СТАНДАРТ БЕЗОПАСНОСТИ
БЕЗОПАСНОСТЬ КАК СТАНДАРТ

Комплексные решения
технической безопасности

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

программного комплекса «ОКиДОКи»

версия 2.23

Модуль «Защита информации»

Ярославль

2024

Оглавление

1 Общие сведения

1.1 Что такое «ОКиДОКи»

«ОКиДОКи» — модульная система для организационного обеспечения информационной безопасности.

Модуль «Защита информации» позволяет:

– вести учет защищаемых объектов (технических средств, информационных систем, абонентских пунктов, информационно-телекоммуникационных сетей, объектов критической информационной инфраструктуры) и применяемых средств защиты информации;

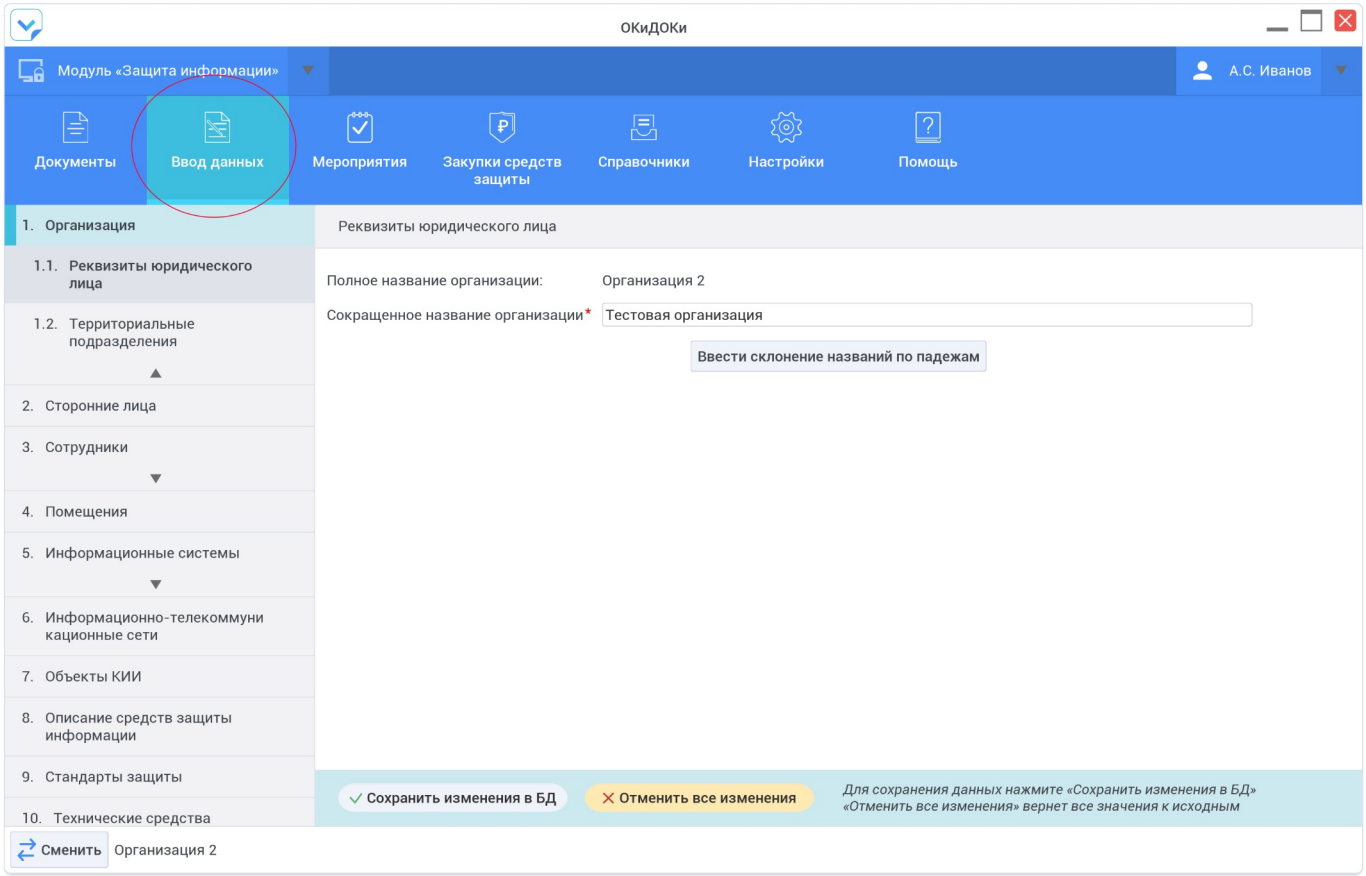
– вести учет закупок средств защиты информации (оборудования и лицензий), а также сертификатов технической поддержки средств защиты информации, анализировать потребность в средствах защиты информации;

– вести учет мероприятий в области обеспечения информационной безопасности (работ по защите информации, внешних и внутренних проверок), оценивать их полноту в отношении защищаемых информационных систем;

– создавать технические паспорта информационных систем.

1.2 С чего начать?

Первым этапом работы с модулем является ввод данных.



Вводимые данные логически сгруппированы, и вводить данные лучше в том порядке, в каком представлены пункты в левом меню.

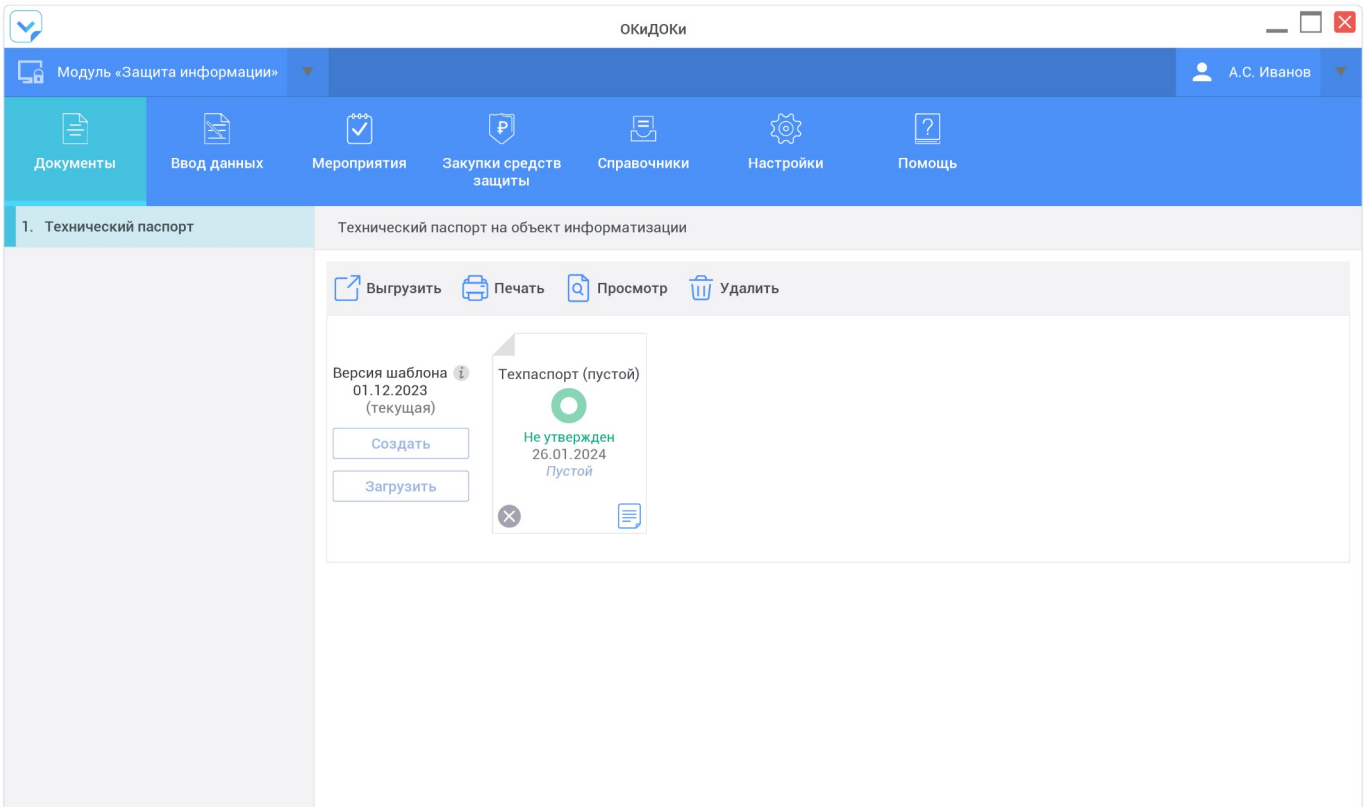
В каждом пункте левого меню данные не отправляются на сервер до тех пор, пока не будет нажата кнопка «Сохранить изменения в БД».

Не обязательно вводить все данные сразу. Однако если данные введены частично, то создаваемые документы могут содержать пустые таблицы и текст, выделенный желтым маркером (например, «Наименование должности руководителя»).

1.3 Как создавать документы?

В разделе «Документы» отражена история создания документов каждого вида.

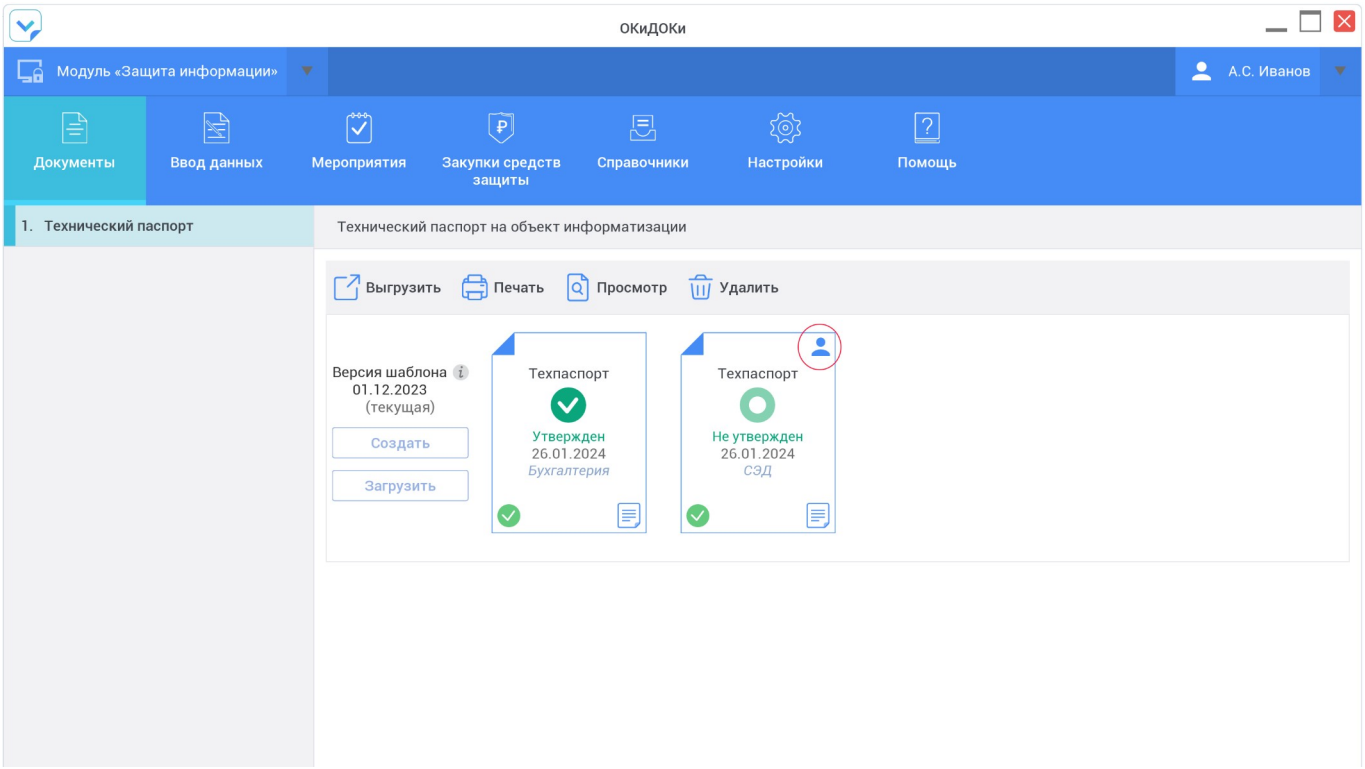
В каждом подразделе можно изменять статусы документов (по нажатию правой кнопкой мыши на документе), загружать свои версии, удалять документы, открывать их для просмотра.



2 Документы

Технический паспорт на каждую информационную систему является документом длительного действия, то есть предполагается, что в каждый момент времени для конкретной информационной системы действующим является только один документ. Если для информационной системы уже есть актуальный технический паспорт, то создать для нее еще один паспорт невозможно.

Технические паспорта, которые были загружены в систему извне, а не созданы ее средствами, отмечены голубым значком «Пользовательский документ».



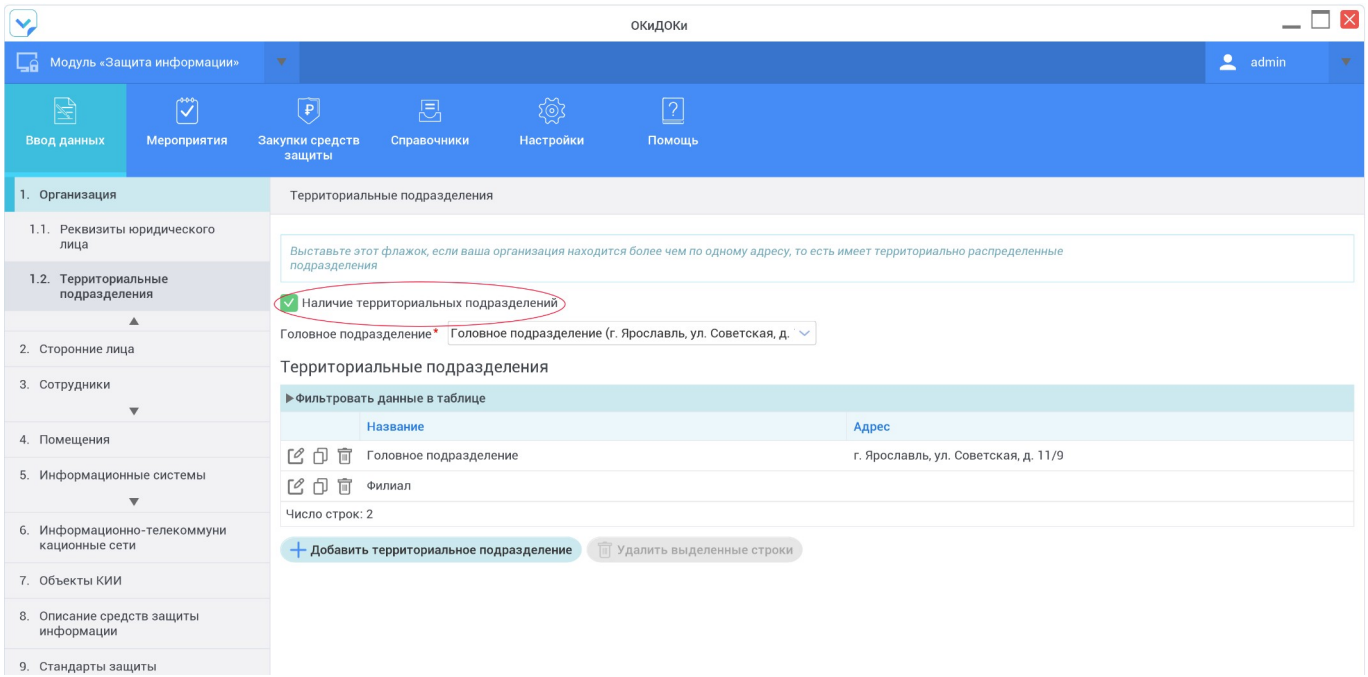
В случае, если после создания документа в разделе «Ввод данных» были внесены изменения (например, изменились характеристики информационной системы, состав входящих в нее технических средств и т. п.), и эти изменения затронули содержание конкретного документа, у него появится значок в виде красной стрелки «Утратил актуальность».

3 Ввод данных

3.1 Подраздел «Организация»

Здесь вводится общая информация об организации.

Если у организации есть территориальные подразделения (не являющиеся отдельными юридическими лицами), то есть она функционирует более чем по одному адресу, следует выставить флажок «Наличие территориальных подразделений». В этом случае будет доступна возможность ввода информации по каждому территориальному подразделению.



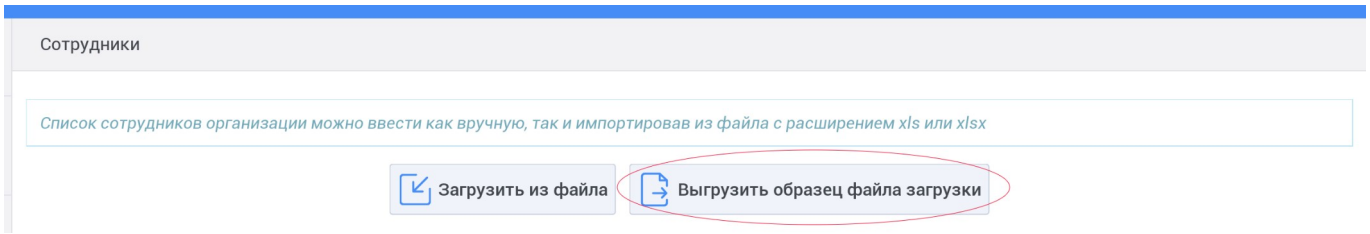
При отсутствии территориальных подразделений при вводе данных о контролируемой зоне организации в поле «Адрес фактического местонахождения организации» по умолчанию отображается юридический адрес организации.

3.2 Подраздел «Сторонние лица»

В подразделе «Сторонние лица» можно внести информацию о сторонних организациях и их сотрудниках, выполняющих для вашей организации какие-либо работы в области информационной безопасности.

3.3 Подраздел «Сотрудники»

Список сотрудников организации можно ввести как вручную, так и импортировав из файла с расширением xls, полученного путем выгрузки из программы «1С». Если помимо имен сотрудников файл содержит их должности (во втором столбце), отделы (в третьем столбце), табельные номера (в четвертом столбце), адрес электронной почты (в пятом столбце), номер телефона (в шестом столбце), эти данные так же будут загружены. Образец файла загрузки можно выгрузить, нажав на соответствующую кнопку.



Кроме того, доступна возможность автоматизированной регулярной загрузки данных о сотрудниках из программы «1С» (см. руководство администратора на программный комплекс «ОКиДОКи»).

3.4 Подраздел «Помещения»

Здесь к ранее добавленным территориальным подразделениям (или к организации в целом) добавляются помещения. Если помещение не является помещением с регламентированным доступом (в нем не осуществляется обработка или хранение защищаемой информации или криптосредств), добавлять его не нужно.

В дальнейшем информация о помещениях будет использована при указании мест размещения технических средств.

3.5 Подраздел «Информационные системы»

В этом подразделе вводятся данные об информационных системах, в которых обрабатывается защищаемая информация (в том числе, персональные данные).

Согласно классическому определению, под информационной системой понимается совокупность содержащейся в базе данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Таким образом, при определении границ и состава информационной системы можно отталкиваться от наличия собственной базы данных, содержащей защищаемую информацию, программных средств, применяемых для ее обработки, круга технических средств (серверов, рабочих станций), на которых обрабатывается защищаемая информация.

3.6 Подраздел «Информационно-телекоммуникационные сети»

В этом подразделе вводятся данные о защищаемых информационно-телекоммуникационных сетях.

3.7 Подраздел «Объекты КИИ»

В данном подразделе указывается, какие информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети из числа введенных ранее являются объектами критической информационной инфраструктуры, то есть, согласно определению, участвуют в осуществлении критических процессов.

После добавления объекта критической информационной инфраструктуры проводится оценка его значимости (определение категории значимости).

3.8 Подраздел «Описание средств защиты информации»

В данном подразделе вводится информация о применяемых средствах защиты информации. Для получения информации о средстве защиты (производитель, версия, номер и срок действий сертификата, характеристики, подтверждаемые сертификатом) обратитесь к имеющейся документации на него.

3.9 Подраздел «Стандарты защиты»

Стандарты защиты представляют собой набор требований по составу средств защиты информации. Они могут применяться в отношении технических средств (то есть перечисленные в стандарте средства защиты должны быть установлены на данные технические средства) либо в отношении информационно-телекоммуникационных сетей и сегментов информационных систем (то есть перечисленные в стандарте средства защиты работают на сетевом уровне и защищают сегмент или сеть в целом).

Стандарты защиты для технических средств добавляются к информационным системам, информационно-телекоммуникационным сетям и абонентским пунктам. При включении технического средства в состав таких систем, сетей или пунктов будет доступен для выбора один из добавленных к ним стандартов защиты. Выбор стандарта означает, что к данному техническому средству отныне предъявляются требования по наличию на нем указанных в стандарте средств защиты информации.

Стандарты защиты «сетевого уровня» добавляются к сегментам информационных систем и информационно-телекоммуникационным сетям. Добавление стандарта означает, что к данному сегменту или сети отныне предъявляются требования по обеспечению их защиты посредством указанных в стандарте средств защиты информации.

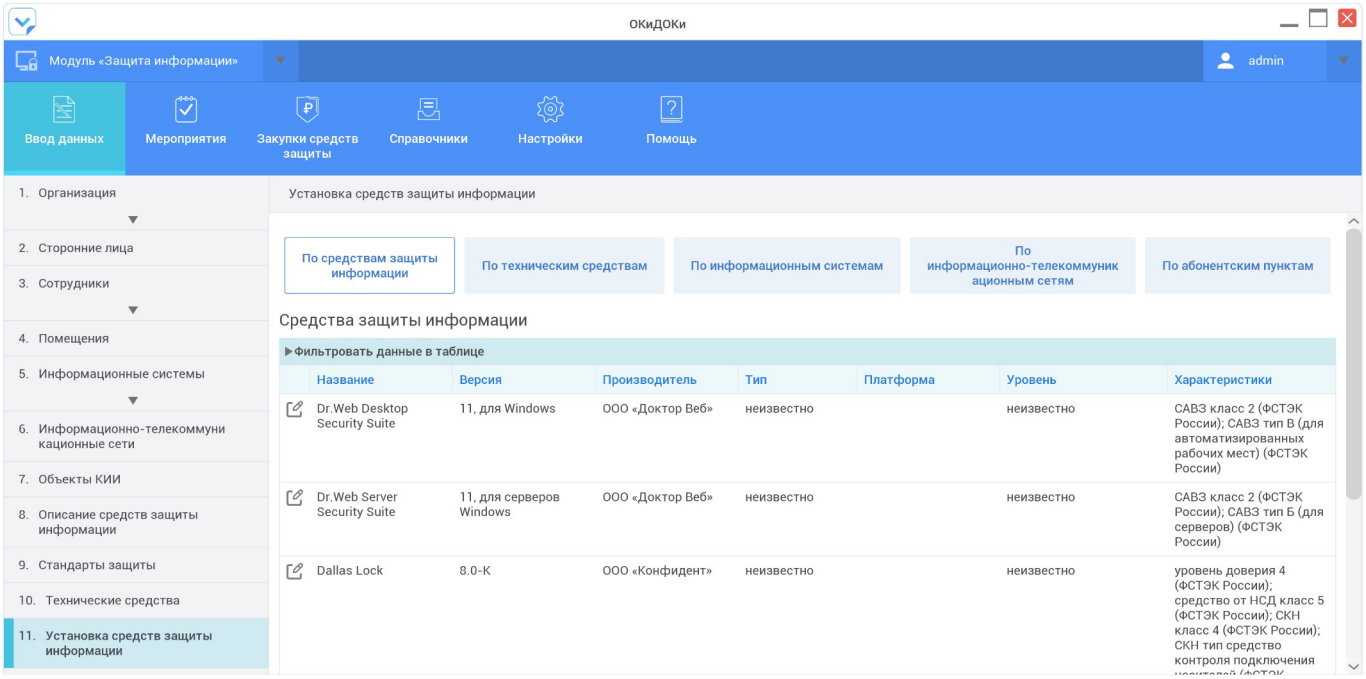
3.10 Подраздел «Технические средства»

Доступна возможность автоматизированной регулярной загрузки данных о технических средствах из программы «1С» (см. руководство администратора на программный комплекс «ОКиДОКи»).

3.11 Подраздел «Установка средств защиты информации»

В данном подразделе задаются связи между средствами защиты информации и защищаемыми объектами, обозначающие **фактическую** установку средств защиты. То есть если стандарты защиты определяют «что должно быть», в данном подразделе описывается «что реально есть».

Ввод информации об установке средств защиты возможен различными способами (отталкиваясь от конкретного средства защиты либо от конкретного защищаемого объекта). Переключение между различными способами группировки данных осуществляется с помощью кнопок в верху панели.



В случае, если для средства защиты внесена информация о закупках (раздел «Закупки средств защиты», то при внесении информации об установке средства защиты можно дополнительно указать конкретную закупку (то есть, по сути, «привязать» к месту установки конкретную лицензию или оборудование с конкретным номером).

4 Мероприятия

Данный раздел предназначен для учета всех мероприятий в области информационной безопасности.

4.1 Подраздел «Работы в отношении защищаемых объектов»

4.1.1 Подраздел «Учет работ»

В данном подразделе вводится общая информация о планируемых и проведенных работах в отношении защищаемых объектов: описание работ, период проведения, исполнитель, ответственный сотрудник внутри организации.

4.1.2 Подраздел «Область проведения работ»

Здесь можно указать, какие типы работ были проведены и в отношении каких объектов (информационных систем в целом или их отдельных сегментов, информационно-телекоммуникационных сетей, абонентских пунктов, средств защиты информации, технических средств).

Ввод этих данных позволит в дальнейшем анализировать полноту проведения работ, находить объекты, в отношении которых какой-либо обязательный этап (тип) работ был пропущен.

4.1.3 Подраздел «Документация по работам»

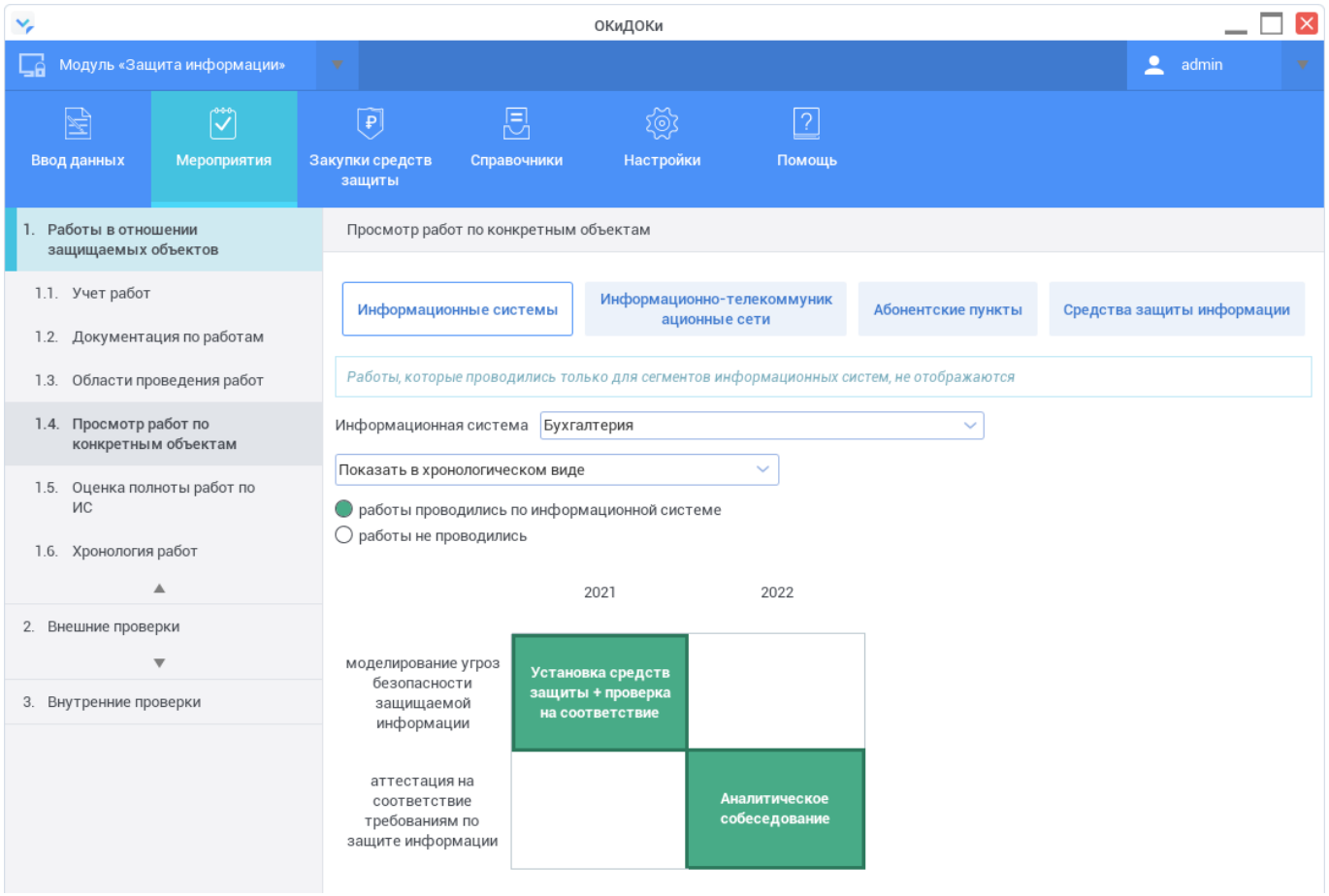
В данном подразделе к введенным ранее работам можно добавить документацию, являющуюся основанием или результатом проведения работ.

При описании результата работ рекомендуется по возможности выбирать тип документа из справочника, относящегося к типу работ, по которым добавляется документация. Это позволит программному комплексу «ОКиДОКи» отображать информацию о наличии некоторых документов (например, аттестата соответствия) при построении различных отчетов.

При загрузке документации следует иметь в виду, что помещение в базу данных программного комплекса «ОКиДОКи» документации, содержащей защищаемую информацию, может повысить требования к защите программного комплекса как информационной системы.

4.1.4 Подраздел «Просмотр работ по конкретным объектам»

Данный подраздел позволяет посмотреть по каждому защищаемому объекту в отдельности, какие работы в отношении него проводились.



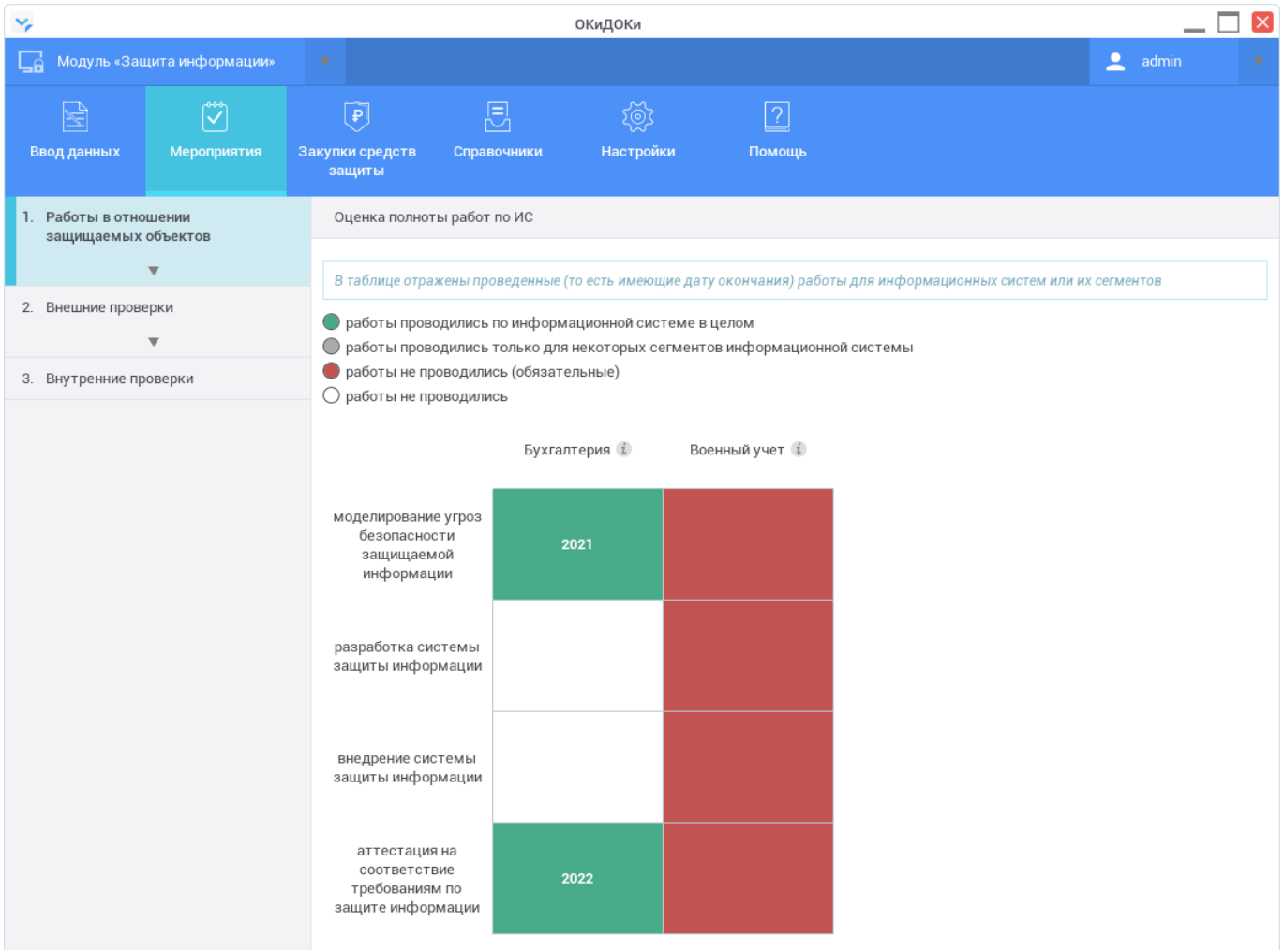
Просмотр информации о работах в отношении конкретного объекта возможен как в хронологическом виде, так и в виде таблицы.

4.1.5 Подраздел «Оценка полноты работ по ИС»

Данный раздел позволяет легко визуально оценить полноту работ по защите информации в отношении каждой информационной системы.

По характеристикам информационной системы (является ли информационной системой персональных данных, объектом критической информационной инфраструктуры и т. п.) определяется состав обязательных для нее работ и отображаются реально проведенные работы, сгруппированные по типам. Красные ячейки означают, что обязательные работы не проводились.

При щелчке на ячейку можно увидеть краткую информацию о соответствующих работах (исполнитель, период проведения). Работы с непроставленной датой окончания в данном подразделе не учитываются и не отображаются.



4.1.6 Подраздел «Хронология работ»

В данном подразделе все работы в отношении всех объектов, в том числе планируемые (не имеющие даты окончания), представлены в хронологическом порядке.

4.2 Подраздел «Внешние проверки»

4.2.1 Подраздел «Учет внешних проверок»

В данном подразделе вводится общая информация о планируемых и проведенных внешних проверках, аудитах в отношении защищаемых объектов: предмет проверки, период проведения, проверяющий орган.

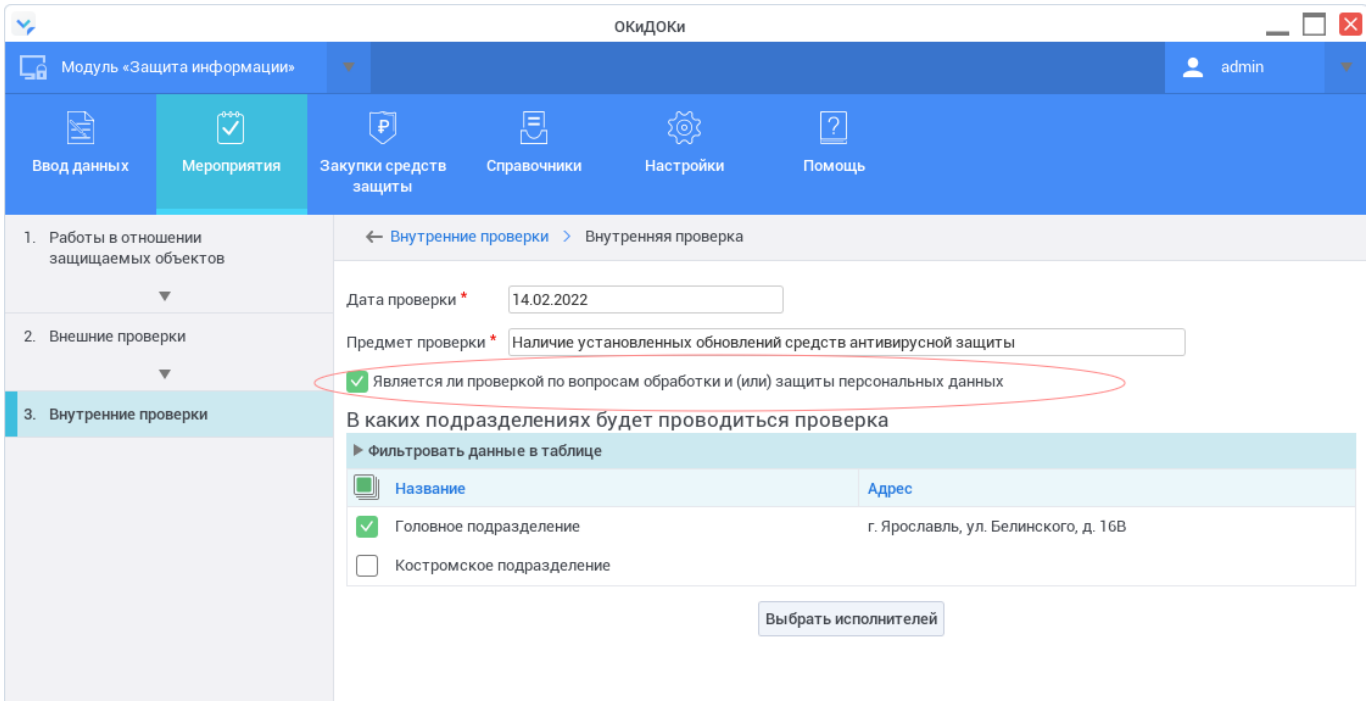
4.2.2 Подраздел «Документация по внешним проверкам»

В данном подразделе к введенным ранее внешним проверкам можно добавить документацию, являющуюся основанием или результатом проведения проверки.

При загрузке документации следует иметь в виду, что помещение в базу данных программного комплекса «ОКиДОКи» документации, содержащей защищаемую информацию, может повысить требования к защите программного комплекса как информационной системы.

4.3 Подраздел «Внутренние проверки»

В данном подразделе вводится общая информация о планируемых и проведенных внутренних проверках, аудитах в отношении защищаемых объектов: дата, предмет проверки, исполнители из числа сотрудников организации.



В случае, если для проверки указано, что в ее предмет входят вопросы обработки и (или) защиты персональных данных, такая проверка может быть включена в план внутренних проверок соблюдения требований по обращению с персональными данными и обеспечению их безопасности, разрабатываемый в модуле «Документы ПДн и СКЗИ».

5 Закупки средств защиты

5.1 Подраздел «Учет закупок»

В данном подразделе ведется учет фактов приобретения средств защиты информации — оборудования и лицензий, а также сертификатов технической поддержки средств защиты информации. Если лицензия бессрочная либо было приобретено оборудование, дату окончания права использования следует оставить пустой.

5.2 Подраздел «Анализ потребностей»

В данном подразделе можно оценить потребность в средствах защиты информации и сертификатах технической поддержки на любую дату.

При оценке потребности учитываются введенные стандарты защиты и их связь с техническими средствами, сегментами информационных систем и информационно-телекоммуникационными сетями, то есть подсчитывается число мест, где средство защиты информации должно быть установлено (поле «Требуется установить»). Также принимается во внимание число мест, где средство защиты информации установлено фактически, независимо от того, требуется оно там или нет (поле «Всего установлено»). Сумма объемов закупок средства защиты без даты окончания права использования, либо срок использования которых еще не истек на дату, на которую оценивается потребность, определяет число имеющихся средств защиты (лицензий) (поле «В наличии на указанную дату»). Разность требуемого и имеющегося отображается в поле «Итого необходимо приобрести».

Следует обратить внимание, что подсчет средств защиты, устанавливаемых на технические средства, программный комплекс «ОКиДОКи» выполняет автоматически. Однако для средств защиты информации сетевого уровня, защищающих сегменты информационных систем и информационно-телекоммуникационные сети в целом, может быть важна топология защищаемых систем, которая программному комплексу «ОКиДОКи» неизвестна. Например, если требуется защитить 3 информационные системы межсетевым экраном с одинаковыми характеристиками, то в зависимости от их взаимной топологии может быть достаточно одного межсетевого экрана либо потребуется два или три — например, если системы расположены в разных сетях. Поэтому для таких средств защиты информации их необходимое число должно быть введено пользователем вручную, основываясь на имеющейся проектной документации на систему защиты информации. Если это число не введено, итоговая потребность в средствах защиты информации не отображается, так как не может быть определена.

Результаты анализа потребности в средствах защиты информации могут быть выгружены в виде спецификации.

6 Справочники

В этом разделе можно добавить собственные значения к некоторым справочникам. Добавленные значения будут доступны только при работе с текущей организацией. Если требуется изменить «стандартные» справочные значения, это можно сделать через модуль «Администратор».

7 Настройки

В этом разделе можно изменять параметры работы модуля «Защита информации» применительно к текущей организации.

7.1 Подраздел «Импорт данных»

7.1.1 Подраздел «Типы технических средств»

В данном подразделе можно добавить преобразования вида «Тип загружаемых технических средств → Тип в программном комплексе «ОКиДОКи», для того чтобы обеспечить загрузку данных о технических средств из файлов, выгруженных из программы «1С», в случае, если файлы содержат типы, отличные от типов, используемых в программном комплексе «ОКиДОКи».

В случае, если для конкретной организации задано преобразование для того же типа загружаемых технических средств, что и «стандартное» преобразование (заданное для всех организаций, работающих с данным сервером программного комплекса «ОКиДОКи», в модуле «Администратор»), то преобразование для конкретной организации будет иметь приоритет.

7.2 Подраздел «Напоминания»

В данном подразделе можно включить либо отключить напоминания об истечении лицензий и сертификатов технической поддержки средств защиты информации.

8 Официальная информация о продукте

Правообладатель: общество с ограниченной ответственностью «Стандарт безопасности» (подтверждено свидетельством о государственной регистрации программы для ЭВМ № 2018665012).

Адрес правообладателя: 150049, Ярославская область, г. о. город Ярославль, г. Ярославль, Мышкинский проезд, д. 10, помещ. 46.

Официальный сайт: www.yarsec.ru.

Телефон для связи по вопросам приобретения продукта: (4852) 587-300.

Электронный адрес службы технической поддержки и консультирования по работе с продуктом: okihelp@yarsec.ru.

Телефон службы технической поддержки и консультирования по работе с продуктом: 8-800-700-71-17.

Программный комплекс «ОКиДОКи» включен в Единый реестр российских программ для электронных вычислительных машин и баз данных (запись № 7000 от 7 октября 2020 г.).