

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ
программного комплекса «ОКиДОКи»
версия 2.8

Модуль «Защита информации»

Ярославль

2020

Оглавление

1	Общие сведения.....	3
1.1	Что такое «ОКиДОКи».....	3
2	Ввод данных.....	4
2.1	Подраздел «Организация».....	4
2.2	Подраздел «Сотрудники».....	4
2.3	Подраздел «Помещения».....	5
2.4	Подраздел «Информационная инфраструктура».....	5
2.4.1	Подраздел «Информационные системы».....	5
2.4.2	Подраздел «Абонентские пункты».....	5
2.4.3	Подраздел «Объекты КИИ».....	5
2.4.4	Подраздел «Средства защиты информации».....	5
2.4.5	Подраздел «Стандарты рабочих мест».....	6
2.4.6	Подраздел «Технические средства».....	6
3	Мероприятия по ИБ.....	7
3.1	Подраздел «Работы в отношении защищаемых объектов».....	7
3.1.1	Подраздел «Учет работ».....	7
3.1.2	Подраздел «Документация по работам».....	7
3.1.3	Подраздел «Область проведения работ».....	7
3.1.4	Подраздел «Просмотр работ по конкретным объектам».....	7
3.2	Подраздел «Внешние проверки в области ИБ».....	8
3.2.1	Подраздел «Учет внешних проверок».....	8
3.2.2	Подраздел «Документация по внешним проверкам».....	8
3.3	Подраздел «Внутренние проверки в области ИБ».....	8
4	Справочники.....	10
5	Настройки.....	11
5.1	Подраздел «Импорт данных».....	11
5.1.1	Подраздел «Типы технических средств».....	11
6	Официальная информация о продукте.....	12

1 Общие сведения

1.1 Что такое «ОКиДОКи»

«ОКиДОКи» — модульная система автоматизированного создания и управления документами в области 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 мероприятий в области обеспечения информационной безопасности (работ по защите информации, внешних и внутренних проверок).

2 Ввод данных

2.1 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.

Скриншот интерфейса модуля «Защита информации» (ОКИДОКИ) в разделе «Организация». В левом меню выделен пункт «1. Организация». В правой части экрана, под заголовком «Территориальные подразделения», находится флажок «Наличие территориальных подразделений», который обведен красным кругом. Под ним есть подсказка: «Выставьте этот флажок, если ваша организация находится более чем по одному адресу, то есть имеет территориально распределенные подразделения». Ниже расположены поля для ввода: «Адрес фактического местонахождения организации» (содержит текст «г. Москва, Ленинградский проспект, д. 37, корпус 1»), «Почтовый индекс», «КПП (для обособленных подразделений)». Также есть флажок «Наличие вахты или контрольно-пропускного пункта, куда сдаются ключи в конце рабочего дня». Внизу есть выпадающий список «Контролируемая зона определена:» со значением «по периметру охраняемой территории здания». В самом низу есть таблица «Меры по обеспечению контролируемой зоны» с заголовком «Описание меры» и одной строкой: «создание надежных препятствий на возможных путях несанкционированного проникновения в контролируемую зону».

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

2.2 Подраздел «Сотрудники»

Список сотрудников организации можно ввести как вручную, так и импортировав из файла с расширением xls, полученного путем загрузки из программы «1С». Если помимо имен сотрудников файл содержит их должности (во втором столбце) и отделы (в третьем столбце), эти данные так же будут загружены.

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

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

2.3 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.

2.4 Подраздел «Информационная инфраструктура»

В этом подразделе вводятся данные об информационных системах, в том числе автоматизированных системах управления, информационно-телекоммуникационных сетях, абонентских пунктах сторонних информационных систем, а также входящих в их состав технических средствах и применяемых средствах защиты информации.

2.4.1 Подраздел «Информационные системы»

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.

В данном подразделе доступна для выгрузки в виде документа карточка информационной системы, отражающая ее основные характеристики.

2.4.2 Подраздел «Абонентские пункты»

В этом подразделе вводятся данные о защищаемых рабочих местах сторонних (внешних, не принадлежащих вашей организации) информационных систем.

2.4.3 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).

2.4.4 Подраздел «Средства защиты информации»

В данном подразделе вводится информация о применяемых средствах защиты

информации. Для получения информации о средстве защиты (производитель, версия, номер и срок действия сертификата, характеристики, подтверждаемые сертификатом) обратитесь к имеющейся документации на него.

2.4.5 Подраздел «Стандарты рабочих мест»

Для ускорения ввода данных об однотипных технических средствах (имеющих одинаковую операционную систему и / или состав установленных средств защиты информации) можно описать стандарты рабочих мест.

Для каждого стандарта следует указать одну или несколько информационных систем, для которых он применяется. У одной информационной системы может быть несколько стандартов (например, если в системе используются рабочие места нескольких типов). После этого, при добавлении технического средства в состав информационной системы, у которой есть хотя бы один стандарт, будет доступна опция «Задать требование о соответствии технического средства стандарту». При выборе данной опции можно скопировать характеристики технического средства из стандарта, чтобы не вводить их вручную, если есть уверенность в том, что техническое средство в реальности этими характеристиками обладает. Кроме того, в подразделе «Технические средства» для каждого технического средства, для которого задано требование о соответствии хотя бы одному стандарту, можно видеть, каким стандартам оно действительно соответствует и каким нет.

2.4.6 Подраздел «Технические средства»

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

3 Мероприятия по ИБ

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

3.1 Подраздел «Работы в отношении защищаемых объектов»

3.1.1 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.

3.1.2 Подраздел «Документация по работам»

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

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.

3.1.3 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.

3.1.4 Подраздел «Просмотр работ по конкретным объектам»

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

ОКИДОКИ

Модуль "Защита информации" admin

Ввод данных Мероприятия по ИБ Справочники Настройки Помощь

1. Работы в отношении защищаемых объектов

1.1. Учет работ

1.2. Документация по работам

1.3. Области проведения работ

1.4. Просмотр работ по конкретным объектам

2. Внешние проверки в области ИБ

3. Внутренние проверки в области ИБ

Просмотр работ по конкретным объектам

Информационные системы Информационно-телекоммуникационные сети Абонентские пункты Средства защиты информации

Информационная система Бухгалтерия

Год начала работ

Год окончания работ

Статус готовности работ

Работы в отношении информационной системы

Название	Тип	Описание	Дата начала	Дата окончания	Исполнитель	Ответственный сотрудник
Моделирование угроз безопасности	моделирование угроз безопасности защищаемой информации		15.06.2020	31.08.2020	ООО «ИБ-Сервис»	

3.2 Подраздел «Внешние проверки в области ИБ»

3.2.1 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.

3.2.2 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.

3.3 Подраздел «Внутренние проверки в области ИБ»

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».

ОКИДОКИ

Модуль "Защита информации" admin

Ввод данных Мероприятия по ИБ Справочники Настройки Помощь

1. Работы в отношении защищаемых объектов

2. Внешние проверки в области ИБ

3. Внутренние проверки в области ИБ

← Внутренние проверки в области ИБ > Внутренняя проверка

Дата проверки * 01.02.2021

Предмет проверки * применение средств антивирусной защиты

✓ Является ли проверкой по вопросам обработки и (или) защиты персональных данных

В каких подразделениях будет проводиться проверка

Название	Адрес
✓ Головное подразделение	г. Москва, Ленинградский проспект, д. 37, корпус 1

Выбрать исполнителей

4 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».

5 Настройки

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

5.1 Подраздел «Импорт данных»

5.1.1 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.

6 Официальная информация о продукте

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

Адрес правообладателя: 150047, г. Ярославль, ул. Угличская, д. 39В.

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: oki@yarsec.ru.

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