

**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**  
**программного комплекса «Киберстаб»**  
**версия 1.0**

**Модуль «Модель угроз»**

**Ярославль**

**2024**

## Оглавление

1 Общие сведения.....	3
1.1 Что такое «Киберстаб».....	3
1.2 С чего начать?.....	3
1.3 Как создавать документы?.....	4
2 Ввод данных.....	5
2.1 Подраздел «Организация».....	5
2.2 Подраздел «Информационные системы».....	5
2.3 Подраздел «Объекты КИИ».....	6
2.4 Подраздел «Согласующие лица».....	6
2.5 Подраздел «Виды рисков (ущербов) и возможные негативные последствия»...7	
2.6 Подраздел «Информационные ресурсы и компоненты».....	8
2.7 Подраздел «Источники угроз безопасности информации».....	8
2.8 Подраздел «Техники для построения сценариев реализации угроз».....	9
2.9 Подраздел «Условия реализации угроз».....	9
2.10 Подраздел «Список актуальных угроз».....	9
2.11 Подраздел «Связи актуальных угроз с объектами воздействия».....	10
3 Документы.....	11
4 Официальная информация о продукте.....	13

# 1 Общие сведения

## 1.1 Что такое «Киберстаб»

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

Модуль «Модель угроз» позволяет провести моделирование угроз безопасности защищаемой информации, обрабатываемой в информационных системах.

## 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.

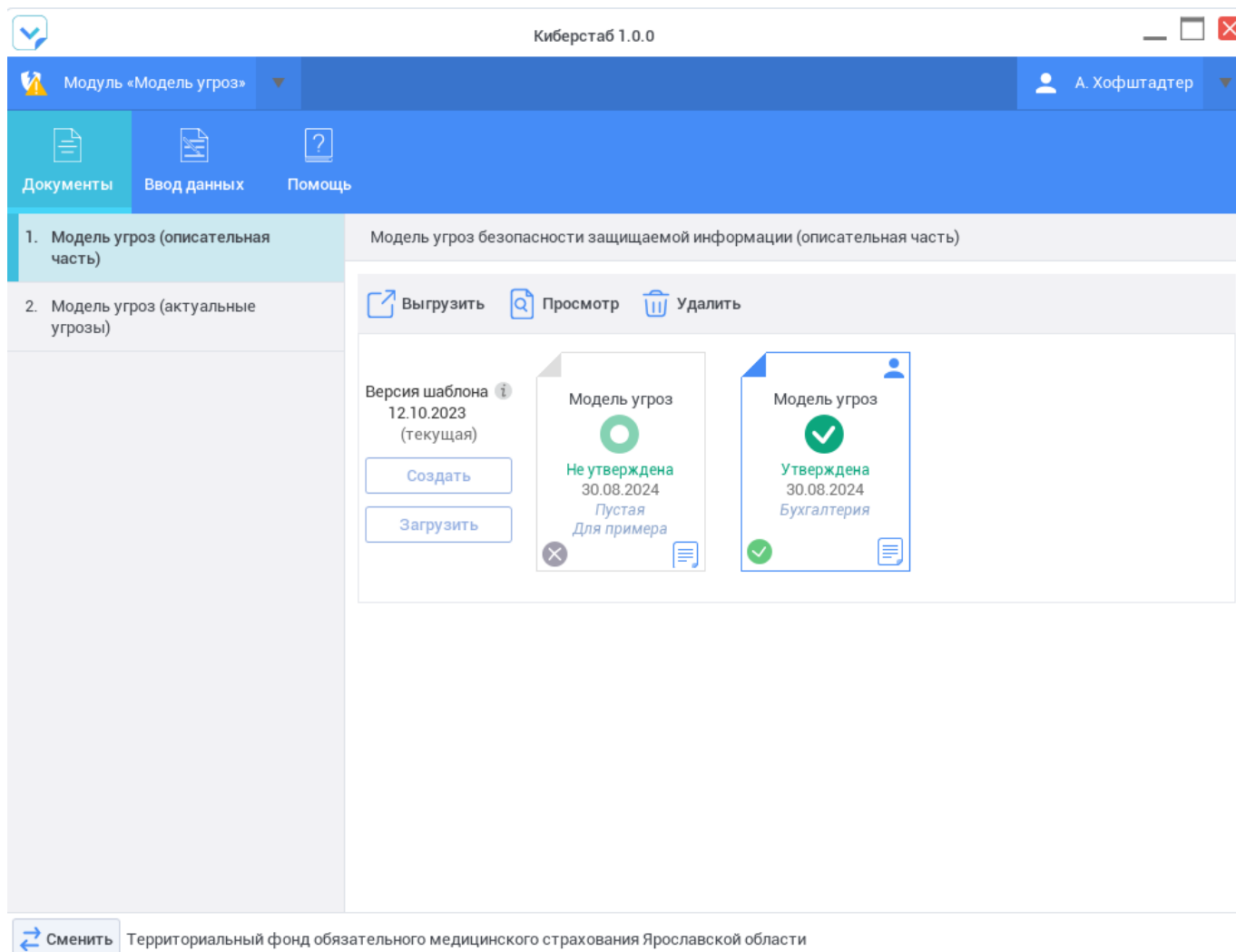
В каждом пункте левого меню данные не отправляются на сервер до тех пор, пока не будет нажата кнопка «Сохранить изменения в БД».

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 ответственного пользователя криптосредств**»).

### 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 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.

Киберстаб 1.0.0

Модуль «Модель угроз»

А. Хофштадтер

Документы Ввод данных Помощь

1. Организация

Территориальные подразделения

1.1. Реквизиты юридического лица

1.2. Территориальные подразделения

Выставьте этот флажок, если ваша организация находится более чем по одному адресу, то есть имеет территориально подразделения

☒ Наличие территориальных подразделений

Головное подразделение \* Головное подразделение (г. Ярославль, ул. Советская, д. 1)

2. Информационные системы

3. Объекты КИИ

4. Согласующие лица

5. Виды рисков (ущербов) и возможные негативные последствия

6. Информационные ресурсы и компоненты

7. Источники угроз безопасности информации

Территориальные подразделения

Фильтровать данные в таблице

Название	Адрес
Головное подразделение	г. Ярославль, ул. Советская, д. 11/9
Тверское подразделение	г. Тверь, ул. Коммунистов, д. 5
Подразделение 2	

Число строк: 3

+ Добавить территориальное подразделение Удалить выделенные строки

Сохранить изменения в БД Отменить все изменения

Для сохранения данных нажмите ... «Отменить все изменения» вернет все ...

Сменить Территориальный фонд обязательного медицинского страхования Ярославской области

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 «Информационные системы»

В этом подразделе вводятся данные об информационных системах, в которых осуществляется обработка защищаемой информации.

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.

При создании информационной системы можно выбрать, будет ли проводиться моделирование угроз по системе в целом (выбор по умолчанию), либо отдельно по каждому сегменту информационной системы.

Для дальнейшего моделирования угроз необходимо ввести виды защищаемой информации и предъявляемые характеристики безопасности информации, а также классы / уровни защищенности в случае, если информационная система классифицируется по тем или иным требованиям защиты информации.

Список используемого прикладного программного обеспечения можно ввести как вручную, так и импортировав из файла с расширением xls,xlsx или ods. Образец файла загрузки можно выгрузить, нажав на соответствующую кнопку.

В подразделе «Шаблоны информационных систем» можно на основе ранее введенной информационной системы создать «шаблон», в котором зафиксируется введенная по системе информация. Дальнейшее изменение данных о системе не будет оказывать влияния на шаблон. На основе шаблона можно создавать новые информационные системы, в которые будет скопирована информация, содержащаяся в шаблоне (кнопка «Создать ИС по шаблону» в подразделе «Описание информационных систем»). Шаблоны информационных систем могут передаваться в другие организации, эксплуатирующие программный комплекс «Киберстаб» (подробнее о настройках передачи шаблонов информационных систем см. руководство администратора на программный комплекс «Киберстаб»).

## **2.3 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.

Для дальнейшего моделирования угроз необходимо ввести категории значимости объектов критической информационной инфраструктуры.

## **2.4 Подраздел «Согласующие лица»**

В подразделе «Штатное расписание» описываются отделы и должности, существующие в организации. Штатное расписание можно ввести как вручную, так и импортировав из файла с расширением xls,xlsx или ods. Образец файла загрузки можно выгрузить, нажав на соответствующую кнопку.

Список сотрудников организации в подразделе «Сотрудники» так же можно ввести как вручную, так и импортировав из файла с расширением xls,xlsx или ods. 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 «Киберстаб»).

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

Для работы в модуле «Модель угроз» достаточно ввести только данные о сотрудниках и сторонних лицах, которые будут участвовать в подписании (утверждении, согласовании) моделей угроз безопасности защищаемой информации. У этих сотрудников необходимо выставить флажок «Имеет право подписи».

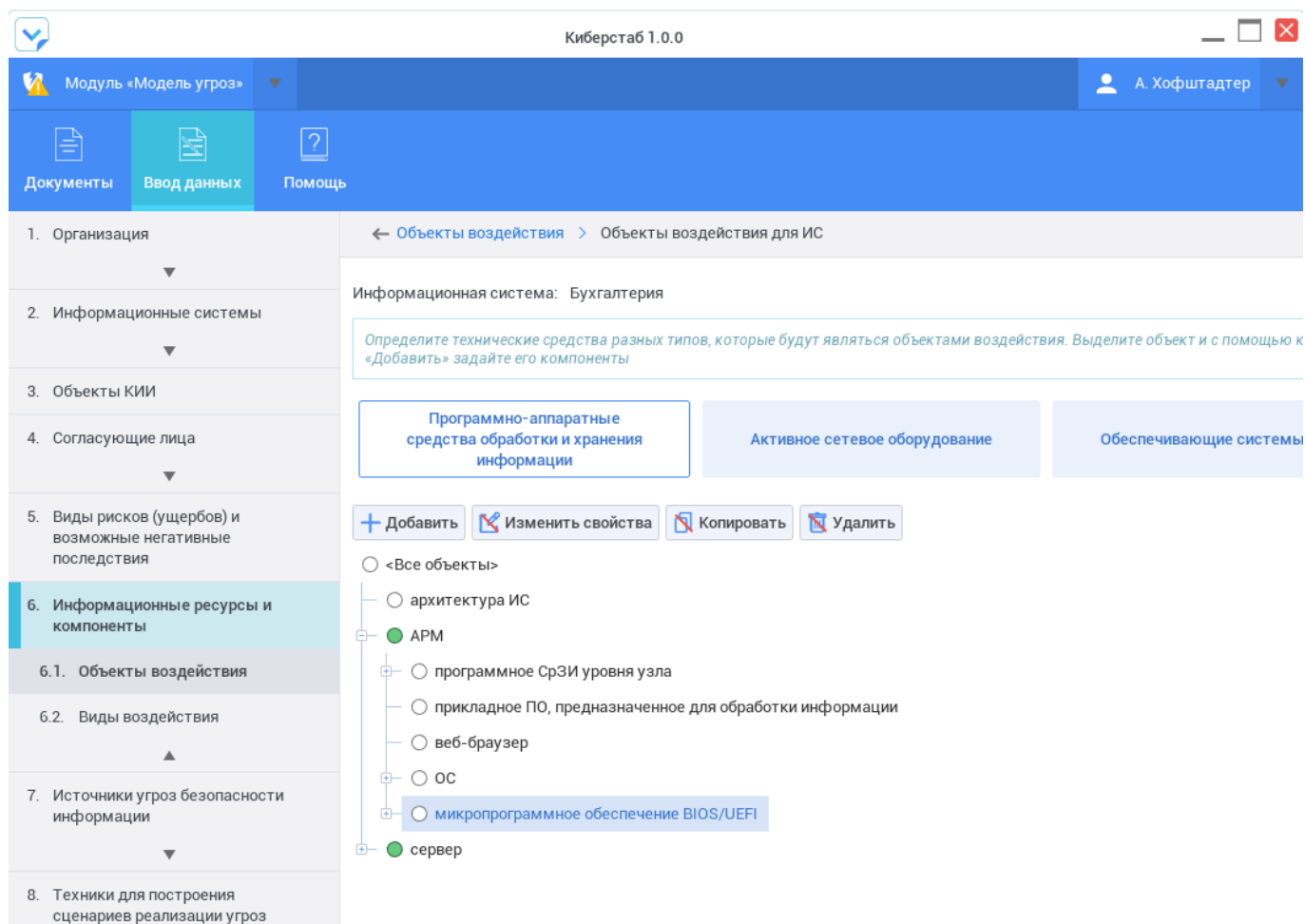
## 2.5 Подраздел «Виды рисков (ущербов) и возможные негативные последствия»

В данном подразделе определяются возможные негативные последствия от нарушения характеристик безопасности защищаемой информации. Для облегчения выбора по каждому уровню ущерба предлагаются уточняющие вопросы, после ответа на которые и нажатия кнопки «Применить» будут предложены подходящие

негативные последствия.

## 2.6 Подраздел «Информационные ресурсы и компоненты»

В данном подразделе определяются возможные объекты воздействия, воздействие на которые может нарушить характеристики безопасности защищаемой информации. Объекты воздействия, добавляемые пользователем, отмечены зеленым цветом (их можно удалять); объекты воздействия, добавляемые автоматически, отмечены белым цветом (их удаление невозможно).



В качестве возможных видов воздействия на объекты могут быть выбраны стандартные виды, либо добавлены произвольные виды применительно к конкретному объекту воздействия.

## 2.7 Подраздел «Источники угроз безопасности информации»

В данном подразделе определяются возможные нарушители безопасности защищаемой информации, их цели и применяемые способы реализации угроз.

На основании ранее введенных данных об информационных системах (классы / уровни защищенности, категория значимости для объектов критической информационной инфраструктуры) формируется предварительный список возможных нарушителей, из которого следует выбрать тех, которые должны быть рассмотрены в модели угроз (подраздел «Возможные нарушители»).



В качестве возможных целей реализации угроз могут быть выбраны стандартные цели, либо добавлены произвольные цели применительно к конкретному нарушителю.

Аналогично, в качестве возможных способов реализации угроз могут быть выбраны стандартные способы, либо добавлены произвольные способы применительно к конкретному нарушителю.

## **2.8 Подраздел «Техники для построения сценариев реализации угроз»**

В данном подразделе определяются техники матрицы MITRE ATT&CK, актуальные для каждой информационной системы. Для выбора техник необходимо отметить подходящие фильтры и нажать кнопку «Применить», после чего все рекомендуемые для включения в модель угроз техники будут выделены автоматически.

## **2.9 Подраздел «Условия реализации угроз»**

В данном подразделе перечислены прочие условия, которые могут влиять на актуальность угроз. Некоторые из условий могут быть автоматически выделены / не выделены и заблокированы — это зависит от ранее введенных данных об информационной системе, возможных объектах воздействия в ее составе, а также от актуальности / неактуальности других условий реализации.

## **2.10 Подраздел «Список актуальных угроз»**

В данном подразделе осуществляется непосредственный расчет актуальности угроз безопасности защищаемой информации. На актуальность угрозы влияет множество факторов: наличие соответствующих объектов воздействия и нарушителей; соответствие целей нарушителей и применяемых ими способов реализации возможным видам воздействия на объекты и негативным последствиям, которые могут наступить в результате такого воздействия; актуальность соответствующих условий реализации.

В случае, если список актуальных угроз уже был составлен, но исходные данные для моделирования угроз изменились, у соответствующей информационной системы появится пометка «Список угроз требует перерасчета». В этом случае следует нажать кнопку «Обновить актуальные угрозы».

Киберстаб 1.0.0

Модуль «Модель угроз»

А. Хофштадтер

Документы Ввод данных Помощь

1. Организация

2. Информационные системы

3. Объекты КИИ

4. Согласующие лица

5. Виды рисков (ущербов) и возможные негативные последствия

6. Информационные ресурсы и компоненты

7. Источники угроз безопасности информации

8. Техники для построения сценариев реализации угроз

9. Условия реализации угроз

10. Список актуальных угроз

11. Связи актуальных угроз с объектами воздействия

← Список актуальных угроз > Актуальные угрозы для ИС

Информационная система: Бухгалтерия

Рассчитайте перечень актуальных угроз, определяемый на основе ранее введенных данных

Список угроз требует перерасчета, поскольку изменились исходные данные, влияющие на актуальность угроз

Обновить актуальные угрозы

Список угроз

Идентификатор угрозы	Название угрозы
УБИ.004	угроза аппаратного сброса пароля BIOS
УБИ.008	угроза восстановления и/или повторного использования аутентификационной информации
УБИ.009	угроза восстановления предыдущей уязвимой версии BIOS
УБИ.012	угроза деструктивного изменения конфигурации/среды окружения программ
УБИ.013	угроза деструктивного использования декларированного функционала BIOS
УБИ.014	угроза длительного удержания вычислительных ресурсов пользователями
УБИ.018	угроза загрузки нештатной ОС
УБИ.022	угроза избыточного выделения оперативной памяти

✓ Готово ✗ Отмена Для сохранения данных нажмите «Готово» «Отмена» вернет все значения к исходным

Сменить Территориальный фонд обязательного медицинского страхования Ярославской области

## 2.11 Подраздел «Связи актуальных угроз с объектами воздействия»

В данном подразделе окончательно определяются объекты воздействия для угроз, признанных актуальными. Для большинства угроз связи со всеми возможными объектами воздействия будут заданы автоматически (метка «Все возможные связи заданы» в столбце «Все связи заданы»). Для тех угроз, для которых доступна возможность добавить связь с дополнительными объектами воздействия, отображается метка «Ни одна из доступных связей не задана» - при переходе на панель редактирования таких угроз можно отметить флажками дополнительные объекты воздействия для угрозы, если это необходимо.

Киберстаб 1.0.0

Модуль «Модель угроз»

А. Хофштадтер

Документы Ввод данных Помощь

1. Организация

2. Информационные системы

3. Объекты КИИ

4. Согласующие лица

5. Виды рисков (ущербов) и возможные негативные последствия

6. Информационные ресурсы и компоненты

7. Источники угроз безопасности информации

8. Техники для построения сценариев реализации угроз

9. Условия реализации угроз

10. Список актуальных угроз

11. Связи актуальных угроз с объектами воздействия

← Связи актуальных угроз с объектами воздействия > Связи актуальных угроз с объектами воздействия для ИС

Информационная система: Бухгалтерия

Задайте связи с объектами воздействия для угроз, требующих внимания пользователя, опираясь на графические рекомендации в столбце «Все связи заданы»

Задать все возможные связи угроз с объектами воздействия

Связи угроз с объектами воздействия

Идентификатор угрозы	Название угрозы	Объекты воздействия	Все связи заданы
УБИ.004	угроза аппаратного сброса пароля BIOS	микропрограммное обеспечение BIOS/UEFI -> АРМ; микропрограммное обеспечение BIOS/UEFI -> сервер	✓
УБИ.008	угроза восстановления и/или повторного использования аутентификационной информации	учетные записи пользователей (идентификационная и аутентификационная информация) -> программное СрЗИ уровня узла -> АРМ; учетные записи пользователей (идентификационная и аутентификационная информация)	✓

Готово Отмена Для сохранения данных нажмите «Готово» «Отмена» вернет все значения к исходным

Сменить Территориальный фонд обязательного медицинского страхования Ярославской области

### 3 Документы

Модель угроз безопасности защищаемой информации в силу большого объема создаваемого документа формируется в виде двух томов — описательная часть и собственно расчет актуальных угроз. Для каждой информационной системы, ее

Киберстаб 1.0.0

Модуль «Модель угроз»

А. Хофштадтер

Документы Ввод данных Помощь

1. Модель угроз (описательная часть)

2. Модель угроз (актуальные угрозы)

Модель угроз безопасности защищаемой информации (описательная часть)

Выгрузить Просмотр Удалить

Версия шаблона 12.10.2023 (текущая)

Создать Загрузить

Модель угроз

Не утверждена 30.08.2024 Пустая Для примера

Модель угроз

Утверждена 30.08.2024 Бухгалтерия

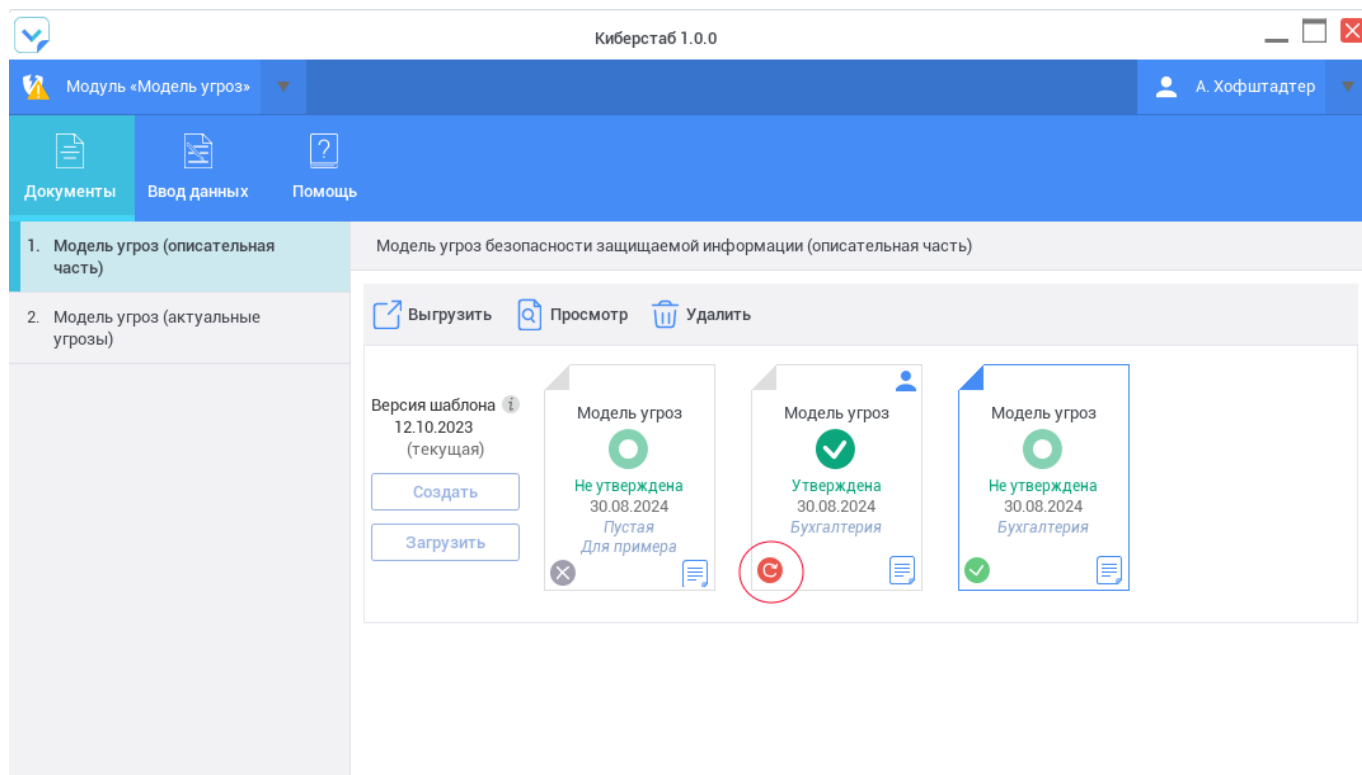
Модель угроз

Не утверждена 30.08.2024 Бухгалтерия

сегмента или абонентского пункта может быть создан или загружен только один актуальный документ.

Документы, 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 нарушителей и т. п.), и эти изменения затронули содержание конкретного документа, у него появится значок в виде красной стрелки «Утратил актуальность».



На текущий момент выгрузка модели угроз доступна только в формате .odt.

#### **4 Официальная информация о продукте**

Правообладатель: общество с ограниченной ответственностью «Стандарт безопасности» (подтверждено свидетельством о государственной регистрации программы для ЭВМ № 2024616571 от 21 марта 2024 года).

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

Официальный сайт: [www.yarsec.ru](http://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](mailto:okihelp@yarsec.ru).

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