

DEVELOP

Dynamic balance

www.develop.de

Руководство пользователя -
Безопасность

ineo⁺ 6501

Содержание

1 Введение

- 1.1 Руководство пользователя – Безопасность 1-3
- 1.2 Устройство руководства пользователя 1-4

2 Функции безопасности

3 Режим повышенной безопасности

- 3.1 Описание режима повышенной безопасности 3-3
- 3.2 Защита данных в режиме повышенной безопасности 3-4

4 Функции безопасности администратора аппарата

- 4.1 Включение/выключение режима повышенной безопасности 4-4
- 4.2 Пароль блокировки НЖМД..... 4-7
- 4.3 Распечатка контрольного журнала 4-10
- 4.4 Анализ контрольного журнала 4-12
- 4.5 Таблица событий, сохраненных в контрольном журнале 4-13

5 Алфавитный указатель





Введение

1 Введение

1.1 Руководство пользователя – Безопасность

В комплект поставки входит программное обеспечение для системы управления следующей версии

Версия программы управления изображением (Image Control I1):
A03U0Y0-00I1-G00-40

О функции отображения версии встроенного ПО:

Указанная выше версия программного обеспечения для системы управления ineo+ (программа управления изображением) может быть подтверждена с помощью функции отображения версии ПЗУ в режиме "Service representative (SE)" (представитель сервисной службы).

При отображении версии встроенного ПО версия программы управления изображением обозначается следующим образом.

Версия программы управления изображением (Image Control I1):
G00 + 2 цифры после дефиса (пример: G00-**))

Имейте это в виду при проверке версии программного обеспечения.

Copyright © 2008 Develop GmbH.

ЗАЯВЛЕНИЕ ОБ ОГРАНИЧЕНИИ ОТВЕТСТВЕННОСТИ:

- Никакая часть данной инструкции оператора не может быть использована или скопирована без разрешения.
- Ни компания-изготовитель, ни компания-продавец не несут никакой ответственности за последствия, вызванные использованием системы печати или данного руководства пользователя.
- Информация, представленная в данном руководстве пользователя, может быть изменена без предварительного уведомления.

1.2 Устройство руководства пользователя

Данное устройство комплектуется также следующими руководствами пользователя в печатном виде.

Руководство пользователя ineo+ 6501 – Копир

В этом руководстве приведено описание аппарата и операций копирования.

Обращайтесь к этому руководству за информацией по технике безопасности, включению/выключению питания аппарата, подаче бумаги, устранению неисправностей, например, при застревании бумаги и доступным операциям копирования.

Руководство пользователя ineo+ 6501 – Ссылки администратора порта получателя (POD)

В этом руководстве приведена подробная информация об управлении устройством и его настройке под Ваши конкретные потребности.

Обращайтесь к этому руководству при настройке устройства и управлении им, включая регистрацию бумаги для копирования и настройку лотка.

Руководство пользователя ineo+ 6501 – Безопасность (данное руководство)

Это руководство описывает функции безопасности.

Обращайтесь к этому руководству за информацией по использованию режима повышенной безопасности и за подробными указаниями по использованию аппарата в этом режиме.

Для обеспечения безопасной эксплуатации устройства изучите "главу 1 Информация по технике безопасности" в "Руководстве пользователя ineo+ 6501 – Копир" перед началом работы.



Функции безопасности

2 Функции безопасности

У устройства iNeo+ 6501 имеется два режима безопасности.

Нормальный режим

Данный режим рекомендуется использовать в случаях, когда пользователем аппарата является один человек, и вероятность несанкционированного доступа и использования аппарата достаточно мала. Этот режим устанавливается по умолчанию при поставке аппарата.

Об эксплуатации в нормальном режиме см. руководство пользователя, входящее в комплект поставки каждого аппарата.


Режим повышенной безопасности

Данный режим рекомендуется использовать в случаях, когда аппарат подключен к локальной вычислительной сети либо к внешним сетям при помощи телефонной линии или иным способом. Управление аппаратом осуществляется администратором в соответствии с данным руководством пользователя, так чтобы пользователи могли работать в безопасной рабочей среде. При этом администратор аппарата является единственным лицом, которое имеет право включать и выключать режим повышенной безопасности, а также вносить другие изменения в режим работы. Администратор аппарата назначается представителем сервисной службы.

Для того чтобы можно было включить режим повышенной безопасности, представитель сервисной службы должен установить на аппарате пароль идентификации CE и пароль администратора аппарата.

При необходимости использования режима повышенной безопасности обращайтесь к представителю сервисной службы.

Режим повышенной безопасности используется в случаях, когда необходимо защитить данные от несанкционированного доступа или повреждения.

При включении режима повышенной безопасности на сенсорной панели  **Безопасн.** отображается значок "Безопасность".

Рабочая среда, в которой рекомендуется использовать режим повышенной безопасности

- Управление аппаратом осуществляется по телефонной линии или по сети.

Создание безопасной рабочей среды

В целях обеспечения безопасности рекомендуется, чтобы супервизоры и администраторы аппаратов использовали режим повышенной безопасности и настроили рабочую среду следующим образом.

- **Квалификационные требования к администратору аппарата**
Администратор аппарата назначается супервизором. Администратор аппарата должен обладать достаточными техническими знаниями, умением и опытом работы в качестве администратора аппарата.
- **Гарантии представителя сервисной службы (CE)**
Супервизор или администратор аппарата могут использовать режим повышенной безопасности только после подписания договора на сервисное обслуживание с представителем сервисной службой (CE). В договоре в явном виде указывается, что представитель сервисной службы не будет вовлечен в какие-либо действия, имеющие обманный или мошеннический характер.
- **Безопасная локальная сеть**
При подключении аппарата к локальной сети убедитесь, что она защищена брандмауэром, предотвращающим доступ из внешней сети.



**Режим повышенной
безопасности**

3 Режим повышенной безопасности

3.1 Описание режима повышенной безопасности

Следующие меры способствуют повышению уровня безопасности рабочей среды.

- **Настройка сетевой карты аппарата**
При включенном режиме повышенной безопасности доступные функции ограничиваются программой "CS Remote Care".
- **Запрещение внешнего доступа**
Доступ к информации по телефонной линии закрыт за исключением программы CS Remote Care.
- **Создание, хранение и анализ контрольного журнала**
История выполнения операций по обеспечению безопасности фиксируется и сохраняется в отдельном журнале. В журнале сохраняются: дата и время, информация, идентифицирующая человека, выполнившего ту или иную операцию, и результат выполнения операции – все это позволяет отслеживать попытки несанкционированного доступа к защищенным данным. При заполнении выделенного для контрольного журнала пространства на диске данные перезаписываются.
- **Идентификация администратора аппарата**
Представитель сервисной службы вводит в аппарат идентификационные данные администратора аппарата.
Для получения доступа к настройкам аппарата администратор аппарата должен ввести соответствующий пароль. На каждом аппарате допускается регистрация только одной идентификационной строки.
- **Режим Настройки администратора аппарата**
При успешной идентификации администратора аппарата активизируется режим настроек администратора, в котором осуществляется изменение параметров различных функций аппарата.
По окончании внесения изменений не забудьте выйти из режима настроек администратора.

3.2 **Защита данных в режиме повышенной безопасности**

Данные, защищенные в режиме повышенной безопасности, сохраняются в аппарате в виде отдельного документа.

Включение/выключение режима повышенной безопасности

Включение/выключение режима повышенной безопасности осуществляется администратором аппарата.

Если режим повышенной безопасности отключен, то существует потенциальная опасность несанкционированного доступа к данным, поэтому будьте осторожны.

4

Функции безопасности администратора аппарата

4 Функции безопасности администратора аппарата

Администратор аппарата осуществляет включение и выключение режима повышенной безопасности.

Для этого в аппарате должен быть установлен 8-значный идентификационный пароль SE и пароль администратора аппарата. Для установки пароля администратора аппарата обращайтесь к представителю сервисной службы. Чтобы изменить пароль, администратор аппарата должен выполнить действия, описанные в Руководстве пользователя Ссылки администратора порта получателя (POD).

Для защиты данных от несанкционированного доступа и повреждения рекомендуется назначить администратора аппарата и использовать режим повышенной безопасности.



Внимание

В качестве пароля не следует использовать имена, дни рождения, табельные номера и т. п., то есть информацию, которую легко можно вычислить.

Также не следует сообщать пароль другим лицам.

4.1 Включение/выключение режима повышенной безопасности

Ниже приводится описание действий при включении и выключении режима повышенной безопасности.



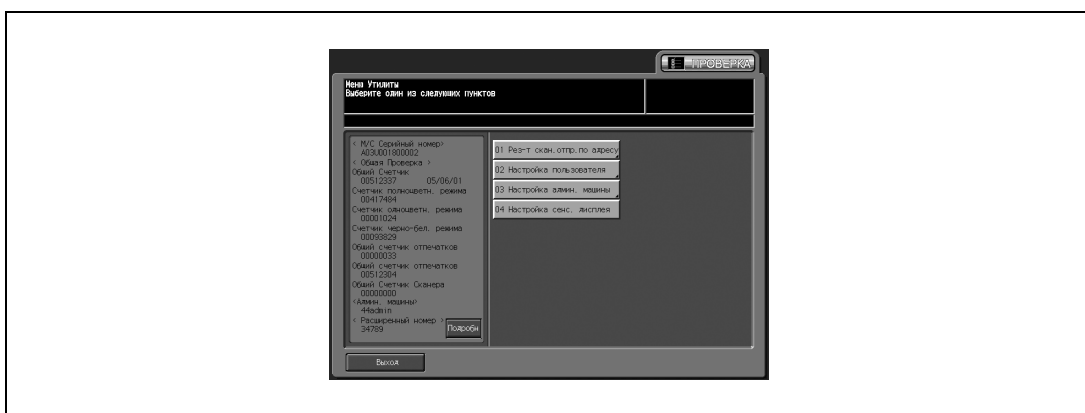
Примечание

Пароль чувствителен к регистру.

Если ввести неверный пароль или пароль, содержащий менее 8 буквенно-цифровых символов, и затем нажать [OK], появляется предупреждение "Неверный пароль", и все кнопки блокируются на пять секунд. По истечении пяти секунд введите правильный пароль.

Если идентификация пользователя не будет выполнена, этот факт будет зафиксирован в контрольном журнале.

- 1 Нажмите [Утилиты/Счетчик] на панели управления для вывода окна ПРОВЕРКА.
- 2 Нажмите [03 Настройка админ. аппарата].



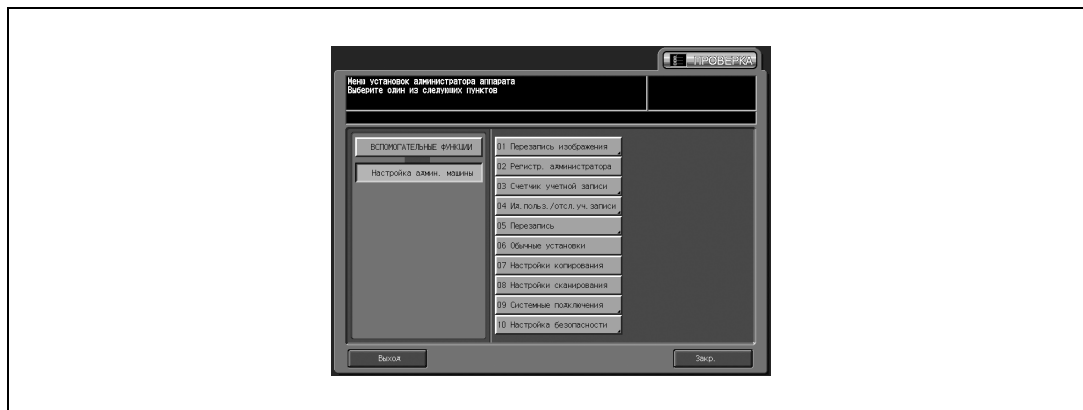
Появляется окно ввода пароля.

- 3 Введите пароль.
Введите 8-значный пароль администратора аппарата с сенсорной панели и нажмите [OK].

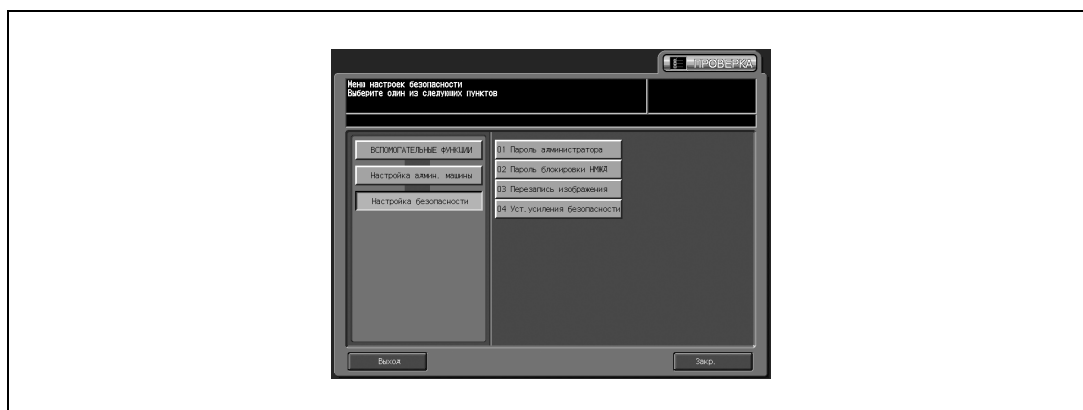


Появляется окно "Настройки администратора аппарата".

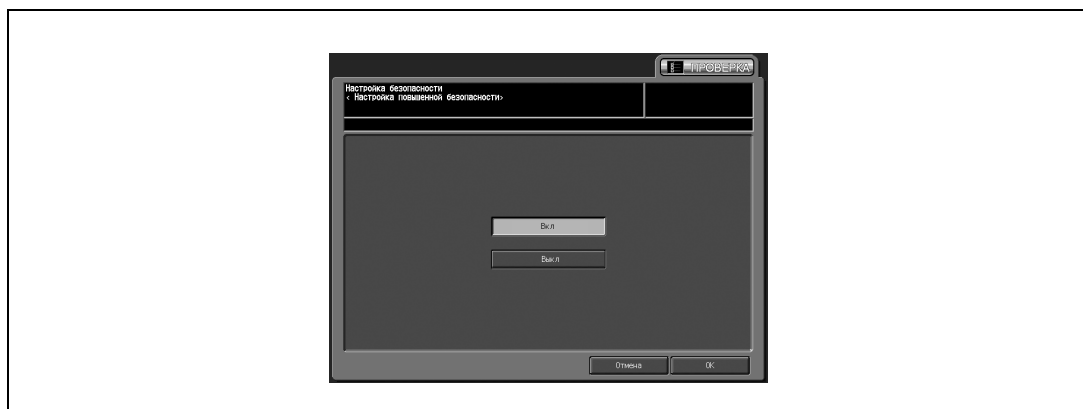
4 Нажмите [10 Настройка безопасности].



5 Нажмите [04 Уст.усиления безопасности].



6 Включите или выключите режим повышенной безопасности.
 Чтобы включить режим повышенной безопасности, нажмите [Вкл] для активизации опции.
 Чтобы выключить режим повышенной безопасности, нажмите [Выкл].



7 Нажмите [ОК].



Появляется всплывающее окно подтверждения перезагрузки.

8 Нажмите [Да].

Происходит перезагрузка аппарата, после чего будут активизированы новые параметры.

4.2 Пароль блокировки НЖМД

Если режим повышенной безопасности включен, то может быть установлен блокирующий пароль (от 8 до 32 алфавитно-цифровых символов, чувствительный к регистру) на жесткий диск, защищающий хранящиеся на нем данные.

Если имеется возможность внешнего доступа к жесткому диску, то считывание данных возможно только при вводе соответствующего блокирующего пароля.



Внимание

В качестве пароля не следует использовать имена, дни рождения, табельные номера и т. п., то есть информацию, которую легко можно вычислить.

Также не следует сообщать пароль другим лицам.



Примечание

Функция ввода блокирующего пароля возможна только при включенном режиме повышенной безопасности. Если режим повышенной безопасности выключен, на дисплее появляется сообщение "Включите режим повышенной безопасности".



Примечание

Пароль чувствителен к регистру.

Если ввести неверный пароль или пароль, содержащий менее 8 буквенно-цифровых символов, и затем нажать [OK], появляется предупреждение "Неверный пароль", и все кнопки блокируются на пять секунд. По истечении пяти секунд введите правильный пароль.

Если идентификация пользователя не будет выполнена, этот факт будет зафиксирован в контрольном журнале.



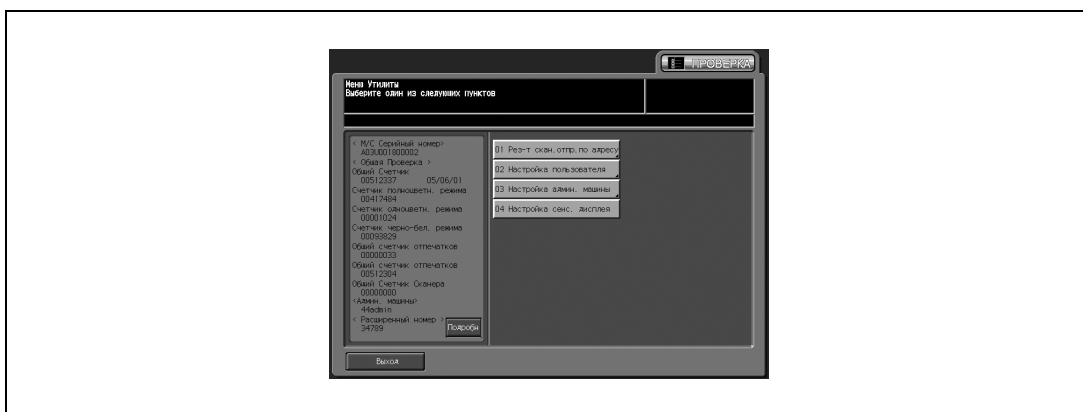
Подробнее

Серийный номер основного блока будет напечатан в правом верхнем углу контрольного журнала. Подробнее см. "Распечатка контрольного журнала" на странице 4-10 и образец контрольного журнала "Анализ контрольного журнала" на странице 4-12.

Если идентификация пользователя не будет выполнена, этот факт будет зафиксирован в контрольном журнале.

Текущий пароль не может быть использован в качестве нового пароля.

- 1 Нажмите [Утилиты/Счетчик] на панели управления для вывода окна "ЛПРОВЕРКА".
- 2 Нажмите [03 Настройка админ. машины].



Появляется окно ввода пароля.

- 3 Введите пароль.
Введите 8-значный пароль администратора аппарата с сенсорной панели и нажмите [OK].

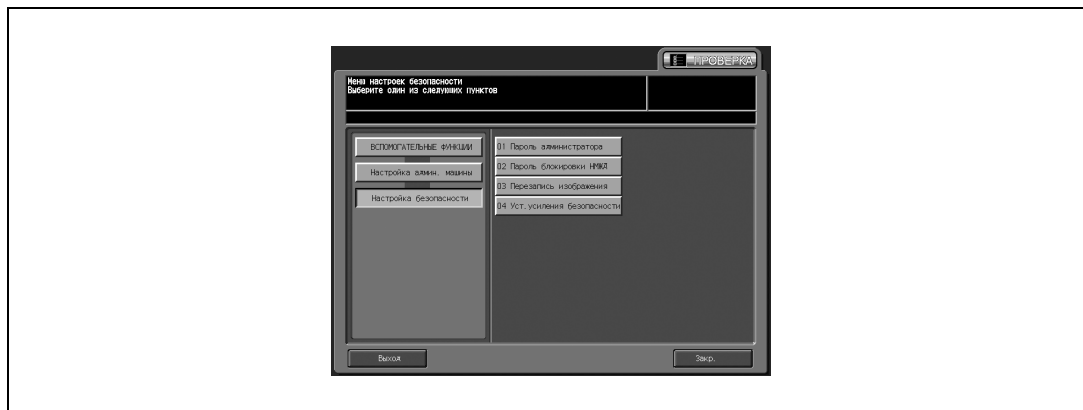


Появляется окно Меню установок администратора аппарата.

- 4 Нажмите [10 Настройка безопасности].



- 5 Нажмите [02 Пароль блокировки НЖМД].



Появляется окно Меню Пароль блокировки жесткого диска.

- 6 Нажмите [Текущий пароль] для ввода текущего пароля, а затем нажмите [OK].
Первый пароль: 13-значный буквенно-цифровой серийный номер основного блока



- 7 После успешного завершения идентификации нажмите [Новый пароль] для ввода нового пароля.
Эта кнопка не активизируется до тех пор, пока идентификация не будет успешно завершена.
- Нажмите [OK] для возвращения в предыдущее окно.
- 8 Нажмите [Пров. ввода] для повторного ввода нового пароля.
- Нажмите [OK] для возвращения в предыдущее окно.
- 9 Нажмите [OK].

4.3 Распечатка контрольного журнала

Контрольный журнал создается автоматически при получении доступа к данным, хранящимся в аппарате.

Все данные из контрольного журнала можно вывести на печать следующим образом.



Примечание

Пароль чувствителен к регистру.

Если ввести неверный пароль или пароль, содержащий менее 8 буквенно-цифровых символов, и затем нажать [OK], появляется предупреждение "Неверный пароль", и все кнопки блокируются на пять секунд. По истечении пяти секунд введите правильный пароль.

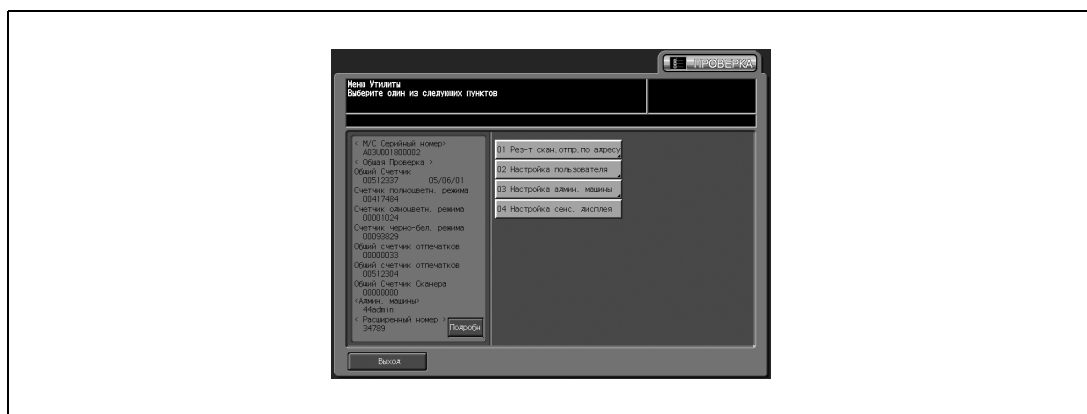
Если идентификация пользователя не будет выполнена, этот факт будет зафиксирован в контрольном журнале.



Примечание

Чтобы остановить печать, нажмите кнопку [Стоп] на панели управления, а затем нажмите [Отмена] во всплывающем окне подтверждения.

- 1 Нажмите [Утилиты/Счетчик] на панели управления для вывода окна ПРОВЕРКА.
- 2 Нажмите [03 Настройка админ.аппарата].



Появляется окно ввода пароля.

- 3 Введите [пароль].
Введите 8-значный пароль администратора аппарата с сенсорной панели и нажмите [OK].

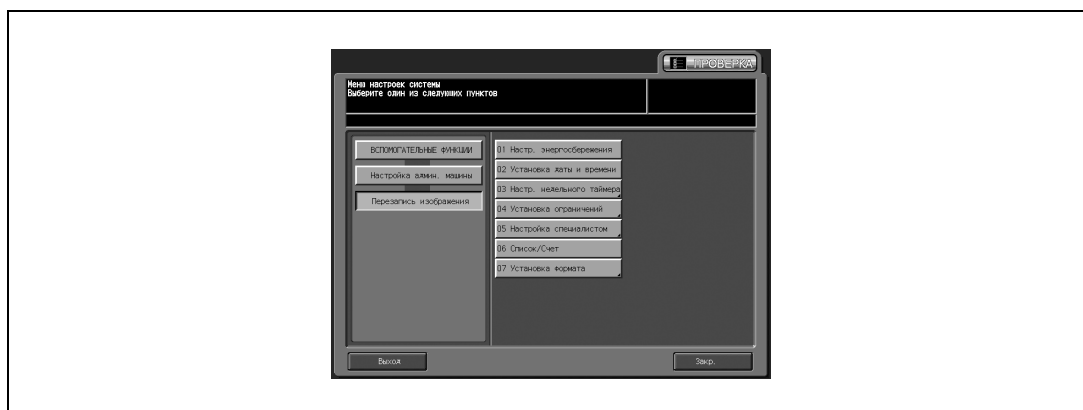


Появляется окно Меню установок администратора аппарата.

4 Нажмите [01 Установка системы].



5 Нажмите [06 Список/Счет].



Появляется окно Печать списка настроек управления.

6 Нажмите [Отчет аудита], а затем [КОПИЯ].



7 Нажмите [Старт] на панели управления.

4.4 Анализ контрольного журнала

Администратор аппарата должен регулярно проводить анализ записей контрольного журнала (один раз в месяц) или в случае уведомления о несанкционированном доступе или повреждении данных, хранящихся в аппарате, отправленного в режиме повышенной безопасности.

Данный аппарат рассчитан на сохранение до 750 записей в месяц.

Если предполагается, что в течение месяца в контрольном журнале будет более 750 записей, то анализ записей следует проводить чаще, не дожидаясь, пока количество записей достигнет указанного значения.

Audit log report									
					P.1 29/06/2006 16:33 A03U001900004 TC:49279				
No	date/time	id	action	result	No	date/time	id	action	result
0001	26/06/2006 10:32	-2	03	OK	0002	26/06/2006 10:32	-2	03	OK
0003	26/06/2006 10:32	-2	02	OK	0004	26/06/2006 10:31	-2	03	OK
0005	23/06/2006 14:10	-2	05	OK	0006	23/06/2006 14:10	-2	02	OK
0007	23/06/2006 14:10	-2	02	OK	0008	23/06/2006 14:08	-2	03	OK
0009	23/06/2006 14:03	-2	03	OK	0010	23/06/2006 14:03	-2	02	OK
0011	23/06/2006 14:02	-2	03	OK	0012	23/06/2006 13:59	-2	03	OK
0013	23/06/2006 13:59	-2	02	OK	0014	23/06/2006 13:57	-2	03	OK
0015	23/06/2006 11:21	-2	03	OK	0016	23/06/2006 11:21	-2	02	OK
0017	23/06/2006 11:20	-2	03	OK	0018	23/06/2006 11:19	-2	03	OK
0019	23/06/2006 11:19	-2	02	OK	0020	23/06/2006 11:17	-2	03	OK
0021	30/05/2006 21:26	-2	03	OK	0022	30/05/2006 21:26	-2	02	OK
0023	30/05/2006 21:25	-1	01	OK	0024	30/05/2006 21:25	-2	02	OK
0025	30/05/2006 21:24	-2	03	OK	0026	30/05/2006 20:24	-2	03	OK
0027	30/05/2006 20:24	-2	02	OK	0028	30/05/2006 20:23	-1	01	OK
0029	30/05/2006 20:22	-2	04	OK	0030	30/05/2006 20:21	-2	02	OK
0031	30/05/2006 20:21	-2	02	NG	0032	30/05/2006 20:21	-1	01	NG
0033	30/05/2006 20:20	-2	03	OK	0034	30/05/2006 20:10	-2	03	OK
0035	30/05/2006 20:09	-2	04	OK	0036	30/05/2006 20:07	-2	04	OK
0037	30/05/2006 20:07	-1	06	OK	0038	30/05/2006 20:06	-1	05	OK
0039	30/05/2006 20:06	-1	05	OK	0040	30/05/2006 20:05	-2	06	OK
0041	30/05/2006 20:04	-2	03	OK	0042	30/05/2006 19:42	-2	04	OK
0043	30/05/2006 19:38	-2	04	OK	0044	25/05/2006 17:00	-2	03	OK
0045	25/05/2006 17:00	-2	02	OK	0046	25/05/2006 17:00	-2	02	NG
0047	25/05/2006 17:00	-1	05	OK	0048	25/05/2006 17:00	-1	05	OK
0049	25/05/2006 16:59	-1	01	OK	0050	25/05/2006 16:59	-1	01	NG
0051	25/05/2006 16:58	-2	19	OK	0052	25/05/2006 16:57	-2	19	OK
0053	25/05/2006 16:57	-2	06	OK	0054	25/05/2006 16:56	-2	02	OK
0055	25/05/2006 16:55	-2	02	NG	0056	25/05/2006 14:55	-2	03	OK
0057	25/05/2006 14:55	-2	02	OK	0058	25/05/2006 14:54	-1	01	OK
0059	25/05/2006 14:54	-1	01	NG	0060	25/05/2006 14:54	-1	01	NG
0061	26/04/2006 14:37	-2	03	OK	0062	26/04/2006 14:37	-2	02	OK
0063	26/04/2006 14:32	-2	03	OK	0064	26/04/2006 14:32	-2	02	OK
0065	26/04/2006 14:28	-2	02	OK	0066	26/04/2006 14:28	-2	02	NG
0067	26/04/2006 14:27	-2	02	OK	0068	26/04/2006 11:18	-2	03	OK

Информация в контрольном журнале

Контрольный журнал содержит следующую информацию.

1. date/time: дата и время выполнения операции, которая стала причиной появления записи в контрольном журнале.
2. id: лицо, выполнившее операцию, либо лицо, ставшее причиной активизации функции обеспечения безопасности.
"-1": операция, выполненная СЕ (представитель сервисной службы).
"-2": операция, выполненная администратором аппарата.
Другое целое число: показывает, кто стал причиной активизации функции обеспечения безопасности.
3. action: характер операции.
Детальная проверка операции, на которую указывает действие в следующей таблице.
4. result: результат операции.
Для операций с идентификацией пароля: успешная или неуспешная идентификация обозначается как ОК или NG.
Для операций без идентификации пароля: все записи в контрольном журнале обозначаются как ОК.

4.5 Таблица событий, сохраненных в контрольном журнале

№	Операция	ID	Сохраненное действие	Результат
1	Идентификация CE	ID CE	01	OK/NG
2	Идентификация администратора	ID администратора аппарата	02	OK/NG
3	Установка/изменение параметров режима повышенной безопасности	ID администратора аппарата	03	OK
4	Распечатка контрольного журнала	ID администратора аппарата	04	OK
5	Изменение/регистрация пароля CE	ID CE	05	OK
6	Изменение/регистрация пароля администратора аппарата	ID CE/ID администратора аппарата	06	OK
13	Изменение пароля блокировки НЖМД	ID администратора аппарата	19	OK

Целью анализа контрольного журнала является понимание описанных ниже обстоятельств и принятие мер противодействия:

Была ли попытка несанкционированного доступа или повреждения данных

Объект атаки

Детали атаки

Результат атаки

Конкретные методы анализа см. на следующей странице.

Определение несанкционированных действий: идентификация пароля

Если в записях журнала идентификация пароля обозначена как NG (action: 01, 02), это означает, что пункты, защищенные паролем, могли оказаться объектами атаки.

- Записи в журнале, указывающие на безуспешные попытки идентификации пароля (NG), показывают, кто выполнял эту операцию, а также совершались ли несанкционированные действия при безуспешной идентификации пароля.
- Даже если идентификация пароля прошла успешно (OK), запись в журнале показывает, была ли данная операция выполнена легитимным пользователем. Если идентификация прошла успешно после серии безуспешных попыток, особенно в часы, которые не относятся к рабочему времени, необходимо внимательно проверить записи в контрольном журнале.

Определение несанкционированных действий: действия, отличные от идентификации пароля, выполняемые в рамках обеспечения безопасности

Все операции, отличные от идентификации пароля, обозначаются как (OK), поэтому нужно самостоятельно определять, являлось то или иное действие, выполненное под тем или иным идентификационным номером, санкционированным, или нет.

- Проверьте время действия и определите, было ли действие, выполненное пользователем, санкционированным, или нет.

Действия, предпринимаемые при обнаружении несанкционированных операций

Если в результате анализа записей журнала установлено, что причиной несанкционированного действия стала утечка пароля, пароль необходимо немедленно сменить.



Алфавитный указатель

5 Алфавитный указатель

С

CS remote care 3-3

А

Администратор аппарата 2-3

Анализ контрольного журнала 4-12

Б

Брандмауэр 2-3

В

Включение/выключение режима повышенной безопасности 4-4

З

Значок Безопасность 2-3

И

Идентификация администратора аппарата 3-3

К

Контрольный журнал 3-3, 4-10, 4-12

Н

Настройки сетевой карты аппарата 3-3

Несанкционированные действия 4-13

Нормальный режим 2-3

О

Окно Утилиты 4-4, 4-8, 4-10

П

Пароль администратора аппарата 4-3

Пароль блокировки НЖМД 4-7

Пароль идентификации CE 4-3

Представитель сервисной службы (CE) 2-3

Р

Распечатка контрольного журнала 4-10

Режим Настройки администратора аппарата 3-3

Режим повышенной безопасности 2-3, 3-3

Ф

Функции безопасности администратора аппарата 4-3

