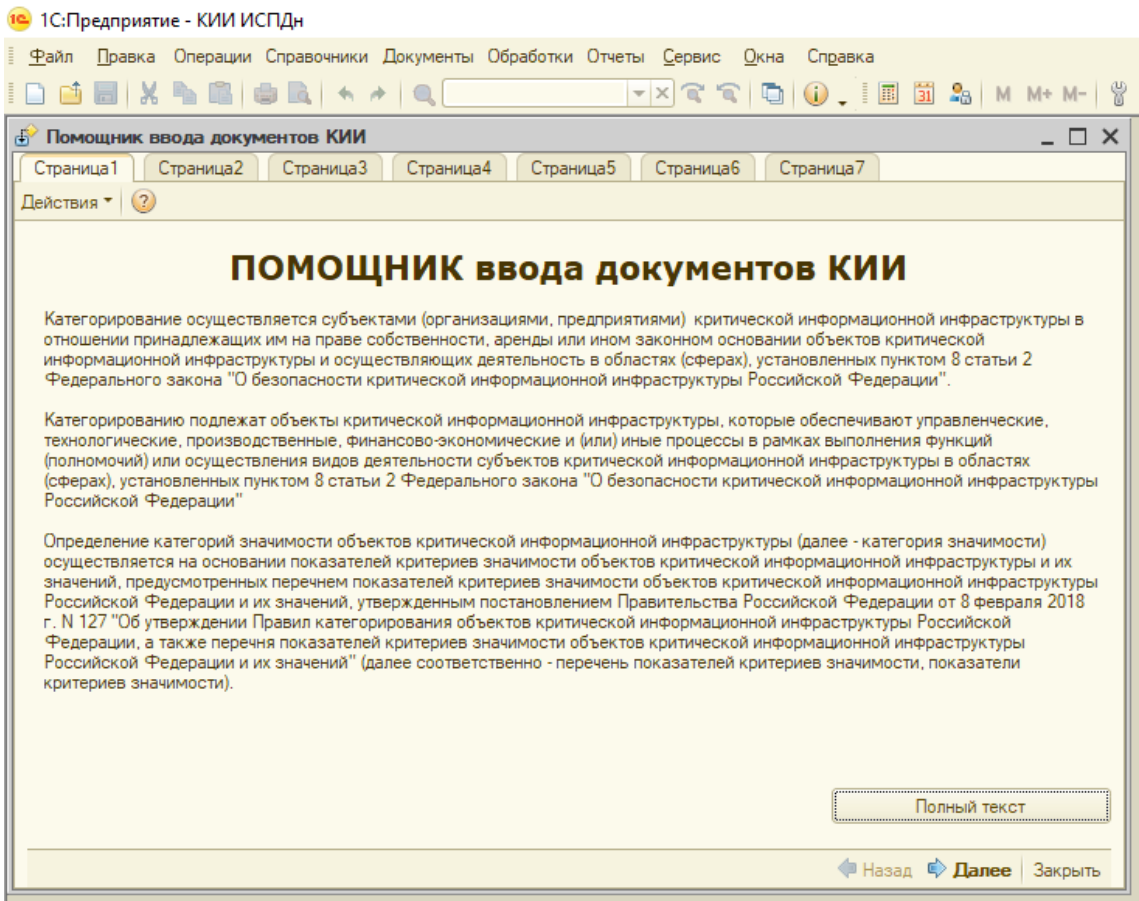
Возможности документа позволяют использовать встроенный макет или подгрузить свой макет. Возможности редактирования обеспечиваются встроенными механизмами 1С:Предприятия

Нажмите на кнопу «Макет» Внизу документа для выбора макета

Документ.ПриказВнутренний

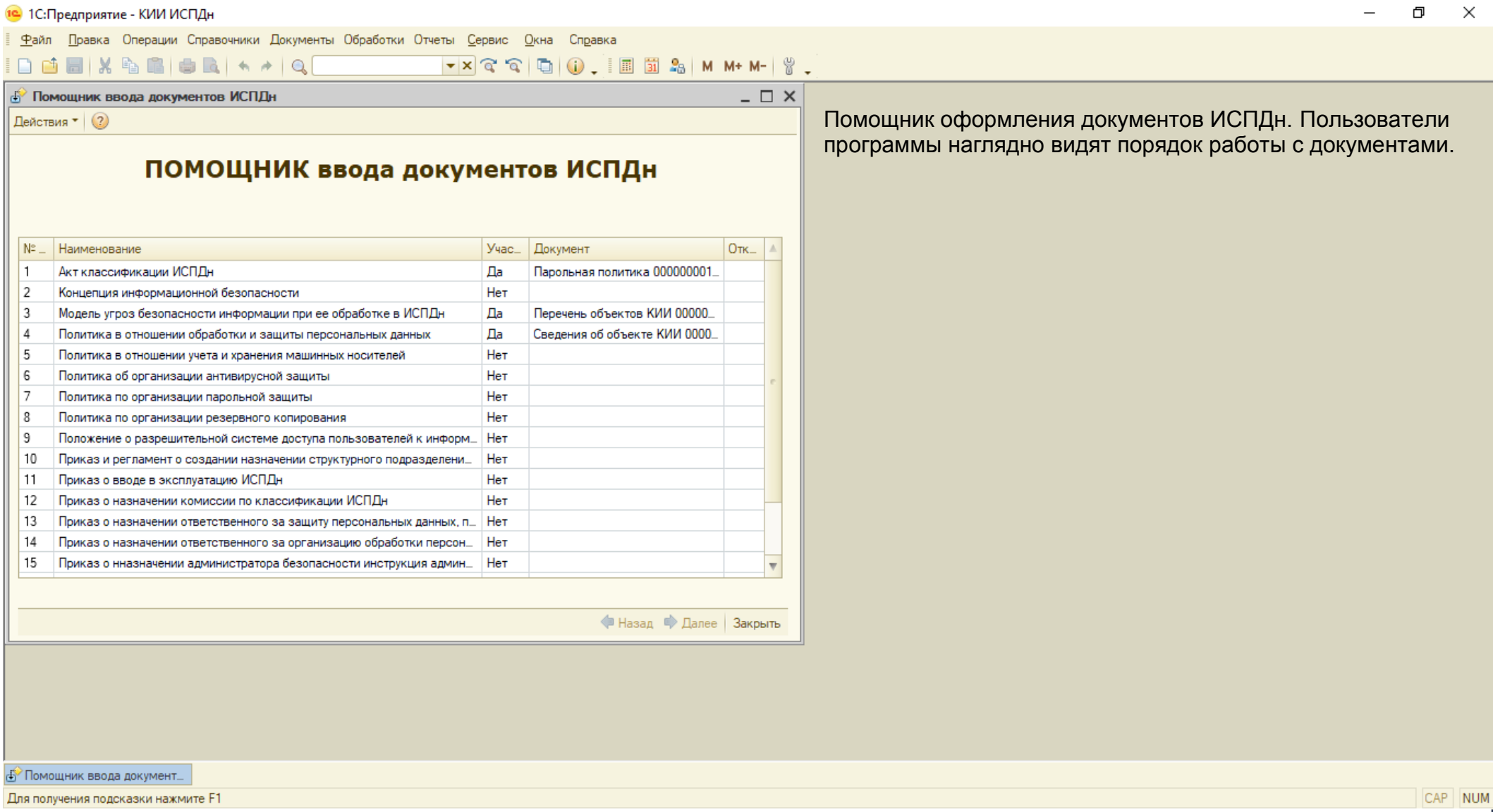


Помощник.ВводДокументовКИИ



Помощник оформления документов КИИ. Пользователи программы наглядно видят порядок работы с документами.

Помощник.ВводДокументовИСПДн



Помощник оформления документов ИСПДн. Пользователи программы наглядно видят порядок работы с документами.