СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «ТОБОЛ-ИПК»

Формуляр

Листов 47

2021

СОДЕРЖАНИЕ

1. ОБЩИЕ УКАЗАНИЯ

1.1. Перед эксплуатацией изделия «Специальное программное обеспечение «Тобол-ИПК» ЦКДИ.00621-01 (далее по тексту – СПО «Тобол-ИПК») необходимо ознакомиться с соответствующими эксплуатационными документами в составе:

– Администратор безопасности. Руководство системного программиста ЦКДИ.00621-01 32 01;

– Руководство оператора ЦКДИ.00621-01 34 01.

1.2. Формуляр должен находиться в подразделении, ответственном за эксплуатацию СПО «Тобол-ИПК» и вестись в течение всего срока эксплуатации и хранения изделия.

1.3. В формуляр в обязательном порядке вносят сведения, касающиеся комплектности, технического состояния, хранения и эксплуатации данного изделия.

1.4. Все сведения вносят и удостоверяют их своей подписью лица, ответственные за изготовление, приемку и упаковывание изделия, а также ответственные за его хранение, транспортирование, выполнение работ и эксплуатацию.

1.5. Все записи в формуляре производят только чернилами, отчетливо и аккуратно. Допускается использовать при записях шариковые ручки с черной или фиолетовой (синей) пастой. Подчистки, помарки и незаверенные исправления не допускаются. Правильность и своевременность заполнения формуляра контролируют должностные лица.

1.6. Неправильная запись должна быть аккуратно зачеркнута и рядом записана новая, которую заверяет ответственное лицо.

1.7. После подписи проставляют фамилию и инициалы ответственного лица (вместо подписи допускается проставлять личный штамп исполнителя).

1.8. В раздел «Особые отметки» вносят данные, не предусмотренные другими разделами формуляра, необходимость в которых возникает в эксплуатации изделия, также данные о вводе изделия в эксплуатацию.

1.9. Незаполнение разделов и таблиц формуляра во время эксплуатации изделия является нарушением условий его эксплуатации.

1.10. При передаче изделия на другое предприятие итоговые суммирующие записи по наработке заверяют печатью предприятия, передающего изделие.

1.11. Правильность и своевременность заполнения формуляра контролируют соответствующие должностные лица.

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Наименование изделия – специальное программное обеспечение «Тобол-ИПК»

Обозначение изделия – ЦКДИ.00621-01

Заводской номер № _____

Дата ввода в эксплуатацию изделия _____

Тип носителя: компакт-диск.

Адрес предприятия-изготовителя: Российская Федерация, АО «ФЦНИВТ «СНПО «Элерон», 115563, Москва, ул. Генерала Белова, 14,

ФАКС: 8 (495) 393-91-63.

Сайт: www.eleron.ru

2.2. Специальное программное обеспечение «Тобол-ИПК» (далее по тексту – СПО «Тобол-ИПК») является специальным программным средством со встроенными средствами защиты от несанкционированного доступа к информации, применяемом в автоматизированных системах физической защиты (далее по тексту – АСФЗ).

2.3. СПО «Тобол-ИПК» предназначено для сбора, обработки, хранения информации от технических средств физической защиты (далее по тексту – ТСФЗ) и реализации функций системы оптико-электронного наблюдения (далее по тексту – СОЭН), обеспечивающей дистанционный видеоконтроль территории охраняемого объекта.

2.4. Дистрибутив СПО «Тобол-ИПК» поставляется на установочном компакт-диске №1 с маркировкой:
Специальное программное обеспечение «Тобол-ИПК» ЦКДИ.00621-01.

2.5. СПО «Тобол-ИПК» устанавливается на автоматизированные рабочие места (далее по тексту – АРМ) и серверы в соответствии с лицензией.

2.6. СПО «Тобол-ИПК» сертифицировано на соответствие требованиям:

– руководящего документа «Системы физической защиты ядерных объектов. Автоматизированные системы физической защиты. Защита

информации от несанкционированного доступа. Требования безопасности информации» (приложение 3 к приказу Госкорпорации «Росатом» от 08.08.2011 № 1/669-П) – по первому (1) классу защищенности АСФЗ;

– документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76) – по второму (2) уровню доверия;

– технических условий ЦКДИ.00621-01 98 01.

2.7. СПО «Тобол-ИПК» сертифицировано в Системе сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00) и имеет сертификат соответствия № _____ (выдан ФСТЭК России «____» _____ 20__ г., действителен до «____» _____ 20__ г.).

3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1. СПО «Тобол-ИПК» обеспечивает соответствие 2-му уровню доверия в соответствии с руководящим документом «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76) и может быть использовано в АСФЗ до 1 класса защищенности включительно, действие которых распространяется на защищенную зону и/или внутреннюю зону и особо важную зону, или особо важную зону в отдельности, в которых обрабатывается информация, составляющая служебную тайну, и иная информация с ограниченным доступом и/или составляющая государственную тайну со степенью секретности не выше «совершенно секретно» в соответствии с руководящим документом «Системы физической защиты ядерных объектов. Автоматизированные системы физической защиты. Защита информации от несанкционированного доступа. Требования безопасности информации», согласованным ФСТЭК России от 30.05.2011 №240/2/2185 для реализации следующих функций защиты информации:

- идентификация и аутентификация пользователей при осуществлении доступа к СПО «Тобол-ИПК»;
- идентификация компьютеров АСФЗ;
- идентификация периферийных устройств;
- управление доступом пользователей к программам, опциям меню, командам, периферийным устройствам, операциям с данными АСФЗ;
- регистрация попыток доступа к СПО «Тобол-ИПК» (прием/сдача смены);
- регистрация неуспешной идентификации компьютеров и периферийных устройств;
- регистрация попыток доступа персонала к программам, командам, периферийным устройствам, операциям с данными АСФЗ;
- регистрация попыток изменения полномочий пользователей;
- регистрация несанкционированного физического доступа к оборудованию АСФЗ;

– сигнализация попыток нарушения безопасности информации;

– регистрация и учет выходных печатных документов;

– контроль целостности средств защиты информации от несанкционированного доступа (далее по тексту – СЗИ НСД);

– контроль целостности программ и чувствительных данных АСФЗ;

– архивирование, восстановление и дублирование чувствительных данных АСФЗ;

– тестирование СЗИ НСД;

– управление резервированием (дублирование) критичного оборудования и чувствительных данных.

3.2. Среда функционирования СПО «Тобол-ИПК»: операционная система ОС «Astra Linux Special Edition» РУСБ.10015–01 (далее по тексту – ОС Astra Linux), сертифицированная ФСТЭК России на соответствие требованиям по безопасности информации (сертификат ФСТЭК России № 2557, от 27 января 2012 года, техническая поддержка до 31 декабря 2028 года). Для функционирования серверных приложений СПО «Тобол-ИПК» использует СУБД PostgreSQL из состава сертифицированной версии ОС Astra Linux. Взаимодействие с базами данных осуществляется с применением архитектуры «клиент-сервер».

3.2.1. Требования к аппаратной платформе

Требования к аппаратной платформе приведены в таблицах 1-4.

Таблица 1 – Сервер обработки данных

Наименование	Характеристика
Оперативная память	16 ГБ
Процессор	Intel Core i5
SSD или HDD под систему	250 ГБ SSDx2 или 2 ТБ HDDx2
Оптический дисковод	DVD-RW
Сетевой адаптер	2xEthernet 1000
Видеоадаптер(ы)	SXGA, выход VGA
Последовательные порты RS-232/485	Не менее 2

Таблица 2 – Сервер хранения видеоархива

Наименование	Характеристика
Оперативная память	16 ГБ
Процессор	Intel Xeon E3 V6, 3.5 ГГц или выше
SSD или HDD под систему	250 ГБ SSDx2 или 2 ТБ HDDx2
HDD, в mobile rack под видеоархив	Требования к оперативному или долговременному видеоархиву определяются количеством каналов в проектной документации, сроком хранения данных согласно действующему регламенту, принятому на объекте. При количестве HDD от 6 до 10 использовать конфигурацию RAID5 + Hotspare (2 HDD), при количестве 10-24 – RAID6 или 60 + Hotspare (HDD)
Оптический дисковод	DVD-RW
Сетевой адаптер	2xEthernet 1000
Видеоадаптер(ы)	SXGA, выход VGA

Таблица 3 – Сервер видеоаналитики

Наименование	Характеристика
Оперативная память	32 ГБ
Процессор	Intel Xeon Silver 4210R, 2.4-3.2 ГГц
SSD или HDD	500 ГБ SSDx2 или 2 ТБ HDDx2
Оптический дисковод	DVD-RW
Сетевой адаптер	2xEthernet 1000
Видеоадаптер(ы)	Не ниже nVidia Quadro P4000. Количество определяется количеством каналов видеоаналитики заданной в проектной документации

Таблица 4 – АРМ

Наименование	Характеристика
Оперативная память	8 ГБ. 16 ГБ для АРМ с отображением видеоизображений с камер
Процессор	Intel Core i5
SSD или HDD	250 ГБ SSDx2 или 2 ТБ HDDx2. Mobile rack для АРМ Администратора
Оптический дисковод	DVD. DVD-RW для АРМ Администратора
Сетевой адаптер	Ethernet 1000
Видеоадаптер(ы)	Full HD, HDMI от 1 до 4. Количество определяется проектной документацией
Звуковая карта и колонки звуковые	

Последовательные порты RS-232/485	Не менее 2, для рабочего места бюро пропусков

3.3. В состав дистрибутива СПО «Тобол-ИПК» входят следующие программы, реализующие требования по назначению:

1) программа «Оператор»;
2) программа «Администратор»;
3) программный сервер «Сервер управления и мониторинга (СУМ)»;
4) программный сервер «Сервер управления режимом (СУР)»;
5) система комплексного мониторинга надежности (СКМН), включающая в себя программы «Сервер СКМН» и «Клиент СКМН»;
6) программа «Аппаратно-программный интерфейс (АПИ) оборудования полевой сети (ОПС)»;
7) программа «АПИ Камер»;
8) программа «АПИ Архива»;
9) программа «АПИ Менеджера архивов»;
10) программа «АПИ Аналитики»;
11) программа «Сервер обслуживания»;
12) программа «Клиент сервиса обслуживания»;
13) программа «Редактор отчетных форм»;
14) программа «Адаптер интеграции»;
15) программа «Утилита печати пропусков»;
16) программа «Конфигуратор»;
17) программа «Служба очередей»;
18) программа «Служба сообщений для видеосистемы»;
19) программа «Сервис управления»;
20) программа «Контроль целостности».

3.3.1. Программа «Оператор» обеспечивает выполнение следующих функций:

1) автоматический оперативный контроль обстановки на объекте;
2) вывод сообщений о текущих событиях;
3) отображение статуса компонентов АСФЗ на графических планах объекта;

4) сбор, обработку и отображение видеопотока в HD и SD качестве от аналоговых, цифровых или тепловизионных камер (далее по тексту – ТК) СОЭН;

5) автоматическое оповещение оператора о нештатных ситуациях;

6) отображение объектового журнала тревожных событий;

7) отображение состояния технических средств системы контроля и управления доступом (далее по тексту – СКУД), системы охранной сигнализации (далее по тексту – СОС), СОЭН;

8) оперативное управление техническими средствами СКУД, СОС, СОЭН;

9) автоматизированная постановка и снятие с охраны участков блокирования;

10) автоматизированное управление доступом персонала на объект через локальный участок прохода (точку доступа): шлюз, контрольно-пропускной пункт, оснащенный турникетами, металлодетекторами, радиационными порталами;

11) автоматизированную оперативную верификацию персонала, отображение персональных данных, результатов контроля весовых характеристик и служебной информации при проходах в контролируемые зоны;

12) автоматизированный учет пропускного документооборота на объекте;

13) автоматический контроль количества и местонахождения сотрудников на территории объекта;

14) автоматический контроль направлений проходов, весовых и других характеристик;

15) обеспечение проверки корректности ввода данных со стороны пользователя при формировании запросов к серверу;

16) конфигурирование элементов графического отображения устройств и компонентов АСФЗ;

17) гибкую настройку внешнего вида и расположения окон;

18) формирование графических планов объекта;

19) оповещение оператора о нештатных ситуациях на контролируемом участке прохода;

20) отображение объектового журнала событий доступа;

21) создание и редактирование оператором базы данных сотрудников, в том числе ввод анкетных данных, фотоизображений, весовых и других данных, присвоение пропусков;

22) формирование внешнего облика (дизайна) пластиковых карт пропусков;

23) вывод на печать внесенных в базу данных пропусков;

24) определение и корректировку оператором полномочий (прав доступа) и категорий сотрудников;

25) определение оператором временных зон, территориальных зон и правил доступа;

26) просмотр и анализ архива событий;

27) формирование и печать отчетов.

3.3.2. Программа «Администратор» обеспечивает:

1) конфигурирование подключенного оборудования и его диагностику;

2) конфигурирование встроенных средств защиты информации от несанкционированного доступа в части разграничения полномочий пользователей в соответствии с уровнем конфиденциальности АРМ;

3) обработку сообщений, поступающих от технических средств интегрированных систем посредством аппаратно-программного интерфейса (далее- АПИ), формирование команд управления;

4) обработку и передачу команд в технические средства интегрированных систем;

5) формирование событий для отображения в программе «Оператор».

3.3.3. Программа «СУМ» обеспечивает управление доступом, охранной сигнализацией, системой электроосвещения, отвечает за конфигурирование оборудования, осуществляет общую логическую взаимосвязь между отдельными экземплярами программ, входящих в состав СПО «Тобол-ИПК».

3.3.4. Программа «СУР» обеспечивает ввод данных пользователей и персонала объекта, пропускной документооборот, хранение отчетной и ретроспективной информации.

Примечание. Пользователи СПО «Тобол-ИПК» – администраторы, администраторы безопасности, операторы, осуществляющие постоянный

контроль за работой и управление системой с рабочих станций и специализированных пультов, пунктов управления системы физической защиты и с контрольно-пропускных пунктов. Пользователи имеют различные права и привилегии. Персонал АСФЗ (абоненты) - персонал физической защиты, командировочные лица и посетители объекта, осуществляющие проход в (из) охраняемые зоны и зоны ограниченного доступа. Персонал АСФЗ не имеет доступа к СПО «Тобол-ИПК», имеет доступ к ограниченному интерфейсу АСФЗ только посредством устройств ввода идентификационных признаков (далее по тексту – УВИП) (электронный пропуск и другие данные).

3.3.5. Программы «Сервер СКМН» и «Клиент СКМН» осуществляют контроль и мониторинг состояния оборудования с целью обеспечения стабильности параметров и надежности функционирования программных и аппаратных средств.

3.3.6. Программа «АПИ ОПС» обеспечивает взаимодействие сервера СУМ из состава СПО «Тобол-ИПК» с периферийной аппаратурой АСФЗ.

3.3.7. Программа «АПИ Камер» обеспечивает выполнение следующих функций:

1) выполнение захвата и управления видеопотоком;

2) настройки параметров сенсоров видеокамер;

3) управление позиционированием видеооборудования;

4) возможность отключить передачу изображения с камеры в видеопотоке.

3.3.8. Программа «АПИ Архива» обеспечивает запись, хранение, изменение, чтение видеоданных и метаинформации.

3.3.9. Программа «АПИ Менеджера архивов» обеспечивает выполнение следующих функций:

1) синхронизацию оперативного и долговременного видеоархивов;

2) координацию потоков данных, поступающих от оперативного и долговременного архивов;

3) хранение конфигурации подключения к «АПИ Архива» и «АПИ Управления камерами».

3.3.10. Программа «АПИ Аналитики» обеспечивает выполнение следующих функций:

1) обработку запросов от «АПИ Камер» на получение трансляции аналитики;

2) предоставление интерфейса для настройки и мониторинга работоспособности программных серверов видеоанализа;

3) настройку и обеспечение работоспособности программных серверов видеоанализа;

4) реализацию логики управления и контроля за выполнением аналитических функций.

3.3.11. Программы «Сервер обслуживания» и «Клиент сервиса обслуживания» решают задачи по централизованному обслуживанию и обновлению программного обеспечения комплекса. Программа «Сервер обслуживания» выполняет рассылку обновлений, а программы «Клиент сервиса обслуживания», хранят информацию об установленной версии СПО «Тобол-ИПК» и отдельных его компонентов, взаимодействуют с репозиторием обновлений и контролируют процесс запуска инсталляционных пакетов, обеспечивающих установку обновленного программного обеспечения.

3.3.12. Программа «Редактор отчетных форм» обеспечивает возможность создания и сохранения шаблонов для пропусков и отчетов.

3.3.13. Программа «Адаптер интеграции» обеспечивает взаимодействие с внешними системами.

3.3.14. Программа «Утилита печати пропусков» обеспечивает проверку работы принтера для печати пропусков и фотоаппарата в автономном режиме (без подключения к серверу).

3.3.15. Программа «Конфигуратор» обеспечивает конфигурацию программных средств без их повторной инсталляции.

3.3.16. Программа «Служба очередей» обеспечивает взаимодействие между программами посредством организации очередей с пакетами передачи данных.

3.3.17. Программа «Служба сообщений для видеосистемы» обеспечивает передачу команд управления и служебных сообщений.

3.3.18. Программа «Сервис управления» обеспечивает запуск, останов и контроль выполнения программ.

3.3.19. Программа «Контроль целостности» обеспечивает периодический контроль целостности файлов путем запуска программы md5sum из состава ОС Astra Linux и сравнения результатов с заданными контрольными суммами.

3.4. Встроенные средства защиты информации (СЗИ) из состава СПО «Тобол-ИПК» представляет собой совокупность следующих подсистем защиты информации:

- подсистемы управления доступом;
- подсистемы регистрации и учета;
- подсистемы обеспечения целостности.

3.4.1. Подсистема управления доступом

Подсистема обеспечивает выполнение следующих функций безопасности:

1) при осуществлении доступа к СПО «Тобол-ИПК» проводится идентификация и аутентификация операторов (приём смены), администраторов безопасности по их идентификаторам (имя учетной записи или номер) и паролям со сроком действия не более одного месяца и длиной не менее восьми алфавитно-цифровых символов (при обработке информации с максимальным грифом секретности – «совершенно секретно») и не менее шести алфавитно-цифровых символов (при обработке информации с максимальным грифом секретности – «секретно» и другой информации, не составляющей государственной тайны). Формируемые пароли удовлетворяют минимальным требованиям к их качеству – включать заглавные и прописные буквы, цифры и специальные знаки (подчеркивание, дефис, тильда и т.д.);

2) полный доступ к программным ресурсам АСФЗ имеют только администраторы безопасности со всеми правами доступа и управления. В процессе эксплуатации они могут, при необходимости осуществлять

перезагрузку операционной системы на любых компьютерах. Операторы имеют права на перезагрузку рабочих мест при аварийной ситуации и при технической необходимости, предусмотренной в эксплуатационной документации. В процессе эксплуатации перезагрузка операционной системы во время приёма-сдачи смены операторами не осуществляется. После загрузки ОС Astra Linux администратором безопасности на компьютерах системы операторам должен предоставляться ограниченный интерфейс соответствующей функциональности АРМ в рамках, предоставленных администратором безопасности прав и полномочий, не позволяющим выполнять какие-либо программы и команды операционной системы;

3) проводится идентификация компьютеров АСФЗ (серверов, рабочих станций, контроллеров, групповых контроллеров) по их именам и/или логическим (IP) и/или физическим (MAC) адресам при загрузке (перезагрузке) системы на компьютерах и с заданной периодичностью в автоматическом режиме в процессе работы системы, а также по запросу администратора безопасности и/или оператора;

4) проводится контроль соответствия физических адресов подключенных периферийных устройств адресам, установленным при их конфигурации с заданной периодичностью в автоматическом режиме в процессе работы СПО «Тобол-ИПК», а также по запросу администратора безопасности и/или оператора;

5) проводится контроль доступа (управление доступом) персонала АСФЗ к программам, пунктам меню программ, командам, операциям с данными АСФЗ по таблицам санкционирования.

3.4.2. Подсистема регистрации и учета

Подсистема регистрации и учета обеспечивает выполнение следующих задач:

1) осуществляется регистрация попыток доступа к СПО «Тобол-ИПК» операторов (приём смены) администраторов безопасности. В параметрах регистрации указываются:

- время и дата попытки доступа к СПО «Тобол-ИПК» персонала АСФЗ;
- идентификатор (имя учетной записи) оператора АСФЗ;

– идентификаторы (наименование, адрес) компьютера, на котором проведена попытка доступа;

– результат попытки доступа: успешный или неуспешный – несанкционированный, причина неуспешной попытки (неправильные идентификатор, пароль и т.п.);

2) осуществляется регистрация неуспешной идентификации компьютеров (несоответствие MAC-адреса IP-адресу сервера или АРМ) и периферийных устройств (прерывания связи с периферийными устройствами). В параметрах регистрации указываются:

– время и дата проведения идентификации;

– идентификаторы (наименование, адрес) компьютера и/или периферийного устройства, не прошедшие успешную идентификацию (периферийного устройства, с которым прервана связь);

3) осуществляется регистрация попыток логического доступа персонала АСФЗ к программам, командам, периферийным устройствам (техническим средствам охраны, считывателям, устройствам преграждающим управляемым (УПУ), УВИП, исполнительным устройствам, видеокамерам и т.д.) и операциям с данными АСФЗ. В параметрах регистрации указываются:

– время и дата попытки доступа;

– вид запрашиваемой операции с данными (просмотр, удаление, добавление, изменение);

– идентификатор (имя учетной записи) оператора АСФЗ;

– спецификация (наименование) запрошенной программы, команды (включение, отключение, блокирование, разблокирование периферийных устройств, открытие УПУ, блокирование УПУ и т.п.);

– результат попытки: успешный или неуспешный – несанкционированный (отсутствует право на запуск программы, на выполнение команды, на выполнение операции с данными);

4) осуществляется регистрация завершения сеанса работы оператора (сдача смены оператором). В параметрах регистрации указываются:

– время и дата завершения работы;

– идентификатор (имя учетной записи) оператора (администратора безопасности);

– идентификаторы (наименование, адрес) компьютера, на котором завершена работа (сдана смена оператором);

5) осуществляется регистрация попыток изменения полномочий (прав) операторов. В параметрах регистрации указываются:

– время и дата попытки внесения изменения;

– идентификатор (имя учетной записи) оператора, проводившего изменение (попытку изменения);

– идентификатор (имя учетной записи) оператора, у которого пытались изменить полномочия;

– вид запрошенного изменения (удаление, добавление, изменение прав, внесение, исключение из списка доступа, изменение имени, пароля и т.п.);

– результат попытки: успешный или неуспешный – несанкционированный (отсутствует право на изменение);

6) осуществляется регистрация попыток изменения прав доступа оператора на объект. В параметрах регистрации должны быть указаны:

– время и дата попытки внесения изменения;

– идентификатор (имя учетной записи) оператора, проводившего изменение (попытку изменения);

– идентификатор (имя учетной записи) оператора, у которого пытались изменить права доступа на объект;

– вид запрошенного изменения (удаление, добавление, изменение прав, внесение, исключение из списка доступа);

– результат попытки: успешный или неуспешный – несанкционированный (отсутствует право на изменение);

7) осуществляется регистрация несанкционированного физического доступа к оборудованию АСФЗ, в шкафы и/или помещения, где установлено оборудование. Регистрация несанкционированного физического доступа должна осуществляться по факту тревожных сообщений о срабатывании датчиков вскрытия, установленных на охрану при открывании дверей шкафов или помещений. В параметрах регистрации указываются:

– время и дата несанкционированного физического доступа к оборудованию или в помещения АСФЗ (вскрытия дверей, коммуникационных шкафов и т.п.);

– место осуществления доступа (наименование/адрес компьютера, периферийного устройства, номер помещения, коммуникационного шкафа, идентификатор защищаемого оборудования и т.п.);

8) осуществляется настройка отображения сообщений от средств регистрации, а также задание размера архива сообщений, при достижении которого включается функция защиты от переполнения жесткого диска, должны быть доступны только администратору безопасности. Ручное удаление записей из архива должно быть запрещено всем пользователям. Каждому оператору должно индивидуально назначаться право на просмотр сообщений о тех или иных событиях, предусматривающее средства фильтрации, сортировки и поиска сообщений;

9) проводится сигнализация (оперативное отображение) попыток несанкционированного доступа к СПО «Тобол-ИПК» на компьютере, используемом при попытке доступа, и/или компьютере администратора безопасности;

10) проводится индикация (оперативное отображение) неуспешной идентификации компьютеров (несоответствие MAC-адреса IP-адресу) или периферийных устройств (прерывания связи с периферийными устройствами) на перезагружаемом компьютере. Данные сигнализации включают в себя идентификаторы (наименование, адрес) компьютера и/или периферийного устройства, не прошедших успешную идентификацию (периферийного устройства, с которым прервана связь);

11) проводится регистрация и учет выходных печатных документов. Выдача печатных документов осуществляется только в соответствии с установленным перечнем шаблонов с указанием их уровня конфиденциальности (степени секретности);

12) доступ к просмотру журнала событий имеют только пользователи, наделенные соответствующими полномочиями. Изменить содержимое журнала событий, равно как и удалить его, невозможно ни с какими правами. Записи журнала событий, по истечению заранее определенного времени, переносятся

в архив, либо удаляются из базы данных автоматически (в зависимости от настроек).

3.4.3. Подсистема обеспечения целостности

Подсистема обеспечения целостности обеспечивает выполнение следующих задач:

1) контроль целостности СЗИ НСД при загрузке и с заданной периодичностью в автоматическом режиме в процессе работы СПО «Тобол-ИПК», а также по запросу администратора безопасности и/или оператора по эталонным контрольным суммам всех файлов и данных СЗИ НСД;

2) контроль целостности чувствительных данных АСФЗ, включая программы, при загрузке СПО «Тобол-ИПК» и с заданной периодичностью в автоматическом режиме в процессе работы, а также по запросу администратора безопасности и/или оператора по эталонным контрольным суммам;

3) дублирование на разных компьютерах в реальном масштабе времени чувствительные данные АСФЗ (базы данных, файлы), блокирование доступа к которым или их искажение/потеря может привести к нарушению работоспособности, включая данные СЗИ НСД. При недоступности одного набора чувствительных данных АСФЗ автоматически переключается на второй (дублируемый) набор данных;

4) реализация средств автоматического архивирования (резервного копирования) и восстановления чувствительных данных АСФЗ, включая данные СЗИ НСД;

5) автоматизированное (программное) тестирование СЗИ НСД;

6) управление переключением при организации резервирования «в горячем режиме» критичного оборудования, отказ которого может привести к отказу всей АСФЗ (серверы, коммуникационное оборудование, линии связи и т.д.).

4. КОМПЛЕКТНОСТЬ

4.1. Комплектность СПО «Тобол-ИПК» представлена в таблице 5.

Таблица 5 – Комплектность СПО «Тобол-ИПК»

Обозначение	Наименование	Кол.	Порядковый учетный номер	Примечание
ЦКДИ.00621-01 12 01	Специальное программное обеспечение «Тобол-ИПК». Инсталлятор	1		Компакт-диск ЦКДИ.00621-01 №1
ЦКДИ.00621-01 30 01-1	Специальное программное обеспечение «Тобол-ИПК». Формуляр. Часть 1	1		Твердая копия
ЦКДИ.00621-01 30 01-2	Специальное программное обеспечение «Тобол-ИПК». Формуляр. Часть 2	1		В электронном виде. Компакт-диск ЦКДИ.00621-01 №2
ЦКДИ.00621-01 32 01	Специальное программное обеспечение «Тобол-ИПК». Администратор безопасности. Руководство системного программиста	1		В электронном виде. Компакт-диск ЦКДИ.00621-01 №2
ЦКДИ.00621-01 34 01	Специальное программное обеспечение «Тобол-ИПК». Руководство оператора	1		В электронном виде. Компакт-диск ЦКДИ.00621-01 №2

Продолжение таблицы 5

Обозначение	Наименование	Кол.	Порядковый учетный номер	Примечание
	Заверенная копия сертификата соответствия средства защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00	1		Твердая копия

Контрольные суммы дистрибутива СПО «Тобол-ИПК» рассчитаны с использованием программы фиксации и контроля исходного состояния Gostsum по стандарту ГОСТ Р 34.11-2012, которая входит в состав сертифицированной версии ОС Astra Linux (сертификат № 2557, выдан 27.01.2012 года, техническая поддержка осуществляется до 31.12.2028 года) и программы фиксации и контроля целостности информации «ФИКС-UNIX 1.0» по алгоритму «Уровень 3» (Сертификат соответствия № 680, выдан ФСТЭК России 30 октября 2002 года, техническая поддержка осуществляется до 2026 года) и соответствуют контрольным суммам, приведенным в настоящем формуляре на СПО «Тобол-ИПК» ЦКДИ.00621-01 30 01-1, Приложение 1.

Контрольные суммы исполняемых файлов СПО «Тобол-ИПК» рассчитаны с использованием программы фиксации и контроля исходного состояния Gostsum по стандарту ГОСТ Р 34.11-2012, которая входит в состав сертифицированной версии ОС Astra Linux (сертификат № 2557, выдан 27.01.2012 года, техническая поддержка осуществляется до 31.12.2028 года) и соответствуют контрольным суммам, приведенным в формуляре на СПО «Тобол-ИПК» ЦКДИ.00621-01 30 01-2.

5. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

5.1. При эксплуатации СПО «Тобол-ИПК» на объектах информатизации, где производиться обработка конфиденциальной информации, необходимо выполнение следующих ограничений:

1) наличие администратора безопасности, отвечающего за эксплуатацию СПО «Тобол-ИПК»;

2) установка осуществляется на оборудование, соответствующее требованиям, определенным в настоящем документе;

3) периодический контроль целостности дистрибутивных носителей СПО «Тобол-ИПК» (один раз в год в процессе проведения регламентных работ);

4) проведение периодического контроля целостности исполняемых файлов СПО «Тобол-ИПК» (не реже одного раза в месяц);

5) периодический контроль целостности средств защиты информации (не реже одного раза в квартал);

6) проведение периодической проверки на наличие актуальных уязвимостей (недостатков) в СПО «Тобол-ИПК» и среде его функционирования с использованием средств анализа защищенности (не реже одного раза в месяц);

7) проведение периодической проверки СПО «Тобол-ИПК» и среды его функционирования на наличие компьютерных вирусов с использованием средств антивирусной защиты (не реже одного раза в месяц);

8) периодический контроль дистрибутивных носителей СПО «Тобол-ИПК» (один раз в год в процессе проведения регламентных работ);

9) для программного обеспечения среды функционирования СПО «Тобол-ИПК» установка всех актуальных обновлений, выпущенных разработчиком операционной системы, либо применены меры, позволяющие исключить возможность эксплуатации известных уязвимостей в программном обеспечении среды функционирования;

10) выполнены рекомендации разработчиков по безопасному конфигурированию СПО «Тобол-ИПК» согласно документу «Администратор безопасности. Руководство системного программиста» ЦКДИ.00621-01 32 01;

11) обеспечена сохранность оборудования и физическая целостность системных блоков и другого оборудования, оснащенных компонентами СПО «Тобол-ИПК»;

12) при эксплуатации СПО «Тобол-ИПК» должна быть обеспечена сохранность паролей и идентификаторов администратора безопасности;

13) не реже одного раза в месяц должен проводиться периодический контроль целостности исполняемых файлов СПО «Тобол-ИПК»;

14) программная среда функционирования СПО «Тобол-ИПК» должна быть свободна от вредоносного программного обеспечения;

15) программная среда функционирования СПО «Тобол-ИПК» не должна содержать средств разработки и отладки программного обеспечения;

16) каналы передачи данных (включая каналы управления), используемые СПО «Тобол-ИПК», должны быть либо расположены в пределах контролируемой зоны и защищены с использованием организационно-технических мер, либо, в случае их выхода за пределы контролируемой зоны, должны быть защищены путем применения средств криптографической защиты информации, сертифицированных в системе сертификации ФСБ России.

Контроль СПО «Тобол-ИПК» проводится организацией, эксплуатирующей изделие, при первичном закреплении и в дальнейшем в процессе проведения регламентных работ.

Проверка целостности исполняемых файлов в процессе эксплуатации осуществляется путем подсчета их контрольных сумм и сравнения их с контрольными суммами, приведенными во второй части настоящего формуляра ЦКДИ.00621-01 30 01-2.

В случае обнаружения уязвимостей, должно производиться их устранение в соответствие с методами и процедурами, приведенными в разделе 12.

Проведение периодической проверки СПО «Тобол-ИПК» и среды его функционирования на наличие компьютерных вирусов проводится с использованием сертифицированных по требованиям безопасности информации средств антивирусной защиты. Обновление баз данных средств антивирусной защиты должно осуществляться не реже одного раза в месяц.

Контроль дистрибутивных носителей СПО «Тобол-ИПК» состоит из визуального выявления механических повреждений компакт-диска и проверки сохранности информации, записанной на компакт-диске. Проверка сохранности информации, записанной на компакт-диске, осуществляется путем подсчета контрольной суммы файла дистрибутива СПО «Тобол-ИПК» и сравнения их с контрольной суммой, приведенной в таблице 1.1 приложения 1 настоящего формуляра.

Периодический контроль средств защиты информации производится путем периодического тестирования следующих подсистем:

- подсистемы управления доступом;
- подсистемы регистрации и учета;
- подсистемы контроля целостности.

Методика периодического контроля приведена в приложении 2 настоящего формуляра.

Формат заполнения результатов периодического контроля основных характеристик при эксплуатации и хранении представлен в таблице 6.

Таблица 6 – Результаты периодического контроля основных характеристик при эксплуатации и хранении

Проверяемая характеристика		Дата проведения измерения					
		20__г.		20__г.		20__г.	
Наименование измерения	Величина	Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)
Значения контрольных сумм	При проверке значение должно совпадать со значением, указанным в формуляре						

6. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

6.1. Специальное программное обеспечение «Тобол-ИПК» ЦКДИ.00621-01 заводской № _____ соответствует требованиям технических условий ЦКДИ.00621-01 98 01 и признано годным для эксплуатации.

Дата выпуска _____

Руководитель предприятия

М.П. _____ _____ _____

подпись фамилия дата

Начальник ОТК

_____ _____ _____

подпись фамилия дата

7. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

7.1. Специальное программное обеспечение «Тобол-ИПК» ЦКДИ.00621-01 заводской № _____ упаковано АО «ФЦНИВТ «СНПО «Элерон» в слим-бокс, снабженный этикеткой, опломбирован ОТК пломбой с оттиском клейма «_____» «_____».

Маркирован идентификатором РОСС RU.01_____._____

Дата упаковки «____» _____г.

Упаковку произвел _____ _____

подпись инициалы, фамилия

Изделие после упаковки принял:

Контролер ОТК _____ _____

подпись инициалы, фамилия

8. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

8.1. Предприятие-изготовитель АО «ФЦНИВТ «СНПО «Элерон» гарантирует соответствие качества специального программного обеспечения «Тобол-ИПК» требованиям технических условий ЦКДИ.00621-01 98 01 при соблюдении потребителем условий и правил хранения, транспортирования и эксплуатации, установленных в эксплуатационной документации.

8.2. Предприятие-изготовитель принимает на себя обязательства по поиску ошибок реализации и уязвимостей в специальном программном обеспечении «Тобол-ИПК» на протяжении всего его жизненного цикла, а также обязательства по своевременному информированию потребителя о найденных ошибках и уязвимостях, методах безопасного применения специального программного обеспечения «Тобол-ИПК».

8.3. Гарантийный срок хранения – не более 5 лет даты изготовления при соблюдении условий хранения в соответствии с разделом 7 технических условий ЦКДИ.00621-01 98 01 и с периодической проверкой согласно 6.6 технических условий ЦКДИ.00621-01 98 01 дистрибутивного компакт-диска один раз в год на объекте эксплуатации.

8.4. Гарантийный срок эксплуатации (отсчитывается с даты ввода изделия в эксплуатацию) и срок гарантийного обслуживания определяются условиями договора поставки специального программного обеспечения «Тобол-ИПК».

8.5. Гарантийные обязательства предприятия-изготовителя специального программного обеспечения «Тобол-ИПК» не распространяются на копии, изготовленные по инициативе потребителя.

8.6. Действие гарантийных обязательств на выполнение функций специального программного обеспечения «Тобол-ИПК» прекращается, если потребителем внесены изменения в специальное программное обеспечение «Тобол-ИПК» без согласования с предприятием-изготовителем или специальное программное обеспечение «Тобол-ИПК» передано другому предприятию (потребителю).

8.7. Базовая поддержка безопасности специального программного обеспечения «Тобол-ИПК» входит в стоимость поставляемого изделия и обеспечивается предприятием-изготовителем в течение срока действия сертификата соответствия ФСТЭК России.

8.8. Иные виды технической поддержки (расширения сервисов технической поддержки) предоставляются предприятием-изготовителем на возмездной основе, в соответствии с действующими политиками и правилами оказания технической поддержки продуктов предприятия-изготовителя.

9. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

9.1. Рекламации принимаются в период действия гарантийных обязательств.

9.2. В рекламации должно быть изложено:

- наименование неисправного компонента СПО «Тобол-ИПК»;
- дата обнаружения неисправности;
- характер неисправности (описание обнаруженного дефекта);
- условия возникновения неисправности.

9.3. Рекламационные акты, претензионные письма направляются по адресу: г. Москва, ул. Генерала Белова, д. 14, АО «ФЦНИВТ «СНПО «Элерон».

9.4. Все предъявляемые рекламации регистрируют в таблице 7.

Таблица 7 – Предъявляемые рекламации

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

10. СВЕДЕНИЯ О ХРАНЕНИИ

10.1. Компакт-диск с СПО «Тобол-ИПК» в упаковке, поставленной предприятием-изготовителем, хранится в вертикальном положении на предназначенном для этой цели стеллаже. Программная документация располагается на рабочих местах операторов. Хранение компакт-диска и документации осуществляется при температуре окружающего воздуха от плюс 5°С до плюс 40°С и относительной влажности воздуха от 40 до 80 % при температуре 25°С.

10.2. В помещении для хранения компакт-диска с СПО «Тобол-ИПК» не должно быть агрессивных примесей (паров кислот, щелочей).

10.3. При хранении не допускаются резкие изменения температуры окружающего воздуха (более 20°С в час) и воздействия внешних магнитных полей напряженностью более 4000 А/м.

10.4. Сроки хранения и условия хранения СПО «Тобол-ИПК» указывают в таблице 8.

Таблица 8 – Сроки хранения и условия хранения

Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
установки на хранение	снятия с хранения		

11. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

11.1. Сведения о закреплении СПО «Тобол-ИПК» заносят в таблицу 9.

Таблица 9 – Сведения о закреплении СПО «Тобол-ИПК»

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

12. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

12.1. Предприятие-изготовитель осуществляет прием сообщений о недостатках от потребителей по телефону, указанному на информационном ресурсе предприятия-производителя (https://www.eleron.ru/) и электронной почте support@eleron.ru.

12.2. Информирование потребителей о мерах, направленных на нейтрализацию выявленных уязвимостей СПО «Тобол-ИПК» и выпускаемых обновлениях СПО «Тобол-ИПК», выполняется путем публикации информации на информационном ресурсе предприятия-производителя (https://support.eleron.ru/).

12.3. Предоставление потребителям обновления СПО «Тобол-ИПК» на компакт диске осуществляется после проведения необходимых испытаний. Перед установкой полученных обновлений СПО «Тобол-ИПК» администратору безопасности необходимо провести контроль полученных файлов и провести инсталляцию обновлений:

– проверить подлинность файлов обновлений посредством электронной подписи. Если подлинность файлов обновлений не подтверждена, необходимо обратиться в службу поддержки предприятия-изготовителя;

– провести расчет контрольных сумм файлов обновлений с использованием программы фиксации и контроля исходного состояния Gostsum по ГОСТ Р 34.11-2012, которая входит в состав сертифицированной версии ОС Astra Linux. Сравнить контрольные суммы файлов обновлений с указанными на компакт-диске. При расхождении контрольных сумм с эталонными значениями необходимо обратиться в службу поддержки производителя;

– произвести инсталляцию актуальных обновлений.

12.4. Предприятие-изготовитель принимает на себя обязательства по поиску ошибок реализации, уязвимостей и по устранению недостатков в СПО «Тобол-ИПК» на протяжении всего его жизненного цикла, а также обязательства по своевременному извещению потребителей о найденных ошибках и уязвимостях, методах безопасного использования СПО «Тобол-ИПК».

12.5. Предприятие-изготовитель периодически (не реже одного раза в месяц) должно проводить поиск известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях. В качестве общедоступных источников в первую очередь должны использоваться база данных уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), а также следующие дополнительные источники:

– https://cve.mitre.org/;

– https://nvd.nist.gov/;

– https://www.exploit-db.com/;

– http://www.rapid7.com/db/;

– http://www.cvedetails.com/;

– http://www.securitylab.ru/ и другие.

12.6. Процедура устранения уязвимостей СПО «Тобол-ИПК» обеспечивает возможность обновления программного обеспечения для устранения актуальных уязвимостей.

12.7. Предприятие-изготовитель должен провести анализ выявленных уязвимостей на предмет возможности их использования для нарушения безопасности. При анализе уязвимостей необходимо учитывать следующие критерии:

– тип ошибки;

– версию программного обеспечения, подверженную уязвимости;

– уровни опасности уязвимости (критическая, высокая, средняя, низкая);

– информацию об устранении.

12.8. В случае выявления информации об уязвимости СПО «Тобол-ИПК» и среды его функционирования из различных источников и отсутствия информации об этой уязвимости в базе данных уязвимостей (далее по тексту –

БДУ), предприятие-изготовитель предоставляет информацию о данной уязвимости в ФСТЭК России для размещения в БДУ.

12.9. Устранение недостатков должно предусматривать:

– разработку компенсирующих мер по защите информации или ограничений по применению средства, а также доведение информации о таких мерах и ограничениях в срок не более 48 ч с момента выявления недостатка;

– доработку, в том числе разработку обновлений СПО «Тобол-ИПК» или разработку мер по защите информации, нейтрализующих недостаток в срок не более 60 дней с момента выявления недостатка.

12.10. При выявлении уязвимостей СПО «Тобол-ИПК» предприятие-изготовитель должно выполнить следующие мероприятия:

– осуществить исправление уязвимости СПО «Тобол-ИПК»;

– разместить информационное сообщение об уязвимостях СПО «Тобол-ИПК» на специализированном разделе информационного ресурса предприятия-производителя https://eleron.ru/;

– довести информацию до конечных потребителей СПО «Тобол-ИПК» об организационно-технических мерах по устранению уязвимостей СПО «Тобол-ИПК» с обеспечением подлинности и целостности доводимой информации;

– оповестить потребителей СПО «Тобол-ИПК» о необходимости установки и порядке установки обновленной версии СПО «Тобол-ИПК»;

– обеспечить гарантированную доставку с обеспечением подлинности и целостности доводимой информации конечным потребителям файлов обновлений СПО «Тобол-ИПК».

12.11. Конечные потребители, при обновлении СПО «Тобол-ИПК», вносят соответствующие отметки в разделы формуляра.

12.12. Информацию об изменении версии СПО «Тобол-ИПК» предприятие-изготовитель заносит в извещение об изменениях на СЗИ, и представляет его в Испытательную лабораторию, ФСТЭК России и доводит до сведения конечных потребителей СПО «Тобол-ИПК».

12.13. Предприятие-изготовитель обязано провести испытания доработанного СПО «Тобол-ИПК» в связи с внесением в него изменений (в случае изменений касающихся функций безопасности, для проведения испытаний привлекается испытательная лаборатория).

12.14. В случае отсутствия, на момент проверки информации по выявленным уязвимостям СПО «Тобол-ИПК», доступных релизов СПО «Тобол-ИПК» с устраненными уязвимостями, предприятие-изготовитель должно разработать и предоставить конечному потребителю перечень (регламент) организационно-технических мероприятий и компенсирующих мер, направленных на исключение возможности эксплуатации выявленной уязвимости злоумышленниками.

12.15. Предприятие-изготовитель предоставляет конечному потребителю СПО «Тобол-ИПК» инструкцию по проведению организационно-технических мероприятий, направленных на исключение возможности эксплуатации выявленной уязвимости злоумышленниками в соответствующем разделе сайта производителя.

12.16. В случае невозможности устранения уязвимостей СПО «Тобол-ИПК», в том числе путем применения обновления, предприятие-изготовитель разрабатывает ограничения по применению СПО «Тобол-ИПК», которые незамедлительно доводит до испытательной лаборатории.

12.17. Если в соответствии с заключением испытательной лаборатории ограничение по применению позволит устранить уязвимость, предприятие-изготовитель с обеспечением подлинности и целостности доводимой информации незамедлительно и гарантированно с обеспечением подлинности и целостности доводимой информации доводит его до конечных потребителей.

12.18. Предприятие-изготовитель вносит необходимые изменения в эксплуатационную документацию и направляет её совместно с заключением испытательной лаборатории в ФСТЭК России. Потребители реализуют указанное ограничение по применению СПО «Тобол-ИПК».

12.19. Если потребитель не может реализовать ограничение по применению СПО «Тобол-ИПК», он прекращает его применение.

12.20. Если уязвимость не устраняется путем обновления или реализацией ограничений по применению, предприятие-изготовитель незамедлительно и гарантированно, с подтверждением, сообщает об этом всем потребителям и во ФСТЭК России. Потребители прекращают применение СПО «Тобол-ИПК».

Сведения об изменениях заносят в таблицу 10.

Таблица 10 – Сведения об изменениях

Основание (входящий номер сопроводи-тельного документа и дата)	Дата прове-дения изменения	Содержание изменения	Порядковый номер изменения	Должность, фамилия и подпись лица, ответствен-ного за проведение изменения	Подпись лица, ответствен-ного за эксплуата-цию изделия

13. ОСОБЫЕ ОТМЕТКИ

ПРИЛОЖЕНИЕ 1

КОНТРОЛЬНЫЕ СУММЫ ДИСТРИБУТИВА СПО «ТОБОЛ-ИПК»

1.1. Контрольные суммы дистрибутива СПО «Тобол-ИПК» приведены в таблице 1.1.

Таблица 1.1 – Контрольные суммы дистрибутива ЦКДИ.00621-01

Наименование	Контрольная сумма (Gostsum)	Контрольная сумма (ФИКС-UNIX 1.0)
Дистрибутив СПО «Тобол-ИПК» (компакт-диск)	0c611b74d56c120d9c7a657b51b351b8a91531829c17fcdeaea9e2e6b368ee0e	9B000652

Примечание. Расчет контрольных сумм дистрибутива СПО «Тобол-ИПК» произведен программой фиксации и контроля исходного состояния Gostsum по ГОСТ Р 34.11-2012, которая входит в состав сертифицированной версии ОС Astra Linux, и программой фиксации и контроля целостности информации «ФИКС-UNIX 1.0» по алгоритму «Уровень 3» (Сертификат соответствия № 680, выдан ФСТЭК России 30 октября 2002 года, техническая поддержка осуществляется до 2026 года).

ПРИЛОЖЕНИЕ 2

МЕТОДИКА ПЕРИОДИЧЕСКОГО КОНТРОЛЯ КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Периодическое тестирование всех функций средств защиты информации СПО «Тобол-ИПК» от несанкционированного доступа должно проводиться не реже одного раза в квартал.

2.2. Проверка подсистемы управления доступом

Проверка подсистемы управления доступом проводится путем контроля:

1) доступа субъектов к программам;

2) доступа субъектов к защищаемым ресурсам.

Перед проведением проверок по данному пункту необходимо:

1) создать в системе несколько тестовых сотрудников (не менее трех) с индивидуальными карточками для их прохода в охраняемые зоны, определенные на стенде испытаний;

2) создать в системе несколько тестовых пользователей, относящихся к категории администраторов безопасности, операторов режима, операторов и постовых, присвоить им персональные идентификаторы и назначить пароли для идентификации и аутентификации;

3) определить (создать новые или назначить уже существующие в системе) защищаемые ресурсы, которые будут использоваться при проведении проверок, при этом в перечень тестовых защищаемых ресурсов должны быть включены ресурсы всех типов.

2.3. Проверка идентификации, подлинности и контроль доступа субъектов

В процессе проверки выполняется создание, модификация или удаление учетных записей пользователей. В процессе создания и модификации учетных записей пользователей проверяется наличие и правильность работы функций контроля уникальности задаваемого идентификатора и длины (не менее восьми символов) пароля.

Проверка правильности работы функций идентификации и аутентификации пользователей проверяется при:

1) приеме пользователем смены в программах «Режим», «Администратор» и «Оператор»;

2) сдаче пользователем смены в программах «Режим» и «Оператор».

В процессе идентификации пользователей должна проводиться проверка принадлежности предъявленного идентификатора множеству всех зарегистрированных в базе учетных записей идентификаторов пользователей. Если пользователь предъявляет идентификатор неизвестный системе (т.е. не зарегистрированный в базе учетных записей), то средства управления должны отвергать попытку приема/сдачи смены.

При успешной идентификации проверяется правильность предъявленного пользователем пароля (аутентификации).

При проверке идентификации и аутентификации пользователей проверяются также функции:

1) контроля срока действия учетной записи пользователя и пароля;

2) блокировки учетной записи пользователя на АРМ, с которого осуществлены подряд три попытки неудачной аутентификации;

3) контроля наличия пользователя в помещении, в котором находится АРМ;

4) контроля наличия разрешения на работу пользователя в данное время суток.

СЗИ СПО «Тобол-ИПК» предусматривают возможность выхода/сдачи смены администратором безопасности в программах «Режим» и «Оператор» вместо оператора, принявшего смену в случае, если тот по каким-либо причинам не может это сделать самостоятельно. Выполняется проверка, что только администратор безопасности может выполнить операцию по выходу/сдаче смены в вышеуказанных программах.

Проверку считать выполненной, если:

1) при многократных попытках ввода неправильного идентификатора и/или пароля доступ отклоняется:

- запуск/останов клиентской части СПО «Тобол-ИПК»;

– операция приема/сдачи смены пользователем;

2) операция входа в программу СПО «Тобол-ИПК» или приема смены отклоняется в случае, если учетная запись пользователя заблокирована;

3) операция входа в программу СПО «Тобол-ИПК» или приема смены отклоняется в случае, если учетная запись пользователя устарела;

4) операция входа в программу СПО «Тобол-ИПК» или приема смены отклоняется в случае, если срок действия учетной записи пользователя еще не наступил;

5) попытки входа в программу СПО «Тобол-ИПК» или приема смены от имени оператора или постового, которые находятся вне помещения, где находится АРМ, отвергнуты;

6) попытки входа в программу СПО «Тобол-ИПК» или приема смены пользователем в неразрешенное время суток отвергнуты;

7) попытка создания учетной записи пользователя отклоняется в случае, если учетная запись с таким идентификатором уже имеется в базе данных (идентификатор не является уникальным);

8) попытка задания администратором безопасности паролей длиной менее 8 символов отвергается;

9) операцию по сдаче смены в программах «Режим» и «Оператор» кроме пользователя, принявшего смену, может выполнить только пользователь с привилегиями администратора безопасности.

2.4. Контроль доступа субъектов к программам

Помимо сертифицированной операционной системы разграничение доступа пользователей к программам СПО «Тобол-ИПК» выполняет СЗИ в соответствии с заданными администратором безопасности привилегиями (ролями).

При испытаниях по данному требованию выполняется проверка разграничения доступа к клиентским программам со стороны пользователей, имеющих разные привилегии (роли).

На АРМах оператора режима, оператора и постового с помощью нажатия различных комбинаций клавиш, включая горячие клавиши (например, Alt+F2) и правой клавиши мыши, выполняется проверка отсутствия возможности выхода у непривилегированных пользователей (оператор режима, оператор, постовой)

из клиентских приложений (программ «Режим», «Оператор») в операционную систему с целью последующего запуска ее штатных программ.

Проверку считать выполненной, если:

1) при попытке доступа пользователя к АРМу:

– успешно осуществить доступ к программе «Оператор» может только оператор, имеющий привилегию «Оператор», или администратор безопасности;

– успешно осуществить доступ к программе «Режим» может только оператор, имеющий привилегию «Оператор режима СУР», или администратор безопасности;

– успешно осуществить доступ к программе «Администратор» может только администратор безопасности;

2) у непривилегированного пользователя (оператора и постового) на АРМ отсутствует возможность выхода из меню клиентской программы в ОС Astra Linux.

2.5. Проверка подсистемы регистрации и учета

Процесс регистрации в СПО «Тобол-ИПК» осуществляется на серверах среднего и верхнего уровней программного обеспечения с помощью сертифицированных по требованиям безопасности встроенных средств защиты информации от несанкционированного доступа ОС Astra Linux, то оценка качества и полноты реализации данных функций защиты производится только в случае необходимости. ОС Astra Linux также выполняет очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютера и внешних накопителей, а также автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти компьютера, выделяемых для обработки защищаемых файлов, внешних устройств, каналов связи, узлов локальной вычислительной сети, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом.

При проведении испытаний проверяется регистрация событий (аудит), связанных с идентификацией и аутентификацией пользователей при входе/выходе в/из программ СПО «Тобол-ИПК», а также приеме/сдаче смены, в

процессе испытания подсистемы управления доступом с указанием в параметрах регистрации:

1) даты и времени попытки входа/выхода или приема/сдачи субъекта;

2) результата попытки: успешный или неуспешный;

3) идентификатор (имя учетной записи) субъекта, предъявленный при попытке доступа;

4) код или пароль, предъявленный при неуспешной попытке.

Проверку считать выполненной, если:

5) средствами (механизмами) объекта испытаний осуществляется регистрация событий (аудит), связанных:

– с идентификацией и аутентификацией пользователей при входе/выходе в/из программ СПО «Тобол-ИПК», а также приеме/сдаче смены;

– с изменением полномочий пользователей;

6) в составе объекта испытаний предусмотрены средства (механизмы), обеспечивающие сигнализацию попыток нарушения защиты на АРМ оператора и администратора безопасности.

Описание средства тестирования СЗИ и настройка автоматического запуска приведены в разделе 17 документа Администратор безопасности. Руководство системного программиста ЦКДИ.00621-01 32 12.

2.6. Проверка подсистемы обеспечения целостности

Контроль целостности производится:

1) для серверной части – в процессе загрузки серверов;

2) для клиентской части – при запуске клиентской программы на выполнение.

Периодический контроль целостности СЗИ НСД настраивается в соответствии с пунктом 18.2 документа Администратор безопасности. Руководство системного программиста ЦКДИ.00621-01 32 12. Администратор безопасности также имеет возможность контролировать целостность СЗИ НСД с помощью программы «Контроль целостности».

Список проверяемых файлов для каждого объекта проверки (программы) содержится в файле XXXCheckFileList.txt. Расчетные значения контрольных сумм содержатся в файле XXX.crc, где XXX – имя объекта проверки.

Периодический контроль целостности осуществляется встроенными средствами СПО «Тобол-ИПК» при этом выполняется сравнение контрольных сумм файлов СЗИ НСД рассчитанных при помощи программы md5sum, которая входит в состав сертифицированной версии ОС Astra Linux, с расчетными значениями.

Проверку считать выполненной, если при запуске любой программы из состава СПО «Тобол-ИПК» наблюдается окно «Контроль целостности файлов программы «*Название программы*». Проверка пройдена» (рис. 2.1).

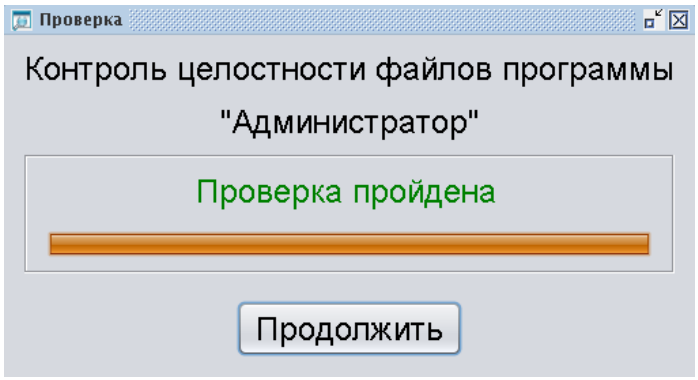

Рис. 2.1

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

АПИ	–	аппаратно-программный интерфейс
АРМ	–	автоматизированное рабочее место
АСФЗ	–	автоматизированная система физической защиты
БДУ	–	база данных уязвимостей
НСД	–	несанкционированный доступ
ОПС	–	оборудование полевой сети
ОС	–	операционная система
ОС Astra Linux	–	операционная система специального назначения «Astra Linux Special Edition»
СЗИ	–	средства защиты информации
СКМН	–	система комплексного мониторинга надежности
СКУД	–	система контроля и управления доступом
СОС	–	система охранной сигнализации
СОЭН	–	система оптико-электронного наблюдения
СПО «Тобол-ИПК»	–	специальное программное обеспечение «Тобол-ИПК» ЦКДИ.00621-01
СУБД	–	система управления базами данных
СУМ	–	сервер управления и мониторинга
СУР	–	сервер управления режимом
ТК	–	тепловизионная камера
ТСФЗ	–	технические средства физической защиты
УВИП	–	устройство ввода идентификационных признаков
УПУ	–	устройство преграждающее управляемое