**Международная Ассоциация пользователей и разработчиков электронных библиотек и новых информационных технологий**

**(Ассоциация ЭБНИТ)**

|  |  |  |
| --- | --- | --- |
|  |  | **УТВЕРЖДАЮ**Директор по развитию Ассоциация ЭБНИТ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_М.В. Гончаров«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2018 г. |

**Комплексное решение АБИС ИРБИС64/128 для Linux (АБИС ИРБИС 64/128)**

**руководство администратора информационной безопасности**

Листов 18

**2022**

**Аннотация**

Настоящий документ описывает работу администратора информационной безопасности (АИБ) САБ ИРБИС 64/128. Роль АИБ может выполнять Администратор САБ ИРБИС 64/128.

Настоящий документ разработан в соответствии с требованиями РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов». Оформление выполнено с использованием ГОСТ 2.105-95.

## Описание операций, проводимых в процессе эксплуатации АИБ системы

### *Начало и завершение работы*

Запуск Панели администрирования информационной безопасности производится следующим способом:

* ввести в браузере адрес http://<адрес сервера> /?id=AIS/Show, будучи авторизованным с ролью АИБ.

После запуска Панели администрирования информационной безопасности на экране отобразится окно Панели администрирования информационной безопасности ().

Рисунок 1 – Окно Панели администрирования информационной безопасности

Выход из Панели администрирования информационной безопасности осуществляется закрытием окна браузера.

### *Навигация по объектам Панели администрирования информационной безопасности*

Пользовательский интерфейс Панели администрирования информационной безопасности организован как тонкий клиент (Рисунок 2).

Рисунок 2 – Интерфейс Панели администрирования информационной безопасности

Для просмотра объекта и его свойств необходимо осуществить двойной щелчок левой кнопкой мыши на объекте.

### *Администрирование механизмов защиты информации*

#### *Настройка политики безопасности*

Настройка и поддержание в актуальном состоянии параметров политики безопасности информации входит в обязанности АИБ системы.

Для настройки параметров политики безопасности информации используется Панель администрирования информационной безопасности.

Политика безопасности, реализуемая АИБ системы с использованием Панели администрирования информационной безопасности, определяет возможности (на уровне программных средств) по контролю действий администраторов и пользователей ИРБИС 64/128, настройке параметров и разграничению прав доступа к информации.

Средства Панели администрирования информационной безопасности позволяют АИБ системы контролировать соответствие фактических полномочий и действий как пользователей, так и администраторов.

Рисунок 3 – Определение политики безопасности

Рисунок 4 – Задание политики безопасности для администратора системы

Подключение доменного пользователя/группы пользователей из домена Windows в систему осуществляется следующими способами:

Рисунок 5 – Добавление доменного пользователя в группу

Права доступа в системе задаются для конкретных объектов системы – база данных, и для функций.

Рисунок 6 – Установка прав для групп «Администраторы АИБ»

#### *Просмотр протокола доступа*

Вызов окна протокола доступа производится при помощи закладки «Протокол доступа» в Панели администрирования информационной безопасности (7).

Рисунок 7 – Окно просмотра протокола доступа

Протокол доступа организован в виде таблицы. В протоколе доступа отражены записи, содержащие следующую информацию:

* Объект – наименование объекта, к которому обращается пользователь;
* Идентификатор – идентификатор объекта;
* Время – дата и время выполнения операции;
* Операция – наименование выполняемой операции;
* Результат – информация о том, успешное или неуспешное действие пытался совершить пользователь;
* IP адрес – IP адрес пользователя, осуществляющего доступ к объекту.

Работа с протоколом доступа осуществляется при помощи клавиш управления курсором, полос прокрутки, главного меню и панели инструментов.

**Примечание:** Периодически, не реже 1 (одного) раза в неделю, администратор информационной безопасности ИРБИС 64/128 должен проводить анализ журналов регистрации событий на предмет выявления фактов попытки несанкционированного доступа к ресурсам ИРБИС 64/128.

#### *Очистка протокола доступа*

Существует только один способ очистки протокола доступа – путем сохранения его в файл. Для того чтобы очистить протокол доступа, необходимо в окне протокола доступа на панели инструментов выбрать пункт «Очистить». После этого появится окно, в котором необходимо указать путь до файла, в который будет сохранен протокол.

Рисунок 8 – Окно очистки протокола доступа

Рекомендуется ежемесячно очищать протокол доступа. Архивные копии протокола доступа хранятся на сетевом ресурсе. Хранению подлежат только архивные копии протокола доступа, содержащие информацию о деятельности пользователей за последние 5 лет, остальные архивные копии уничтожаются администратором информационной безопасности.

Доступ к сетевому ресурсу имеет только администратор информационной безопасности.

#### *Просмотр протокола доступа, сохраненного в файл*

.

Рисунок 9 – Протокол доступа, сохраненного в файл

### *Составление и поддержание в актуальном состоянии списка прав доступа к ресурсам ИРБИС 64/128*

В обязанности администратора информационной безопасности ИРБИС 64/128 входит составление и поддержание в актуальном состоянии списка прав доступа и полномочий пользователей ИРБИС 64/128, а также проведение периодического (не реже одного раза в год) контроля на соответствие прав доступа и полномочий, предоставленных в ИРБИС 64/128 пользователям, правам доступа и полномочиям сотрудников подразделения, отраженным в списке прав доступа и полномочий сотрудников.

### *Периодический контроль настроек механизмов защиты и целостности прикладного ПО ИРБИС 64/128*

Периодически, не реже 1 (одного) раза в год, администратор информационной безопасности ИРБИС 64/128 должен проводить контроль настроек механизмов защиты в ИРБИС 64/128 на предмет их соответствия установленным в настоящем разделе требованиям и контроль целостности прикладного ПО ИРБИС 64/128, который должен включать:

* проверку настроек политики безопасности;
* контроль целостности ПО ИРБИС 64/128.

К проверке работоспособности Панели администрирования информационной безопасности в части защиты информации администратором информационной безопасности ИРБИС 64/128 могут быть привлечены пользователи ИРБИС 64/128.

Контроль целостности осуществляется при каждом запуске ИРБИС 64/128 средствами комплекса автоматически. В случае нарушения целостности выдается окно с соответствующим сообщением, и дальнейшая работа блокируется.

По результатам тестирования администратор информационной безопасности ИРБИС 64/128 должен составить протокол тестирования, содержащий все обнаруженные ошибки и замечания. Все протоколы тестирования должны храниться у администратора информационной безопасности ИРБИС 64/128 в течение 3 (трех) лет.

При обнаружении ошибок Панели администрирования информационной безопасности, которые могут серьезно снизить безопасность информации в ИРБИС 64/128, администратор информационной безопасности ИРБИС 64/128 должен уведомить руководство. На основании указаний руководства, администратор информационной безопасности ИРБИС 64/128 может приостановить доступ пользователей ИРБИС 64/128 к системе до исправления ошибок.

Контроль целостности защищаемой информации обеспечивается за счет внутренних механизмов СУБД ИРБИС 64/128.

1. Перечень событий, регистрируемых средствами Панели администрирования информационной безопасности ИРБИС 64/128

В ИРБИС 64/128 средствами Панели администрирования информационной безопасности фиксируются следующие события информационной безопасности:

1. операций по изменению параметров настроек технических и (или) программных средств защиты информации;
2. операций, связанных с созданием, копированием, в том числе резервным, и (или) удалением ресурсов доступа;
3. операций, связанных с управлением учетными записями;
4. операций, связанных с управлением правами логического доступа;
5. операций, связанных с авторизацией, завершением, и (или) прерыванием (приостановкой) осуществления эксплуатационным персоналом логического доступа к ИРБИС 64/128;
6. операций, связанных с действиями эксплуатационного персонала при осуществлении логического доступа в ИРБИС 64/128;
7. операций, связанных с выполнением установки или обновления системного программного обеспечения серверного и сетевого оборудования, программного обеспечения систем управления базами данных, программного обеспечения технических и (или) программных средств защиты информации;
8. результатов выполнения операций по контролю состава программного обеспечения;
9. операций, связанных с использованием разблокированных коммуникационных портов и встроенных устройств ввода-вывода информации;
10. операций по очистке электронных журналов событий информационной безопасности.
11. Перечень событий, классифицируемых в ИРБИС 64/128 как инциденты нарушения информационной безопасности

В ИРБИС 64/128 следующие события можно отнести к инцидентам нарушения информационной безопасности:

1. попытки несанкционированного доступа к информации, которые могут быть классифицированы следующим образом:
2. попытки несанкционированного подключения к защищаемым ресурсам ИРБИС 64/128 субъектов, не являющихся пользователями системы;
3. попытки несанкционированного чтения или изменения информации защищаемых ресурсов ИРБИС 64/128;
4. Нарушение целостности ПО;
5. Сбои и отказы технических средств:
6. сбой технического оборудования (серверы, ЛВС, рабочие станции пользователей);
7. физическое повреждение ЛВС или оборудования;
8. отключение электричества;
9. Воздействие вредоносного кода на объекты ИРБИС 64/128.
10. Перечень аварийных ситуаций и порядок действия в случае их возникновения

**В.1 Перечень аварийных ситуаций**

Возникновение сбоев и неполадок при работе ИРБИС 64/128 сопровождается появлением сообщений о программных ошибках или некорректным поведением ИРБИС 64/128. Возможны следующие аварийные ситуации:

1. Ошибки при работе прикладного программного обеспечения ИРБИС 64/128:
	1. невозможность запуска ИРБИС 64/128;
	2. отказ доступа к ИРБИС 64/128;
	3. отказ доступа к объектам ИРБИС 64/128
	4. «зависание» и ошибки в работе ИРБИС 64/128 при выполнении операций;
	5. устаревшая версия ИРБИС 64/128, не обеспечивающая решение актуальных прикладных задач;
	6. ошибка при обновлении ИРБИС 64/128;
	7. отсутствие данных в ИРБИС 64/128;
	8. наличие некорректных данных в базе данных ИРБИС 64/128;
	9. ошибки в результате неверных настроек ИРБИС 64/128 (настройки панели информационной безопасности, настройки соединения и т.д.);
	10. нарушение целостности ИРБИС 64/128;
2. Ошибки при работе системного и стороннего ПО:
	1. обнаружение вируса;
	2. некорректные действия пользователей: удаление программных или системных файлов;
	3. ошибки при создании резервной копии ИРБИС 64/128 и восстановлении системы;
3. Сбои по техническим причинам:
	1. сбой технического оборудования (сервера СУБД ИРБИС 64/128, сервера, выполняющего функции домен-контроллера, сервера Web-приложений, рабочей станции пользователя);
	2. физическое повреждение ЛВС или ПЭВМ;
	3. отключение электричества;
4. Нарушение информационной безопасности:
	1. утечка информации;
	2. попытка несанкционированного доступа.

**В.2 Действия в случае аварийных ситуаций**

Действия пользователей ИРБИС 64/128 в результате возникновения аварийных ситуаций приведены в таблице В.1.

Рекомендованное время реакции при возникновении аварийных ситуаций приведено в Таблице В2.

Таблица В.1

| **Аварийная ситуация** | **Описание аварийной ситуации** | **Действия** |
| --- | --- | --- |
| **Ошибки при работе ППО ИРБИС 64/128** |
| Невозможность запуска ИРБИС 64/128 | 1. при запуске ИРБИС 64/128 выдается сообщение об ошибке, либо открытия приложения не происходит;
2. при запуске ИРБИС 64/128 выдается сообщение об отсутствии или истечении срока лицензии.
 | Обратиться в службу поддержки пользователей |
| Отказ доступа к ИРБИС 64/128 | 1. при входе в ИРБИС 64/128, выдается сообщение о запрете входа в систему;
2. в случае доступа к ИРБИС 64/128 через Web-интерфейс появляется сообщение о невозможности отображения страницы.
 | 1. вход в ИРБИС 64/128 разрешен определенным пользователям;
2. проверить правильность ввода имени WEB-сервера и псевдонима виртуального каталога в строке адреса обозревателя Internet Explorer;
3. в случае повторения ошибки обратиться в службу поддержки пользователей.
 |
| Отказ доступа к объектам ИРБИС 64/128 | 1. объект ИРБИС 64/128 отсутствует на главной форме;
2. при запуске объекта выдается сообщение об ошибке.
 | Обратиться к администратору системы. |
| «Зависание» или ошибка в работе ИРБИС 64/128 при выполнении операций | Прикладное программное обеспечение зависает и не реагирует на нажатие кнопок мыши, клавиатуры, кнопок ППО. | 1. завершить процесс при помощи диспетчера процессов, запустить ППО и повторить выполнение операции, вызвавшей зависание ПО;
2. в случае повторного зависания обратиться в службу поддержки пользователей.
 |
| Устаревшая версия ИРБИС 64/128 | Выдается сообщение о необходимости обновления ПО. | 1. завершить работу, запустить ИРБИС 64/128 заново;
2. в случае повторения сообщения обратиться в службу поддержки пользователей.
 |
| Отсутствие данных в ИРБИС 64/128 | Отсутствуют данные в ИРБИС 64/128. | Обратиться к администратору системы. |
| Наличие некорректных данных в базе данных ИРБИС 64/128 | Данные, отображаемые в ИРБИС 64/128, некорректны. | Обратиться к администратору системы. |
| Ошибки в результате неверных настроек ИРБИС 64/128 | Невозможность запуска объекта, отказ доступа к объектам ИРБИС 64/128, запрет копии экрана, выдача прочих сообщений. | Обратиться к администратору системы. |
| Нарушение целостности ИРБИС 64/128 | При запуске ИРБИС 64/128 выдается сообщение о нарушении целостности. | Обратиться в службу поддержки пользователей. |
| **Ошибки при работе системного и стороннего ПО** |
| Обнаружение вируса | 1. наблюдается неадекватная работа РС (вывод на экран непредусмотренных сообщений или изображений, медленная работа, самопроизвольный запуск сторонних процессов, исчезновение файлов и каталогов или искажение их содержимого);
2. появление сообщения антивирусного ПО о наличии вирусов.
 | Не запускать какие-либо процессы, приложения, программы, завершить работу с ПО, выключить рабочую станцию и обратиться к администратору информационной безопасности своего подразделения. |
| Некорректные действия пользователей | 1. случайное удаление программных или системных файлов;
2. ввод и сохранение некорректных данных.
 | 1. Обратиться в службу поддержки пользователей;
2. Обратиться к администратору системы.
 |
| **Сбои по техническим причинам** |
| Сбой технического оборудования  | Не включается рабочая станция, не запускается операционная система, не работает печатное устройство. | 1. проверить подключение кабеля рабочей станции к сети питания;
2. проверить подключение основного кабеля питания рабочей станции к блоку питания;
3. проверить подключение кабеля питания монитора;
4. обратиться в службу поддержки пользователей.
 |
| Физическое повреждение ЛВС или ПЭВМ. | Наблюдаются разрывы, перегибы кабеля, нарушения целостности корпуса оборудования. | Обратиться в службу поддержки пользователей. |
| Отключение электричества | Отключение электричества в здании, при этом питание компьютера осуществляется за счет устройства бесперебойного питания. | 1. сохранить данные, завершить работу с ИРБИС 64/128, выключить рабочую станцию;
2. в случае утери данных после включения питания обратиться в службу поддержки пользователей.
 |
| **Нарушение информационной безопасности** |
| Утечка информации | Обнаружение фактов утечки информации, использование рабочей станции другим пользователем. | Обратиться к руководителю подразделения, уведомить администратора информационной безопасности своего подразделения и администратора информационной безопасности ИРБИС 64/128. |
| Попытка несанкционированного доступа | Обнаружение фактов доступа к рабочей станции (например, удалены данные с рабочей станции, изменены пользовательские настройки, нарушена целостность знаков защиты и т.д.). | Обратиться к администратору информационной безопасности своего подразделения и администратору информационной безопасности ИРБИС 64/128. |

 Таблица В.2

| **Аварийная ситуация** | **Рекомендуемое время первой реакции, не более** | **Рекомендуемое максимальное время устранения аварийной ситуации** |
| --- | --- | --- |
| **Ошибки при работе прикладного программного обеспечения** |
| Невозможность запуска ИРБИС 64/128 | 1 час | 12 часов |
| Отказ доступа к ИРБИС 64/128 | 1 час | 12 часов |
| Отказ доступа к объектам ИРБИС 64/128 | 1 час | 12 часов |
| Зависание или ошибка в работе ИРБИС 64/128 при выполнении операций | 24 часа | 48 часов |
| Устаревшая версия ИРБИС 64/128 | 24 часа | 48 часов |
| Ошибка при обновлении ИРБИС 64/128 | 24 часа | 48 часов |
| Отсутствие данных в ИРБИС 64/128 | 1 час | 24 часа |
| Наличие некорректных данных в базе данных ИРБИС 64/128 | 1 час | 24 часа |
| Ошибки в результате неверных настроек ИРБИС 64/128 | 1 час | 24 часа |
| Нарушение целостности ИРБИС 64/128 | 1 час | 12 часов |
| Невозможность ручной или автоматической загрузки данных в ИРБИС 64/128 | 1 час | 24 часа |
| **Ошибки при работе системного и стороннего ПО** |
| Обнаружение вируса | Рекомендуемое время реакции |
| Некорректные действия пользователей: ошибки при вводе и сохранении данных, удаление программных или системных файлов | 24 часа | 48 часов |
| Ошибки при создании резервной копии ИРБИС 64/128 и восстановлении системы | 30 мин | 6 часов |
| **Сбои по техническим причинам** |
| Сбой технического оборудования | 24 часа | 48 часов |
| Сбои сетевого оборудования | 30 мин | 6 часов |
| Сбои серверного оборудования | 30 мин | 6 часов |
| Физическое повреждение ЛВС или ПЭВМ. | 24 часа | 48 часов |
| **Нарушение информационной безопасности** |
| Утечка информации | 30 мин | 6 часов |
| Попытка несанкционированного доступа | 30 мин | 6 часов |