**ПРОТОКОЛ ПРОВЕДЕНИЯ ИСПЫТАНИЙ № IID-1154**

**Информационной системы «Система оперативного реагирования на инциденты ИБ»**

|  |  |
| --- | --- |
| **Место проведения испытаний:** | г. Москва, ул. Беговая, д. 3с1, дистанционно |
| **Дата проведения испытаний:** | 03.10.2022 – 21.10.2022 |

**Таблица 1   
Объем испытаний реализации требований к защите информации от НСД в ИС (требования для АС класса 1Г)**

| **№  п/п** | **Реализация требования ИБ** | **№  п/п** | **Описание методики испытания** | **Критерий успешного прохождения испытания** | Результат испытания | Примечание  **(ссылка на свидетельство)** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ** | | | | | | |
|  | **ПУД.1 Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов** | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6:**  Параметры, определенные в следующих пунктах профиля ИБ для ОС Astra Linux 1.6 SE «Смоленск», способствуют частичному выполнению требования: 17; 18; 21; 22; 23; 24, 25.  Идентификация и аутентификация привилегированных пользователей при подключении по ssh осуществляется штатными средствами ОС по доменным персонифицированным УЗ.  Требования к сложности, длине паролей, сроку действия соответствуют требованиям, установленным Стандартом Компании «Политики информационной безопасности ПАО «НК «Роснефть» и Обществ Группы» № П3-11.01 С-0054 версия 1.00, введенным в действие 28.03.2017.  Доступ в систему для УЗ суперпользователя root запрещен. УЗ root на компонентах ИС отключена. В файлах /etc/passwd компонентов ИС включена следующая настройка:  root:x:0:0:root:/root:/sbin/nologin  Для УЗ root запрещено подключение к компонентам Системы В файлах /etc/ssh/sshd\_config компонентов ИС включена следующая настройка:  PermitRootLogin no  Выполнение привилегированных команд осуществляется под персонифицированными локальными учетными записями через механизм sudo. Для работы команда sudo просматривает конфигурационный файл /etc/sudoers, который содержит список групп безопасности, имеющих полномочия на ее применение и перечень команд, которые имеют право выполнять пользователи, входящие в эти группы. |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Убедиться, что отсутствуют УЗ, не описанные в ПЭД:  С помощью команды cat открыть файл /etc/samba/smb.conf:  Зафиксировать параметр username map= <местоположение файла с перечнем групп с разрешенным входом>  С помощью команды cat открыть файл с перечнем групп с разрешенным входом.  Раскрыть доменные группы безопасности с помощью оснастки Пользователи и компьютеры Active Directory.  Убедиться, что список УЗ в доменных группах, описанных в конфиг-файле, соответствует согласованной ПЭД. | В файле /etc/samba/smb.conf указан параметр «username map» с указанием местоположения файла с перечнем групп с разрешенным входом.    Список УЗ в доменных группах, описанных в конфиг-файле, соответствует согласованной ПЭД. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  В файле /etc/samba/smb.conf не указан параметр «username map»  Не реализованы компенсирующие меры по ограничению доступа УЗ Active Directory домена rosneft.ru. На серверах ИС возможно подключение от имени любой УЗ домена rosneft.ru.  Файлы:  1.1.1.1  1.1.1.2  Критичность несоответствия: высокая |
|  | С помощью команд getent passwd и getent group вывести список групп и пользователей Системы.  Раскрыть доменные группы безопасности с помощью оснастки Пользователи и компьютеры Active Directory.  Убедиться, что список групп и УЗ соответствует согласованной ПЭД. | Список групп и УЗ соответствует согласованной ПЭД | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  УЗ не соответствуют согласованной ПЭД:  A\_bodunov\_adm\_cdc  Agyutanov\_adm  Ampyatnitskiy\_adm  и другие.  Файлы:  1.1.2.1-1.1.2.10  Критичность несоответствия: высокая |
|  | На АРМ эксперта выполнить подключение через VDI к рабочему столу ADMIN.  Запустить *Командную строку* (cmd.exe) с и выполнить команду:  *dsquery user -name "ИмяУЗ" | dsget user –effectivepso*  где *ИмяУЗ* – имя привилегированной или служебной (сервисной) доменной УЗ.  Убедиться, что в выводе команды присутствует строка:  "CN=EnterpriseAdminsPSO,CN=Password Settings Container,CN=System,DC=rosneft,DC=ru"  или  "CN=AdminsAccountsPolicy,CN=Password Settings Container,CN=System,DC=rosneft,DC=ru" – для привилегированных доменных УЗ,  "CN=TechnologicalAccountsPSO,CN=Password Settings Container,CN=System,DC=rosneft,DC=ru" – для служебных (сервисных) доменных УЗ.  Провести данную проверку привилегированных и служебных (сервисных) доменных УЗ | В выводе команды для привилегированных доменных УЗ присутствует строка:  "CN=EnterpriseAdminsPSO,CN=Password Settings Container,CN=System,DC=rosneft,DC=ru"  или  "CN=AdminsAccountsPolicy,CN=Password Settings Container,CN=System,DC=rosneft,DC=ru"  В выводе команды для служебных (сервисных) доменных УЗ присутствует строка:  "CN=TechnologicalAccountsPSO,CN=Password Settings Container,CN=System,DC=rosneft,DC=ru" | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Файлы:  1.1.3.1, 1.1.3.2  Служебная УЗ не добавлена в группу TechnologicalAccountsPSO  Критичность несоответствия: высокая |
|  | На выбранном сервере Системы с помощью команды klist убедиться, что присутствуют кэшированные билеты Kerberos. | В выводе команды klist присутствуют кэшированные билеты Kerberos. | Пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Файлы:  1.1.4.1 |
|  | С помощью команд cat открыть файл /etc/pam.d/common-password. Убедиться, что для локальных УЗ парольной политикой заданы следующие параметры:  retry=10  minlen=32  lcredit=-1  ucredit=-1  dcredit=-1  ocredit=-1  enforce\_for\_root  reject\_username | На выбранном экспертами сервере в файле /etc/pam.d/common-password для парольной политики заданы следующие параметры:  retry=10  minlen=32  lcredit=-1  ucredit=-1  dcredit=-1  ocredit=-1  enforce\_for\_root  reject\_username | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Настройки парольной политики не соответствуют требованиям.  retry=3  minlen=8  lcredit – не указаны  ucredit – не указаны  dcredit – не указаны  ocredit – не указаны  enforce\_for\_root – не указаны  reject\_username – не указаны  Файлы:  1.1.5.1  Критичность несоответствия: высокая |
|  | С помощью команд:  grep PASS /etc/login.defs  grep LOGIN /etc/login.defs  Убедиться, что значения соответствуют:  PASS\_MIN\_DAYS – 1  PASS\_WARN\_AGE – 14  LOGIN\_RETRIES = 10  LOGIN\_TIMEOUT = 1800 | Значения соответствуют:  PASS\_MIN\_DAYS – 1  PASS\_WARN\_AGE – 14  LOGIN\_RETRIES = 10  LOGIN\_TIMEOUT = 1800 | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Параметр PASS\_MAX\_DAYS и LOGIN\_TIMEOUT – не соответствуют требованиям  Файлы:  1.1.6.1  Критичность несоответствия: высокая |
|  | С помощью команды cat открыть файл /etc/pam.d/su. Убедиться, что строка auth required pam\_wheel.so активна. | В файле su строка auth required pam\_wheel.so активна. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  В файле su строка auth required pam\_wheel.so отсутствует.  Файлы:  1.1.7.1  1.1.7.2  Критичность несоответствия: высокая |
|  | С помощью команды getent group wheel вывести на экран список УЗ. Убедиться, что группа wheel не содержит УЗ. | Группа wheel не содержит УЗ. | Пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Файлы:  1.1.8.1  1.1.10.1  Исполнение команды su ограниченно в sudoers |
|  | На выбранном ранее сервере ввести команду sudo su. Убедиться, что при попытке выполнения данной команды появляется сообщение о запрете ее использования. | При попытке выполнения команды sudo su появляется сообщение о запрете ее использования. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  При выполнении команды sudo su не появляется сообщение о запрете, присвоены права root  Файлы:  1.1.9.1  Критичность несоответствия: высокая |
|  | Открыть файл sudoers, содержащий список групп и их права, командой cat /etc/sudoers. С помощью команды getent group <имя группы>. Вывести на экран список УЗ, входящих в группу.  Убедиться, что появившийся список УЗ и их полномочий соответствует указанным УЗ и их полномочиям в согласованном документе ТПс и ТПр. | Список УЗ и их полномочий соответствуют согласованному документу ТПс и ТПр. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  УЗ не соответствуют согласованной ПЭД:  A\_bodunov\_adm\_cdc  Agyutanov\_adm  Ampyatnitskiy|\_adm  и другие.  Файлы:  1.1.10.1  1.1.2.3-1.1.2.10  Критичность несоответствия: высокая |
|  | Убедиться, что в файле /etc/sudoers директива "include" не активна, вида #(пробел)/etc/sudoers.d | В файле /etc/sudoers директива "include" не активна, имеет вид #(пробел)/etc/sudoers.d | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  В файле /etc/sudoers директива "include" не активна, но активна  директива #includedir /etc/sudoers.d  Файлы:  1.1.10.1  Критичность несоответствия: высокая |
|  | Убедиться, что директория /etc/sudoers.d пустая. | Директория /etc/sudoers.d пустая. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  В директории /etc/sudoers.d присутствуют следующие сущности README и zzz-parsec.  Файлы:  1.1.12.1  Критичность несоответствия: высокая |
|  | С помощью команд:  cat /etc/passwd  sudo cat /etc/shadow  Убедиться, что установлен запрет входа под УЗ root, задан параметр /sbin/nologin (false). В случае если параметр не задан /sbin/nologin проверить, что установлен знак «!» перед паролем в файле /etc/shadow.  Убедиться, что интерактивных вход в Систему под встроенными УЗ запрещен, за исключением случаев, приведенных в ПЭД. | На выбранном экспертами сервере в файле /etc/passwd установлен запрет входа под УЗ root, задан параметр /sbin/nologin (false). При отсутсвии задания /sbin/nologin установлен знак «!» перед паролем в файле /etc/shadow  Интерактивных вход в Систему под встроенными УЗ запрещен, за исключением случаев, приведенных в РОН и ИА. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.rusib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Файлы:  1.1.13.1-1.1.13.3  Присутствуют незаблокированные УЗ:  root, sync, astra-admin, postgres  Присутствует возможность подключения от имени УЗ root  Критичность несоответствия: высокая |
|  | На выбранном ранее сервере ввести команду sudo grep PermitRootLogin /etc/ssh/sshd\_config. Убедиться, что указан запрет регистрации по SSH от УЗ root («PermitRootLogin no»). | На выбранном экспертами сервере в файле /etc/ssh/sshd\_config, указан запрет регистрации по SSH от УЗ root («PermitRootLogin no»). | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  В файле /etc/ssh/sshd\_config, не указан запрет регистрации по SSH от УЗ root («PermitRootLogin no»).  Файлы:  1.1.14.1  Критичность несоответствия: высокая |
|  | С помощью команды cat открыть файл /etc/securetty и убедиться, что файл пуст. | На выбранном экспертами сервере файл /etc/securetty пуст. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  На выбранном экспертами сервере файл /etc/securetty не пустой.  Файлы:  1.1.15.1-1.1.15.6  Критичность несоответствия: высокая |
|  | Убедиться, что в согласованных документах Инструкции администратора и Руководстве по обеспечению непрерывности описан порядок работы с УЗ root. | В согласованных документах Инструкции администратора и Руководстве по обеспечению непрерывности описан порядок работы с УЗ root. | Не пройдено | Раздел 4.2.4 ИА, в РОН информация отсутствует  Критичность несоответствия: средняя |
|  | **На уровне прикладного ПО:**  Идентификация и аутентификация субъектов доступа при подключении по https осуществляется средствами ПО «R-Vision IRP» по доменным персонифицированным УЗ.  Реализован механизм единого входа – SSO (single sign-on), основанный на доменной аутентификации.  Требования к сложности, длине паролей, сроку действия соответствуют требованиям, установленным Стандартом Компании «Политики информационной безопасности ПАО «НК «Роснефть» и Обществ Группы» № ПЗ-11.01 С-0054 версия 1.00, введенным в действие 28.03.2017 г.  Требования к сложности, длине пароля, сроку действия определяется групповыми политиками Active Directory Компании (домен Rosneft.ru). |  | Выполнить подключение по HTTPS к веб-интерфейсу ППО любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор СОРИБ.  В интерфейсе ППО «R-Vision» перейти в раздел «Настройки > Пользователи Системы > Домены (LDAP)».  Убедиться, что указан домен rosneft.ru.  Убедиться, что активирован механизм SSO. | Указан домен rosneft.ru.  Активирован механизм SSO. | Не пройдено | Испытания проводились на Сервер приложений и СУБД(основной сервер) sib-cdc-irp-s1.rosneft.ru (10.192.91.101).  Под УЗ iyukuznetsov\_adm\_cdc с ролью Администратор СОРИБ  Происходит запрос пароля при логине.  Не активирован механизм SSO  В настройках ППО отсутствуют настройки SSO  Файл 1.2.1, 1.2.1.2  Критичность несоответствия: высокая |
|  | В интерфейсе ППО «R-Vision» перейти в раздел «Настройки > Пользователи Системы > Пользователи».  Зафиксировать перечень УЗ.  Убедиться, что в перечне отсутствуют УЗ, не описанные в ПЭД. | В ППО «R-Vision» отсутствуют УЗ, не описанные в ПЭД. | Не пройдено | Испытания проводились на Сервер приложений и СУБД(основной сервер) sib-cdc-irp-s1.rosneft.ru (10.192.91.101).  Под УЗ iyukuznetsov\_adm\_cdc с ролью Администратор СОРИБ  Присутствуют следующие УЗ не описанные в ПЭД:  a\_bodunov\_adm\_cdc  RYTursunbaev  agyutanov  Файлы 1.2.2.1-1.2.2.3  Критичность несоответствия: высокая |
|  | **На уровне СУБД Postgres PRO:**  Идентификация и аутентификация привилегированных пользователей при подключении к СУБД осуществляется штатными средствами СУБД по доменным персонифицированным УЗ.  Требования к сложности, длине паролей, сроку действия соответствуют требованиям, установленным Стандартом Компании «Политики информационной безопасности ПАО «НК «Роснефть» и Обществ Группы» № П3-11.01 С-0054 версия 1.00, введенным в действие 28.03.2017. |  | Выполнить подключение по SSH к любому серверу приложений и СУБД любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  С помощью команды cat открыть конфигурационный файл pg\_hda.conf. Убедиться, что указан метод аутентификации в соответствии с проектно-эксплуатационной документацией. | В конфигурационном файле pg\_hda.conf, указан метод аутентификации в соответствии с проектно-эксплуатационной документацией. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ aiurentsev\_adm\_cdc с ролью «Системный администратор»  В проектно-эксплуатационной документации не описан метод аутентификации  Файлы:  1.3.1  Критичность несоответствия: высокая |
|  | Выполнить подключение по SSH к любому серверу приложений и СУБД любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор СУБД.  Подключиться к терминалу СУБД от имени доменной УЗ с ролью Администратор СУБД с помощью команды:  psql –d rvision  или от имени локальной административной УЗ с помощью команды:  psql -U rvision -d rvision -h localhost –W и ввести пароль УЗ rvision.  В терминале СУБД выполнить команды:  select \* from pg\_user;  select \* from pg\_roles;  \du  Убедиться, что отсутствуют УЗ, не описанные в ПЭД. | В результате выполнения команд в перечне УЗ отсутствуют УЗ, не описанные в ПЭД. | Не пройдено | Проверка проводилась на сервере sib-cdc-irp-s1 из под УЗ aamyagkikh\_adm\_cdc с ролью Администратора СУБД. Доступ к СУБД из под доменной УЗ отсутствует. Доступ к СУБД осуществлялся из под локальной УЗ rvision  Файл 1.3.2.1  В СУБД присутствуют неописанные УЗ(postgres).  Критичность несоответствия: высокая. |
|  | **Специальными средствами:**  Доступ привилегированных пользователей к Системе осуществляется только через СКДПП ЦОД.  Доступ непривилегированных пользователей осуществляется с использованием ПКЗИ-КТ. |  | На типовом АРМ привилегированного (или непривилегированного) пользователя проверить наличие ПКЗИ. Убедится, что доступ к ресурсам Системы или любому из ее серверов с отключенным ПКЗИ невозможен. Включить ПКЗИ и подключиться к Системе.  Убедиться, что с включенным ПКЗИ доступ к ресурсам Системы предоставлен. | Доступ к Системе с отключенным ПКЗИ невозможен.  Доступ к Системе с включенным ПКЗИ возможен | Пройдено | Испытания проводились с рабочей ВМ Admin в vmWare Horizon  Файлы  1.4.1.1, 1.4.2.1 |
|  | На типовом АРМ привилегированного пользователя от имени привилегированной УЗ осуществить попытку доступа к ресурсам Системы или любому из ее серверов с применением СКДПП ЦОД, затем без применения СКДПП ЦОД | Удалось осуществить попытку доступа к Системе с применением СКДПП ЦОД  Не удалось осуществить попытку доступа к Системе без применения СКДПП ЦОД | Пройдено | Испытания проводились с рабочей ВМ Admin в vmWare Horizon  Файлы  1.4.2.1, 1.4.2.2 |
|  | **ПУД.2 Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ** | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6:**  Параметры, определенные в следующих пунктах профиля ИБ для ОС Astra Linux 1.6 SE «Смоленск», способствуют частичному выполнению требования: 17; 18; 21; 22; 23; 24, 25.  Идентификация терминалов, ЭВМ и узлов сети осуществляется по IP-адресам и именам DNS встроенными средствами ОС Astra Linux. |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  С помощью команды sudo netstat –n получить информацию о состоянии сетевых соединений с сервером. Убедиться, что отображаются подключения с указанием IP-адреса или DNS-имени хоста. | В результате выполнения команды отображаются подключения с указанием IP-адреса или DNS-имени хоста. | Пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Файлы:  2.1.1.1-2.1.1.6 |
|  | **На уровне СУБД Postgres PRO:**  Идентификация терминалов, ЭВМ и узлов сети осуществляется по IP-адресам и именам DNS встроенными средствами СУБД. |  | Выполнить подключение по SSH к любому серверу приложений и СУБД любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор ИБ.  С помощью команды cat открыть журнал /var/lib/pgsql/12/data/log/Postgresql.log  Убедиться, что в журнале присутствуют события подключения к СУБД, для каждого события подключения указаны DNS-имя или IP-адрес хоста. | В журнале присутствуют события подключения к СУБД, для каждого события подключения указаны DNS-имя или IP-адрес хоста. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s2 под УЗ savolkov6\_adm\_cdc с ролью Администратор ИБ  Файлы:  2.2.1.1  DNS-имя или IP-адрес хоста отсутствуют  Уровень критичности: высокий |
|  | **Специальными средствами:**  **На уровне ОС Astra Linux SE 1.6:**  Идентификация ЭВМ осуществляется по IP-адресам средствами МЭ Check Point. |  | Экспертами провести проверку правил МЭ непосредственным анализом правил МЭ в интерфейсе его управления. Сверить полученные данные с таблицей правил МЭ согласованного ТПр в части межсетевого взаимодействия. Доступ к информационной системе терминируется на МЭ FW-CloudDC-DH2-Main | На момент проверки расхождений между правилами на МЭ и задокументированными в согласованном ТПр правилами не выявлено | Не пройдено | На межсетевых экранах имеются избыточные правила доступа.  Приложение:  Протокол МЭ IID-1154 07.10.2022.docx  Критичность несоответствия: высокая |
|  | **ПУД.3 Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам** | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6:**  Параметры, определенные в следующих пунктах профиля ИБ для ОС Astra Linux 1.6 SE «Смоленск», способствуют частичному выполнению требования: 17; 18; 21; 22; 23; 24, 25.  Идентификация программ, томов, каталогов, файлов, по именам осуществляется штатными средствами ОС. |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команду: sudo lsblk –f  Убедиться, что в результате отобразилась текущая разметка диска с указанием имен разделов и их границ. | В результате выполнения команды отобразилась текущая разметка диска с указанием имен разделов и их границ. | Пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Не блочное устройство.  Файлы:  3.1.1.1 |
|  | Выполнить команду: ls -al /  Убедиться, что в результате отобразились имена каталогов и файлов с указанием их размера, прав доступа и даты изменения. | В результате выполнения команды отобразились имена каталогов и файлов с указанием их размера, прав доступа и даты изменения. | Пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Файлы:  3.1.2.1 |
|  | Выполнить команду:  ps –aux (или *ps -eo pid,stime,uid,gid,cmd | tail -30*)  Убедиться, что в результате отобразились имена исполняемых программ, пути их расположения, владельцы процесса, время запуска. | В результате выполнения команды отобразились имена исполняемых программ, пути их расположения, владельцы процесса, время запуска. | Пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  Файлы:  3.1.3.1 |
|  | **На уровне прикладного ПО:**  Объекты ПО идентифицируются по нескольким параметрам. |  | Выполнить подключение по HTTPS к веб-интерфейсу ППО любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор СОРИБ.  Перейти в раздел «Инциденты» или «Уязвимости». Зафиксировать перечень объектов ППО.  Убедиться, что объекты ППО идентифицируются по нескольким параметрам, таким как: Дата, Тип, Категория, Статус, Описание, Ответственный. | Объекты ППО идентифицируются по нескольким параметрам, таким как: Дата, Тип, Категория, Статус, Описание, Ответственный. | Пройдено | Испытания проводились на Сервер приложений и СУБД(основной сервер) sib-cdc-irp-s1.rosneft.ru (10.192.91.101).  Под УЗ iyukuznetsov\_adm\_cdc с ролью Администратор СОРИБ  Файл 3.2.1 |
|  | **ПУД.4 Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа** | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6:**  Параметры, определенные в следующих пунктах профиля ИБ для ОС Astra Linux 1.6 SE «Смоленск», способствуют частичному выполнению требования: 17; 18; 21; 22; 23; 24, 25  Контроль доступа субъектов к защищаемым ресурсам осуществляется с использованием идентификаторов субъектов и групп, имеющих доступ к защищаемым ресурсам (чтение, запись, исполнение), списков контроля доступа (ACL) и механизмами системных привилегий ОС семейства Linux.  Матрица доступа субъектов к защищаемым объектам приведена в Таблица 17. |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команду: getfacl <объект безопасности по выбору эксперта>  Убедиться, что субъектам безопасности назначены права на объекты безопасности в соответствии с матрицей доступа, описанной в ТПр.  Убедиться, что в результате выполнения команды присутствует параметр default.  Проанализировать минимум три объекта безопасности. | Субъектам безопасности назначены права на объекты безопасности в соответствии с матрицей доступа, описанной в ТПр. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1.rosneft.ru под УЗ aiurentsev\_adm\_cdc с ролью «Системный администратор»  В матрице доступа ТПр описаны не все объекты доступа  Журналы /var/log/audit/audit.log и /var/lib/pgsql/12/data/log/Postgresql.log не найдены  Файлы:  4.1.1.1  Критичность несоответствия: высокая |
|  | **На уровне прикладного ПО:**  Контроль доступа субъектов осуществляется штатными средствами ПО «R-Vision IRP».  Матрица доступа субъектов к защищаемым объектам приведена в разделе 7.3.7. |  | Выполнить подключение по HTTPS к веб-интерфейсу ППО любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор СОРИБ.  Перейти в раздел «Настройки > Роли пользователей». Зафиксировать перечень ролей. Убедиться, что отсутствуют роли, не описанные в ПЭД. Убедиться, что все роли имеют полномочия в соответствии с матрицей доступа (табл. 18 ТПр).  Перейти в раздел «Настройки > Пользователи системы». Зафиксировать перечень ролей и УЗ. Убедиться, что всем привилегированным УЗ присвоены роли в соответствии с ПЭД. | Отсутствуют роли, не описанные в ПЭД. Роли обладают полномочиями в соответствии с матрицей доступа (табл. 18 ТПр)  Всем привилегированным УЗ присвоены роли в соответствии с ПЭД. | Не пройдено | Испытания проводились на Сервер приложений и СУБД(основной сервер) sib-cdc-irp-s1.rosneft.ru (10.192.91.101).  Под УЗ iyukuznetsov\_adm\_cdc с ролью Администратор СОРИБ  Отсутствует описание «Полномочия ролей на доступ к веб-консоли ПО «R-vision»» функциональных блоков «Индикаторы», «дашборды». Так же у следующих ролей настроены полномочия не в соответствии с ПЭД:  Аналитик ИБ SOC  Файл 4.2.1.1-4.2.1.69  Критичность несоответствия: высокая |
|  | Выполнить подключение по SSH к любому серверу приложений и СУБД любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор СУБД.  Подключиться к терминалу СУБД от имени доменной УЗ с ролью Администратор СУБД с помощью команды:  psql –d rvision  или от имени локальной административной УЗ с помощью команды:  psql -U rvision -d rvision -h localhost –W и ввести пароль УЗ rvision.  В терминале СУБД выполнить команды:  select \* from users;  select \* from roles;  select \* from users\_roles;  \du  Убедиться, что отсутствуют роли и УЗ, не описанные в ПЭД. | В результате выполнения команд в перечне УЗ ППО отсутствуют УЗ, не описанные в ПЭД. | Не пройдено | Проверка проводилась на сервере sib-cdc-irp-s1 из под УЗ aamyagkikh\_adm\_cdc с ролью Администратора СУБД. Доступ к СУБД осуществлялся из под локальной УЗ rvision  Файлы 1.3.2.1, 4.2.2.1.  В СУБД присутствуют неописанные роли.  Критичность несоответствия: высокая |
|  | **На уровне СУБД Postgres PRO:**  Контроль доступа субъектов осуществляется штатными средствами СУБД.  Матрица доступа субъектов к защищаемым объектам приведена в разделе 7.3.7. | 1 | Выполнить подключение по SSH к любому серверу приложений и СУБД любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор СУБД.  Получить перечень баз данных с помощью команды: psql –l  Подключиться к терминалу СУБД от имени доменной УЗ с ролью Администратор СУБД с помощью команды:  psql –d rvision  или от имени локальной административной УЗ с помощью команды:  psql -U rvision -d rvision -h localhost –W и ввести пароль УЗ rvision.  В терминале СУБД выполнить команды:  select \* from pg\_roles ‑ вывести информацию об объектах безопасности, а также информацию об ограничениях на доступ субъектов безопасности к объектам безопасности.  Убедиться, что параметр rolecanlogin имеет значение true для пользователей и сервисных УЗ в соответствии с матрицей доступа, описанной в ТПр. | Параметр rolecanlogin имеет значение true для пользователей и сервисных УЗ в соответствии с матрицей доступа в ТПр. | Не пройдено | Проверка проводилась на сервере sib-cdc-irp-s1 из под УЗ aamyagkikh\_adm\_cdc с ролью Администратора СУБД. Доступ к СУБД осуществлялся из под локальной УЗ rvision  Файлы 1.3.2.1, 4.2.2.1.  В СУБД присутствуют неописанные роли.  Критичность несоответствия: высокая |
| **ПОДСИСТЕМА РЕГИСТРАЦИИ И УЧЕТА** | | | | | | |
|  | **ПРУ.1 Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:**   1. **Дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы.** 2. **Результат попытки входа: успешная или неуспешная – несанкционированная.**   **Идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа** | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6:**  Параметры, определенные в следующих пунктах профиля ИБ для ОС Astra Linux 1.6 SE «Смоленск», способствуют выполнению требования: 31.  Регистрация событий входа (выхода) в сеанс ОС (из сеанса ОС) осуществляется встроенными средствами регистрации событий ОС в журнале /var/log/auth.log  В параметрах регистрации указываются:  1. Дата и время входа (выхода) субъекта;  2. Имя учетной записи субъекта;  3. Результат попытки входа (успешная или неуспешная).  События в журналах хранятся не менее 90, с последующим архивированием событий в СРК ЦОД с помощью агента и хранением не менее 1 года.  Процедура создания архивов журналов событий описана в Инструкции администратора. |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор ИБ.  Осуществить попытку подключения к выбранному серверу с помощью заведомо некорректного пароля. Убедиться, что появилось сообщение об ошибке подключения.  Отключиться и повторить подключение к выбранному серверу с корректными учетными данными.  Открыть журнал /var/log/auth.log с помощью команды:  cat /var/log/auth.log | grep <УЗ Администратора ИБ>  Убедиться, что в журнале зафиксированы события успешного подключения, неуспешного подключения с некорректным паролем, событие выхода.  В параметрах регистрации каждого события содержится:   1. Дата и время входа (выхода) субъекта; 2. Имя учетной записи субъекта**\***; 3. Результат попытки входа (успешная или неуспешная).   **\****Имя УЗ может отображаться в виде идентификатора пользователя (UID). Чтобы идентифицировать пользователя по имени УЗ, необходимо выполнить команду: sudo getent passwd UID.* | В журнале /var/log/auth.log зафиксированы события успешного подключения, неуспешного подключения с некорректным паролем, событие выхода.  В параметрах регистрации каждого события содержится:   1. Дата и время входа (выхода) субъекта; 2. Имя учетной записи субъекта; 3. Результат попытки входа (успешная или неуспешная). | Пройдено | Испытания проводились на сервере sib-cdc-irp-s2 под УЗ savolkov6\_adm\_cdc с ролью Администратор ИБ  Файлы:  5.1.1.1 |
|  | Убедиться, что в журнале /var/log/auth.log содержатся события за последние 90 дней с момента проведения проверки.[[1]](#footnote-1) | В журнале /var/log/auth.log содержатся события за последние 90 дней с момента проведения проверки. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s2 под УЗ savolkov6\_adm\_cdc с ролью Администратор ИБ  Файлы:  5.1.2.1  События хранятся менее 90 дней  Уровень критичности: высокий |
|  | С помощью команды cat открыть файл /etc/logrotate.d/rsyslog.  Убедиться, что параметры автоматического архивирования журналов /var/log/auth.log и /var/log/audit/audit.log ОС соответствуют указанным в проектно-эксплуатационной документации. | Параметры автоматического архивирования журналов /var/log/auth.log и /var/log/audit/audit.log ОС соответствуют указанным в проектно-эксплуатационной документации. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s2 под УЗ savolkov6\_adm\_cdc с ролью Администратор ИБ  Файлы:  5.1.3.1  Для журнала /var/log/auth.log параметры не соответствуют указанным в ПЭД.  Согласно ИА должна осуществляться ротация журналов /var/log/secure,  /var/log/audit/audit.log при помощи утилиты logrotate, настройки для данных журналов отсутствуют.  Уровень критичности: высокий |
|  | Командой cd перейти в каталог /etc/cron.daily и убедиться в наличие задания logrotate.[[2]](#footnote-2) | В планировщике заданий cron присутствует задание logrotate. | Пройдено | Испытания проводились на сервере sib-cdc-irp-s2 под УЗ savolkov6\_adm\_cdc с ролью Администратор ИБ  Файлы:  5.1.4.1 – 5.1.4.2 |
|  | Проверка проводится с участием Администратора СРК ЦОД.  Запросить у Администратора СРК ЦОД список действующих заданий резервного копирования в ИС. Убедиться, что перечень заданий и объектов резервного копирования соответствует РОН.  Убедиться, что перечень серверов в СРК соответствует перечню серверов ИС, описанному в ПЭД.  Убедиться, что в задании резервного копирования журналов событий ОС с серверов Системы указан срок хранения архивов журналов не менее 1 года.  Проверить журналы СРК ЦОД на наличие успешно завершенных заданий на резервное копирование журналов серверов ИС.[[3]](#footnote-3) | Перечень заданий и объектов резервного копирования соответствует РОН.  Перечень серверов в СРК соответствует перечню серверов ИС, описанному в ПЭД.  Для задания резервного копирования журналов событий ОС с серверов Системы указан срок хранения архивов журналов не менее 1 года.  Имеются успешно завершенные задания на резервное копирование журналов событий ОС с серверов Системы | Не пройдено | Папка: РК  РК журнала /var/log/auth.log не задано,  срок хранения архивов журналов не менее 1 года не задан.  Критичность несоответствия: высокая |
|  | Убедиться, что в согласованном документе Инструкция администратора описана процедура создания архивов журналов событий ОС.[[4]](#footnote-4) | В Инструкции администратора описана процедура создания архивов журналов событий ОС.  Документ согласован. | Пройдено | Раздел 4.2.5 ИА |
|  | **На уровне прикладного ПО**:  Регистрация событий осуществляется штатными средствами ПО «R-Vision IRP».  Для каждого из событий регистрируется следующая информация:   1. Дата и время входа; 2. Идентификатор УЗ; 3. Результат запуска (успешный, неуспешный).   Журнал событий доступен через web-интерфейс ПО R-Vision IRP в разделе «Настройки» - «Журнал». |  | Выполнить подключение по WEB к ПО «R-Vision IRP» согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор ИБ.  В интерфейсе ПО перейти в раздел «Настройки» - «Журнал», открыть журнал событий.  Убедиться, что в журнале содержатся события, для каждого из которых регистрируется следующая информация:   1. Дата и время входа; 2. Идентификатор УЗ; 3. Результат запуска (успешный, неуспешный). | В журнале ПО «R-Vision IRP» содержатся события, для каждого из которых регистрируется следующая информация:   1. Дата и время входа; 2. Идентификатор УЗ; 3. Результат запуска (успешный, неуспешный). | Пройдено | Испытания проводились на сервере sib-cdc-irp-s2 под УЗ savolkov6\_adm\_cdc с ролью Администратор ИБ  Файлы:  5.2.1.1  В журнале зафиксированы события успешного и неуспешного входа под УЗ аудитора, а также выхода |
|  | **На уровне СУБД Postgres PRO:**  Регистрация событий входа (выхода) осуществляется встроенными средствами регистрации событий СУБД в журнале /var/lib/pgsql/12/data/log/ Postgresql.log  В параметрах регистрации указываются:   1. Дата и время входа (выхода) субъекта; 2. Имя учетной записи субъекта; 3. Результат попытки входа (успешная или неуспешная).   События в журналах хранятся не менее 90, с последующим архивированием событий в СРК ЦОД с помощью агента и хранением не менее 1 года.  Процедура создания архивов журналов событий описана в Инструкции администратора |  | Выполнить подключение по SSH к любому серверу приложений и СУБД любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор ИБ.  С помощью команды cat открыть журнал /var/lib/pgsql/12/data/log/Postgresql.log  Убедиться, что в журнале СУБД postgresql.log содержатся события входа (выхода), для каждого из которых в параметрах регистрации указана следующая информация:   1. Дата и время входа (выхода) субъекта; 2. Имя учетной записи субъекта; 3. Результат попытки входа (успешная или неуспешная). | В журнале СУБД postgresql.log содержатся события входа (выхода), для каждого из которых в параметрах регистрации указана следующая информация:   1. Дата и время входа (выхода) субъекта; 2. Имя учетной записи субъекта; 3. Результат попытки входа (успешная или неуспешная). | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1 под УЗ shkhkhayrull\_adm\_cdc с ролью Администратор ИБ  Нет доступа до журнала Postgresql.log  Файл 5.3.1  Критичность несоответствия: высокая |
|  | Убедиться, что в журнале СУБД /var/lib/pgsql/12/data/log/Postgresql.log содержатся события за последние 90 дней с момента провед | В журнале СУБД /var/lib/pgsql/12/data/log/Postgresql.log содержатся события за последние 90 дней с момента проведения проверки. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1 под УЗ shkhkhayrull\_adm\_cdc с ролью Администратор ИБ  Нет доступа до журнала Postgresql.log  Файл 5.3.1  Критичность несоответствия: высокая |
|  | Проверка проводится с участием Администратора СРК ЦОД.  Запросить у Администратора СРК ЦОД список действующих заданий резервного копирования в ИС.  Убедиться в наличии заданий резервного копирования журналов событий СУБД с серверов Системы.  Убедиться, что перечень серверов в СРК соответствует перечню серверов ИС, описанному в ПЭД.  Убедиться, что в задании резервного копирования журналов событий СУБД с серверов Системы указан срок хранения архивов журналов не менее 1 года.  Проверить журналы СРК ЦОД на наличие успешно завершенных заданий на резервное копирование журналов серверов ИС | В СРК ЦОД созданы заданий резервного копирования журналов событий СУБД с серверов Системы.  Перечень серверов в СРК соответствует перечню серверов ИС, описанному в ПЭД.  Для задания резервного копирования журналов событий СУБД с серверов Системы указан срок хранения архивов журналов не менее 1 года.  Имеются успешно завершенные задания на резервное копирование журналов событий СУБД с серверов Системы | Не пройдено | Папка: РК  Заданий РК журналов СУБД нет,  срок хранения архивов журналов не менее 1 года не задан.  Критичность несоответствия: высокая |
|  | Убедиться, что в согласованном документе Инструкция администратора описана процедура создания архивов журналов событий СУБД.[[5]](#footnote-5) | В Инструкции администратора описана процедура создания архивов журналов событий СУБД.  Документ согласован. | Не пройдено | В ИА не описана процедура создания архивов журналов событий СУБД.  Критичность несоответствия: высокая |
|  | **Специальными средствами:**  **На уровнях ОС Astra Linux SE 1.6, прикладного ПО:**  Дополнительно осуществляется регистрация действий привилегированных пользователей Системы средствами СКДПП ЦОД.  Дополнительно настроена передача событий в СМСИБ ЦОД на уровне ОС Astra Linux SE 1.6. |  | Запросить у Аналитика ИБ СКДПП ЦОД подтверждение регистрации действий привилегированных пользователей на уровне ОС Astra Linux SE 1.6 в консоли СКДПП ЦОД.  Убедиться в регистрации действий трех привилегированных пользователей с различными ролями в Системе.[[6]](#footnote-6) | В журнале СКДПП ЦОД присутствуют события с действиями привилегированных пользователей на уровне ОС Astra Linux SE 1.6. | Пройдено | Папка: СКДПП |
|  | Запросить у Аналитика ИБ СКДПП ЦОД подтверждение регистрации действий привилегированных пользователей на уровне ППО «R-Vision IRP» в консоли СКДПП ЦОД.  Убедиться в регистрации действий трех привилегированных пользователей с различными ролями в Системе.[[7]](#footnote-7) | В журнале СКДПП ЦОД присутствуют события с действиями привилегированных пользователей ППО «R-Vision IRP». | Пройдено | Папка: СКДПП |
|  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команду:  cat /etc/rsyslog.d/remote.conf  Убедиться, что в файле remote.conf указаны IP-адреса СМСИБ и журналы ОС, необходимые для отправки событий входа (выхода), запуска (завершения) программ и процессов, попыток доступа на изменение к защищаемым томам, каталогам, файлам сервера:  /var/log/auth.log;  /var/log/audit/audit.log | В файле remote.conf указаны IP-адреса СМСИБ и журналы ОС, необходимые для отправки событий входа (выхода) сервера:  /var/log/auth.log;  /var/log/audit/audit.log | Не пройдено | Испытания проводились на сервере sib-cdc-irp-cl2.rosneft.ru под УЗ aiurentsev\_adm\_cdc с ролью «Системный администратор»  Правила отправки событий содержатся в файлах:  /etc/rsyslog.conf  /etc/rsyslog.d/10-siem.conf  Не настроена отправка журнала /var/log/audit/audit.log  Файлы:  5.4.3.1  Критичность несоответствия: высокая |
|  | Проверка проводится с участием администратора СМСИБ под его УЗ в консоли СМСИБ.  Открыть консоль СМСИБ и убедиться, что в СМСИБ присутствуют записи событий входа (выхода), запуска (завершения) программ и процессов, попыток доступа на изменение к защищаемым томам, каталогам, файлам из журналов ОС.[[8]](#footnote-8) | В СМСИБ присутствуют записи событий входа (выхода), запуска (завершения) программ и процессов, попыток доступа на изменение к защищаемым томам, каталогам, файлам из журналов ОС. | Не пройдено | Событий в СМСИБ от ИС нет.  Файл: RE оценка 1154  Критичность несоответствия: высокая |
|  | **ПРУ.2 Должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются:**   1. **Дата и время выдачи (обращения к подсистеме вывода).** 2. **Спецификация устройства выдачи [логическое имя (номер) внешнего устройства].** 3. **Краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа.**   **Идентификатор субъекта доступа, запросившего документ** | | | | | |
|  | Выдача печатных (графических) документов на «твердую» копию средствами Системы не предусмотрена.  Требования о соблюдении Стандарта Компании «Охрана сведений конфиденциального характера» и запрете печати из Системы любым способом, отличным от печати экспортируемых из Системы файлов, добавлена в Инструкцию пользователя СОРИБ. | 1 | Убедиться, что в согласованном документе ИА в явном виде существует запрет на распечатывание любым способом, отличным от печати выгруженного файла и присутствует ссылка на ОСКХ. | В документе Инструкция администратора в явном виде существует запрет на распечатывание любым способом, отличным от печати выгруженного файла и присутствует ссылка на ОСКХ.  Документ согласован. | Пройдено | Раздел 3.3 ИА |
|  | **ПРУ.3 Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:**   1. **Дата и время запуска;** 2. **Имя (идентификатор) программы (процесса, задания);** 3. **Идентификатор субъекта доступа, запросившего программу (процесс, задание);** 4. **Результат запуска (успешный, неуспешный - несанкционированный)** | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6:**  Параметры, определенные в следующем пункте профиля ИБ для ОС Astra Linux 1.6 SE «Смоленск», способствуют выполнению требования: 31.  Регистрация событий запуска (завершения) программ и процессов осуществляется штатными средствами ОС auditd, файлы журналов /var/log/audit/audit.log.  В параметрах регистрации указываются:   1. Дата и время запуска/остановки процесса; 2. Имя (идентификатор) процесса; 3. Имя учетной записи субъекта (учетная запись пользователя, запустившего\завершившего процесс); 4. Результат запуска (успешный или неуспешный).   События в журналах хранятся не менее 90 дней, с последующим архивированием событий в СРК ЦОД с помощью агента и хранением не менее 1 года.  Процедура создания архивов журналов событий описана в Инструкции администратора |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор ИБ.  Выполнить команды:  id -u – отобразить UID текущей УЗ  sudo ausearch -ui <UID> -r | sudo aureport -f -i – отобразить события запуска (завершения процессов) в журнале audit/audit.log  Убедиться, что в журнале /var/log/audit/audit.log зафиксированы события запуска (завершения) программ и процессов, для каждого из которых в параметрах регистрации указана следующая информация:   1. Дата и время запуска/остановки процесса; 2. Имя (идентификатор) процесса; 3. Имя учетной записи субъекта (учетная запись пользователя, запустившего\завершившего процесс); 4. Результат запуска (успешный или неуспешный). | В журнале /var/log/audit/audit.log зафиксированы события запуска (завершения) программ и процессов, для каждого из которых в параметрах регистрации указана следующая информация:   1. Дата и время запуска/остановки процесса; 2. Имя (идентификатор) процесса; 3. Имя учетной записи субъекта (учетная запись пользователя, запустившего\завершившего процесс); 4. Результат запуска (успешный или неуспешный). | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s2 под УЗ shkhkhayrull\_adm\_cdc с ролью Администратор ИБ  Нет доступа.  Файл 7.1.1  Критичность несоответствия: высокая |
|  | Убедиться, что в журнале /var/log/audit/audit.log содержатся события за последние 90 дней с момента проведения проверки. | В журнале /var/log/audit/audit.log содержатся события за последние 90 дней с момента проведения проверки. | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s2 под УЗ shkhkhayrull\_adm\_cdc с ролью Администратор ИБ  Нет доступа.  Файл 7.1.1  Критичность несоответствия: высокая |
|  | **На уровне прикладного ПО:**  Осуществляется регистрация действий пользователей и автоматических действий системы (согласно настроенного расписания). Осуществляется регистрация завершения задач на интеграцию с внешними системами.  Регистрация событий запуска (завершения) программ и процессов осуществляется штатными средствами ППО.  В параметрах регистрации указываются:   1. Дата и время запуска; 2. Имя (идентификатор) программы (процесса, задания); 3. Идентификатор субъекта доступа, запросившего программу (процесс, задание); 4. Результат запуска (успешный, неуспешный - несанкционированный). |  | Выполнить подключение по WEB к ПО «R-Vision IRP» согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор ИБ.  В интерфейсе ПО перейти в раздел «Настройки», открыть журнал событий.  Убедиться, что в журнале содержатся события запуска (завершения) программ и процессов, для каждого из которых в параметрах регистрации указана следующая информация:   1. Дата и время запуска; 2. Имя (идентификатор) программы (процесса, задания); 3. Идентификатор субъекта доступа, запросившего программу (процесс, задание); 4. Результат запуска (успешный, неуспешный - несанкционированный). | В журнале ПО «R-Vision IRP» содержатся события запуска (завершения) программ и процессов, для каждого из которых в параметрах регистрации указана следующая информация:   1. Дата и время запуска; 2. Имя (идентификатор) программы (процесса, задания); 3. Идентификатор субъекта доступа, запросившего программу (процесс, задание); 4. Результат запуска (успешный, неуспешный - несанкционированный). | Пройдено | Испытания проводились на сервере sib-cdc-irp-s1 под УЗ shkhkhayrull\_adm\_cdc с ролью Администратор ИБ  Файл 7.2.1 |
|  | **ПРУ.4 Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:**   1. **Дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная.** 2. **Идентификатор субъекта доступа.**   **Спецификация защищаемого объекта [логическое имя (номер)]** | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6:**  Параметры, определенные в следующем пункте профиля ИБ для ОС Astra Linux 1.6 SE «Смоленск», способствуют выполнению требования: 31.  Регистрация попыток доступа на изменение к защищаемым томам, каталогам, файлам осуществляется штатными средствами ОС auditd, файлы журналов /var/log/audit/audit.log  Журнал событий включает:   1. Дата и время доступа к защищаемому объекту; 2. Результат попытки доступа: успешная или неуспешная; 3. Идентификатор субъекта доступа (имя учетной записи); 4. Спецификация защищаемого объекта (путь в файловой системе к защищаемому объекту).   События в журналах хранятся не менее 90 дней, с последующим архивированием событий в СРК ЦОД с помощью агента и хранением не менее 1 года.  Процедура создания архивов журналов событий описана в Инструкции администратора |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор ИБ.  Выполнить команду: sudo getfaud <объект безопасности по выбору экспертов>.  Убедиться, что на выбранный объект безопасности настроен аудит доступа.  С помощью команды cat открыть выбранный объект безопасности.  Выполнить команду:  sudo ausearch -f <защищаемый объект> | sudo aureport -f -i – отобразить события пыток доступа на изменение к защищаемым объектам.  Зафиксировать результат.Убедиться, что в отображенном журнале зарегистрированы события доступа к выбранному объекту безопасности, для каждого из которых в параметрах регистрации указана следующая информация:   1. Дата и время доступа к защищаемому объекту; 2. Результат попытки доступа: успешная или неуспешная; 3. Идентификатор субъекта доступа (имя учетной записи); 4. Спецификация защищаемого объекта (путь в файловой системе к защищаемому объекту). | В журнале /var/log/audit/audit.log зарегистрированы события доступа к выбранному объекту безопасности, для каждого из которых в параметрах регистрации указана следующая информация:   1. Дата и время доступа к защищаемому объекту; 2. Результат попытки доступа: успешная или неуспешная; 3. Идентификатор субъекта доступа (имя учетной записи); 4. Спецификация защищаемого объекта (путь в файловой системе к защищаемому объекту). | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s2 под УЗ shkhkhayrull\_adm\_cdc с ролью Администратор ИБ  Нет доступа.  Файл 7.1.1  Критичность несоответствия: высокая |
|  | **На уровне прикладного ПО:**  Регистрация IP-адресов ЭВМ и терминалов осуществляется штатными средствами ППО.  В параметрах регистрации указываются:   1. дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная; 2. идентификатор субъекта доступа; 3. спецификация защищаемого объекта [логическое имя (номер)]. |  | Выполнить подключение по WEB к ПО «R-Vision IRP» согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор ИБ.  В интерфейсе ПО перейти в раздел «Настройки», открыть журнал событий.  Убедиться, что в журнале содержатся события регистрации IP-адресов ЭВМ, для каждого из которых в параметрах регистрации указана следующая информация:   1. дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная; 2. идентификатор субъекта доступа; 3. спецификация защищаемого объекта [логическое имя (номер)]. | В журнале ПО «R-Vision IRP» содержатся события регистрации IP-адресов ЭВМ, для каждого из которых в параметрах регистрации указана следующая информация:   1. дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная; 2. идентификатор субъекта доступа; 3. спецификация защищаемого объекта [логическое имя (номер)]. | Пройдено | Испытания проводились на сервере sib-cdc-irp-s1 под УЗ shkhkhayrull\_adm\_cdc с ролью Администратор ИБ  Файл 8.2.1 |
|  | **ПРУ.5 Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов)** | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6:**  Параметры, определенные в следующем пункте профиля ИБ для ОС Astra Linux 1.6 SE «Смоленск», способствуют выполнению требования: 31  Очистка освобождаемых областей оперативной памяти осуществляется встроенными средствами сертифицированной ОС.  Настройки приведены в Инструкции администратора |  | Запросить у Руководителя проекта действующие сертификаты соответствия требованиям ИБ компонентов из состава ИС «СОРИБ» согласно Таблице 31 ТПр. | Все компоненты Системы согласно Таблице 31 ТПр имеют действующие сертификаты соответствия | Не пройдено | Не предоставлен сертификат на ПО R-Vision IRP  Файл: sertifikat-sootvetstviya-2557, certificate-3637-2022-07-28  Критичность несоответствия: высокая |
|  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  С помощью команды cat /etc/cron.daily/swap\_wipe убедиться, что настроена периодическая (ежедневно с помощью планировщика заданий cron) принудительная очистка PageCache, inode, dentrie, конфигурационный файл /etc/cron.daily/swap\_wipe имеет следующее содержание:  swap\_used=`free -m | grep Swap | awk '{print $3}'`  mem\_free=`free -m | grep Mem | awk '{print $4}'`  if [ $swap\_used -lt $mem\_free -a $swap\_used -gt 0 ]; then  swapoff -a; swapon -a  echo `date "+%x %T"`": Swap switched (Swap used/Mem free - $swap\_used/$mem\_free)"  else  echo `date "+%x %T"`": Switching swap is impossible or not needed (Swap used/Mem free - $swap\_used/$mem\_free)"  fi  \* Данная проверка проводится в случае использования swap. Убедиться в наличии/отсутствии swap можно с помощью команд:  swapon -s – отобразит путь до swap при его наличии  free -m – в строке Swap в столбце Total указан ненулевой размер при наличии сконфигурированного swap. | Настроена периодическая (ежедневно с помощью планировщика заданий cron) принудительная очистка PageCache, inode, dentrie, конфигурационный файл /etc/cron.daily/swap\_wipe имеет следующее содержание:  swap\_used=`free -m | grep Swap | awk '{print $3}'`  mem\_free=`free -m | grep Mem | awk '{print $4}'`  if [ $swap\_used -lt $mem\_free -a $swap\_used -gt 0 ]; then  swapoff -a; swapon -a  echo `date "+%x %T"`": Swap switched (Swap used/Mem free - $swap\_used/$mem\_free)"  else  echo `date "+%x %T"`": Switching swap is impossible or not needed (Swap used/Mem free - $swap\_used/$mem\_free)"  fi | Не пройдено | Испытания проводились на сервере sib-cdc-irp-s1 под УЗ takovalev\_adm\_cdc с ролью «Системный администратор»  конфигурационный файл /etc/cron.daily/swap\_wipe  не найден.  Файлы:  9.1.2.1  Критичность несоответствия: высокая |
|  | Убедиться, что в согласованном документе Инструкция администратора описана процедура настройки очистки освобождаемых областей оперативной памяти. | В документе Инструкция администратора описана процедура настройки очистки освобождаемых областей оперативной памяти.  Документ согласован. | Не пройдено | В ИА не описана процедура настройки очистки освобождаемых областей оперативной памяти.  Критичность несоответствия: средняя |
| **ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ** | | | | | | |
|  | **ПОЦ.1 Должен быть обеспечен контроль целостности программных средств СЗИ от НСД, а также неизменность программной среды.**  **При этом целостность СЗИ от НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ; целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации** | | | | | |
|  | **Специальными средствами:**  Контроль целостности средств защиты, входящих в состав прикладного ПО, а также неизменность программной среды осуществляется «специальными средствами» СКЗиКЦ ЦОД. Перечень контролируемых объектов, представлен в Приложении 3 ТПр. |  | Проверка проводится с участием администратора СКЗиКЦ ЦОД.  Подключиться к консоли управления СКЗиКЦ с правами администратора.  Убедиться, что в СКЗиКЦ созданы задания контроля целостности на серверах ИС СОРИБ.  Убедиться, что перечень серверов и объектов контроля целостности соответствует Приложению 3 ТПр.  Убедиться, что задан параметр периодичности данных заданий в соответствии с РОН.  Проверить журналы СКЗиКЦ на наличие успешно завершенных заданий контроля целостности на серверах ИС СОРИБ. | В СКЗиКЦ созданы задания контроля целостности на серверах ИС СОРИБ.  Перечень серверов и объектов контроля целостности соответствует Приложению 3 ТПр.  Параметры периодичности выполнения заданий контроля целостности соответствуют РОН.  Имеются успешно завершенные задания контроля целостности на серверах ИС СОРИБ. | Не пройдено | Испытания проводились в консоли RedCheck от имени УЗ aiurentsev\_adm\_cdc  Файлы  10.1.1.1 – 10.1.1.5  Отсутствуют выполненные задания КЦ на серверах ИС  Критичность несоответствия: высокая |
|  | Убедиться, что в Инструкции администратора описана процедура контроля целостности и порядок анализа отчетов контроля защищенности. | В Инструкции администратора описана процедура контроля целостности и порядок анализа отчетов контроля защищенности. | Пройдено | Раздел 6.1 ИА |
|  | **ПОЦ.2 Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время** | | | | | |
|  | **Специальными средствами:**  Осуществляется физическая охрана серверных помещений, мест расположения серверов, а также контроль доступа посторонних лиц в помещения с СВТ.  Помещения соответствуют требованиям безопасности Компании.  Во всех зданиях Компании используется система контроля и управления доступом. Ведется персонифицированный учет посетителей и видеонаблюдение.  Доступ в помещения нахождения серверов регламентируется внутренними распорядками Компании. |  | Проверить наличие в офисе по адресу г. Зеленоград, проезд 4803, дом 27, строение 2. оборудования, указанного в согласованном Техническом паспорте. Проверить оснащенность помещений системой контроля и управления доступом (СКУД), наличие охраны в офисе. | В офисе по указанному адресу серверы расположены в помещениях в соответствии с документацией. Помещения оснащены СКУД, в офисах есть охрана. | Пройдено | Папка: СВТ |
|  | Проверка проводится с участием Администратора ВИ ЦОД.  Выполнить подключение к vCenter ИС ВИ ЦОД с правами администратора. Проверить кластеры, к которым принадлежат серверы Системы, на предмет соответствия ТПр. | Все виртуальные серверы принадлежат соответствующим кластерам Системы и настройки сетевых интерфейсов серверов Системы заданы в соответствии с Техническим проектом. | Пройдено | Файл: 11.1.2, 11.1.2.1 |
|  | **ПОЦ.3 Должно проводиться периодическое тестирование функций СЗИ от НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД** | | | | | |
|  | **Специальными средствами:**  Периодическое тестирование функций СЗИ НСД при изменении программной среды и эксплуатирующего персонала Системы осуществляется с помощью корпоративных средств анализа защищенности и тест-программ, имитирующих попытки НСД СКЗиКЦ ЦОД. |  | Проверки проводятся с участием Администратора СКЗиКЦ.  Зайти в консоль управления СКЗиКЦ с правами администратора. Убедиться, что для данной Системы существует задание на сканирование в режиме «Аудит уязвимостей».  Убедиться, что периодичность выполнения задания соответствует согласованному РОН. | Для Системы существует задача на сканирование в режиме «Аудит уязвимостей». задание на сканирование включена в расписание периодического запуска сканирований. | Не пройдено | Испытания проводились в консоли RedCheck от имени УЗ aiurentsev\_adm\_cdc  Файлы  12.1.1.1, 12.1.1.2  Не настроен периодический запуск задания  Критичность несоответствия: высокая |
|  | Проверить журналы СКЗиКЦ на наличие успешно завершенных заданий на сканирование в режиме «Аудит уязвимостей» на серверах ИС.  Убедиться, что перечень серверов в задании соответствует списку серверов ИС, описанному в ПЭД. | Имеются успешно завершенные задания на сканирование в режиме «Аудит уязвимостей» на серверах ИС.  Перечень серверов в задании соответствует списку серверов ИС, описанному в ПЭД. | Не пройдено | Файлы  12.1.1.1, 12.1.2.1, 10.1.1.5, 12.1.2.2  Отсутствуют выполненные задания «Аудит уязвимостей» на серверах ИС  Критичность несоответствия: высокая |
|  | Зайти в консоль управления СКЗиКЦ с правами администратора. Убедиться, что для данной Системы существует задание на сканирование в режиме «Аудит обновлений».  Убедиться, что периодичность выполнения задания соответствует согласованному РОН. | Для Системы существует задача на сканирование в режиме «Аудит обновлений» задание на сканирование включена в расписание периодического запуска сканирований. | Не пройдено | Файлы  12.1.1.1, 12.1.3.1  Не настроен периодический запуск задания  Критичность несоответствия: высокая |
|  | Проверить журналы СКЗиКЦ на наличие успешно завершенных заданий на сканирование в режиме «Аудит обновлений» на серверах ИС.  Убедиться, что перечень серверов в задании соответствует списку серверов ИС, описанному в ПЭД. | Имеются успешно завершенные задания на сканирование в режиме «Аудит обновлений» на серверах ИС.  Перечень серверов в задании соответствует списку серверов ИС, описанному в ПЭД. | Не пройдено | Файлы  12.1.1.1, 12.1.4.1, 10.1.1.5, 12.1.4.2  Отсутствуют выполненные задания «Аудит уязвимостей» на серверах ИС  Критичность несоответствия: высокая |
|  | Открыть последний отчет по результатам задания «Аудит уязвимостей» и провести анализ на предмет наличия критических и высоких уязвимостей.  Убедиться, что в последнем отчете отсутствуют уязвимости со статусом «Критический» и «Высокий». | В последнем отчете отсутствуют уязвимости со статусом «Критический» и «Высокий» | Не пройдено | В отчете присутствуют высокие и критические уязвимости  Файл: SIB\_SORIB\_IID-1154\_Vuln-1  Критичность несоответствия: высокая |
|  | Открыть последний отчет по результатам задания «Аудит обновлений» и провести анализ на предмет наличия обновлений.  Убедиться, что в последнем отчете отсутствуют обновления со статусом «Критический» и «Высокий». | В последнем отчете отсутствуют обновления со статусом «Критический» и «Высокий» | Не пройдено | В отчете обновлений присутствуют статусы-критический и высокий  Файл: SIB\_SORIB\_IID-1154\_Upd-1  Критичность несоответствия: высокая |
|  | Убедиться, что в согласованном документе Инструкция администратора или Руководство по обеспечению непрерывности приведен порядок действий по обработке отчетов СКЗиКЦ. | В документе Инструкция администратора или Регламент по обеспечению непрерывности приведен порядок действий по обработке отчетов СКЗиКЦ.  Документ согласован. | Пройдено | Раздел 6.2 ИА |
|  | **ПОЦ.4 Должны быть в наличии средства восстановления СЗИ от НСД, предусматривающие ведение двух копий программных средств СЗИ от НСД и их периодическое обновление и контроль работоспособности** | | | | | |
|  | Восстановление механизмов СЗИ НСД программного обеспечения Системы осуществляется из дистрибутивов ПО. Системный администратор ведет две копии дистрибутивов и периодически осуществляет контроль их работоспособности в соответствии с Инструкцией администратора СОРИБ и Руководством по обеспечении непрерывности СОРИБ.  После установки и настройки компонентов ИС производится создание снэпшотов виртуальных серверов ИС средствами ВИ ЦОД с их дальнейшим резервным копированием средствами СРК ЦОД. Также, данная процедура производится при внесении изменений в конфигурацию серверов ИС.  На постоянной основе производится резервное копирование базы данных средствами СРК ЦОД в соответствии с Руководством по обеспечению непрерывности СОРИБ.  Контроль работоспособности резервных копий осуществляется периодическим тестовым восстановлением из резервных копий в соответствии с Инструкцией администратора и Руководством по обеспечению непрерывности. |  | Убедиться в наличии двух копий дистрибутивов ПО.  Убедиться, что в согласованных документах Инструкция администратора и Руководство по обеспечению непрерывности описан порядок контроля работоспособности дистрибутивов. | В документах Инструкция администратора и Руководство по обеспечению непрерывности описан порядок контроля работоспособности дистрибутивов.  Документы согласованы. | Не пройдено | В ИА и РОН не описан порядок контроля работоспособности дистрибутивов.  Не предоставлены дистрибутивы- СУБД, R-Vision IRP  Файл: RE IID-1154 Оценка соответствия - дистрибутивы ОС, kasper,  1154 ОСИБ\_Дистрибутивы ПО  Критичность несоответствия: высокая |
|  | Проверка проводится с участием Администратора ВИ ЦОД.  Выполнить подключение к vCenter ИС ВИ ЦОД с правами администратора.  Убедиться в наличии снэпшотов виртуальных серверов Системы. | В консоли vCenter ИС ВИ ЦОД содержатся снэпшоты виртуальных серверов Системы. | Не пройдено | Не предоставлено подтверждение выполненной задачи в ВИ ЦОД  Файл: RE IID-1154 IID-1155 Оценка соответствия  Критичность несоответствия: высокая |
|  | Проверка проводится с участием Администратора СРК ЦОД.  Выполнить подключение к консоли СРК ЦОД с правами администратора.  Убедиться в наличии резервных копий снэпшотов виртуальных серверов Системы. | В консоли СРК ЦОД содержатся резервные копии снэпшотов виртуальных серверов Системы. | Пройдено | Папка: РК |
|  | Проверка проводится с участием Администратора СРК ЦОД.  Выполнить подключение к консоли СРК ЦОД с правами администратора.  Проверить наличие двух последних резервных копий баз данных с серверов Системы.  Убедиться, что расписание периодичности резервного копирования баз данных соответствует РОН. | В наличии резервных копий баз данных с серверов Системы  Расписание периодичности резервного копирования баз данных соответствует РОН. | Не пройдено | Задачи созданы, но бэкапов БД нет (не настроен клиент).  Папка: РК  Критичность несоответствия: высокая |
|  | Убедиться, что в журнале СРК ЦОД содержатся записи об успешных тестовых восстановлениях из резервных копий Системы.  Убедиться, что тестовое восстановление из резервных копий Системы проводится в соответствии с согласованным РОН. | В журнале СРК ЦОД содержатся записи об успешных тестовых восстановлениях из резервных копий Системы.  Тестовое восстановление из резервных копий Системы проводится в соответствии с согласованным РОН. | Не пройдено | Тестовое восстановление из резервных копий не производилось, восстановление не запланировано.  Файл: 13.1.5, 13.1.5.1  Критичность несоответствия: высокая |
|  | Убедиться, что в согласованном документе Руководство по обеспечению непрерывности описан порядок резервного копирования баз данных с серверов Системы. | В документе Руководство по обеспечению непрерывности описан порядок резервного копирования баз данных с серверов Системы.  Документ согласован. | Пройдено | Раздел 4.2 РОН |
|  | **Для Системы должны быть выпущены следующие документы: Техническое задание, Технический проект, Технический паспорт ИС, Регламент предоставления доступа, Руководство по обеспечению непрерывности, Инструкция администратора, Инструкция пользователя** | | | | | |
|  |  |  | У менеджера проекта запрашиваются следующие документы и проверяется их статус:   1. Техническое задание, 2. Технический проект, 3. Технический паспорт ИС, 4. Регламент предоставления доступа, 5. Руководство по обеспечению непрерывности, 6. Инструкция администратора, 7. Инструкция пользователя | Все необходимые документы предоставлены и их статус – утверждено или согласовано | Пройдено | Все документы согласованы |
|  | **Наличие доступа к ИС у Администраторов ИБ** | | | | | |
|  |  | 1 | Запросить у начальника отдела поддержки систем защиты информации подтверждение наличия доступа к ИС у Администраторов ИБ, которые имеют право доступа к ИС в соответствии с ТПс | Всем Администраторам ИБ предоставлен доступ к ИС в соответствии с ТПс. | Не пройдено | У администраторов ИБ нет в СКДПП серверов ИС.  Файл: Re 1154 оценка  Критичность несоответствия: высокая |

**Таблица 2   
Объем испытаний реализации мер по обеспечению безопасности ПДн**

| **№  п/п** | **Реализация требования ИБ** | **№  п/п** | **Описание методики испытания** | **Критерий успешного прохождения испытания** | Результат испытания | Примечание  **(ссылка на свидетельство)** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА (ИАФ)** | | | | | | |
|  | ИАФ.5 Защита обратной связи при вводе аутентификационной информации | | | | | |
|  | На уровне ОС Astra Linux SE 1.6:  В процессе аутентификации символы аутентификационной информации и их количество не отображаются (при доступе по SSH). |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команду: ssh 127.0.0.1 <имя пользователя>  Убедиться, что при вводе пароля в запрашиваемой форме пароль не отображается. | При вводе пароля в запрашиваемой форме на Astra Linux пароль не отображается. | Пройдено | sib-cdc-irp-s2.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  0.1.1.1 |
|  | **На уровне Прикладного ПО:**  В форме аутентификации прикладного ПО вводимая в поле «Пароль» информация маскируется символами • («точка»).  В форме аутентификации отсутствует возможность просмотра вводимой информации в поле «пароль». |  | Выполнить подключение по HTTPS к веб-интерфейсу ППО любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор СОРИБ.  В открывшемся веб-интерфейсе ППО в правом верхнем углу осуществить выход из учетной записи.  На странице входа в ППО осуществить попытку ввода пароля. Убедиться, что при вводе пароля информация маскируется символами • («точка»). | При вводе пароля информация маскируется символами • («точка»). | Пройдено | Испытания проводились на Сервер приложений и СУБД(основной сервер) sib-cdc-irp-s1.rosneft.ru (10.192.91.101).  Под УЗ iyukuznetsov\_adm\_cdc с ролью Администратор СОРИБ  Файл 0.1.2.1 |
| **УПРАВЛЕНИЕ ДОСТУПОМ СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА (УПД)** | | | | | | |
|  | УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | | | | | |
|  | Назначение прав и привилегий пользователям, администраторам, а также системным учетным записям осуществляется в соответствии с матрицей доступов, приведенной в РПД с соблюдением т. н. принципа «минимально необходимых привилегий» (least privileges). |  | Убедиться, что в согласованном документе РПД описана Матрица доступов. | В РПД описана Матрица доступов.  Документ согласован. | Пройдено | Приложение 1 РПД |
|  | УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | | | | | |
|  | **На уровне Прикладного ПО**:  Ограничение на неуспешные попытки доступа в систему в ПО R-Vision IRP устанавливается встроенными средствами ПО R-Vision IRP в настройках парольной политики. В случае 10 подряд неудачных попыток ввода пароля, доступ блокируется на 30 минут. |  | Выполнить подключение по HTTPS к веб-интерфейсу ППО любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор СОРИБ.  В интерфейсе ППО перейти в раздел «Настройки».  Убедиться, что в настройках парольной политики указаны параметры:  Количество неудачный попыток – 10.  Период блокировки – 30 минут. | В настройках парольной политики ППО указаны параметры:  Количество неудачный попыток – 10.  Период блокировки – 30 минут. | Не пройдено | Испытания проводились на Сервер приложений и СУБД (основной сервер) sib-cdc-irp-s1.rosneft.ru (10.192.91.101).  Под УЗ iyukuznetsov\_adm\_cdc с ролью Администратор СОРИБ  Параметры парольной политики не соответствуют требованиям.  Файл 0.3.1.1  Критичность несоответствия: высокая |
|  | Убедиться, что настройки парольной политики встроенных и служебных УЗ соответствуют политикам Компании. | Настройки парольной политики встроенных и служебных УЗ соответствуют политикам Компании. | Не применимо | Испытания проводились на Сервер приложений и СУБД (основной сервер) sib-cdc-irp-s1.rosneft.ru (10.192.91.101).  Под УЗ iyukuznetsov\_adm\_cdc с ролью Администратор СОРИБ  Встроенные и служебные УЗ не отображаются в интерфейсе «R-Vision»  Файл 4.2.1.59-4.2.1.69 |
| **АНТИВИРУСНАЯ ЗАЩИТА (АВЗ)** | | | | | | |
|  | АВЗ.1 Реализация антивирусной защиты | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6**:  На компонентах Системы установлены средства антивирусной защиты производства АО «Лаборатория Касперского» для ОС Linux. Антивирусные решения, являются централизованно управляемыми. |  | Выполнить команду: sudo /opt/kaspersky/klnagent64/klnagchk  Убедиться, что установленный агент ПО Kaspersky подключен к серверу управления САЗ ЦОД (в секции Server address в качестве источника указан сервер САЗ ЦОД).  Убедиться, что указанные дата/время последнего запроса на синхронизацию соответствует дате проведения испытания. | Установленный агент ПО Kaspersky подключен к серверу управления САЗ ЦОД (в секции Server address в качестве источника указан сервер САЗ ЦОД).  Дата/время последнего запроса на синхронизацию соответствует дате проведения испытания. | Пройдено | sib-cdc-irp-s2.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  0.4.1.1 |
|  | АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | | | | | |
|  | **На уровне ОС Astra Linux SE 1.6**:  Средства антивирусной защиты производят обновление баз данных признаков вредоносных компьютерных программ (вирусов) в автоматическом режиме. Источником обновлений является САЗ ЦОД |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команду:  sudo /opt/kaspersky/kesl/bin/kesl-control --app-info  Зафиксировать результат выполнения команды.  Убедиться, что версия БД сигнатур угроз актуальна.  Убедиться, что источником обновлений является сервер САЗ ЦОД. | Версия БД сигнатур угроз САЗ актуальна.  Источником обновлений является сервер САЗ ЦОД. | Пройдено | sib-cdc-irp-s2.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  0.5.1.1 |
| **КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ (АНЗ)** | | | | | | |
|  | АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | | | | | |
|  | Организационная мера: В Инструкции администратора предусмотрен порядок действий администратора в части контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации. |  | Убедиться, что в согласованном документе Инструкция администратора описан порядок действий в части контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации. | В документе Инструкция администратора описан порядок действий в части контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.  Документ согласован. | Пройдено | Разделы 4, 6.3 ИА |
| **ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ (ОДТ)** | | | | | | |
|  | ОДТ.3 Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | | | | | |
|  | Контроль безотказного функционирования проводится в отношении средств обеспечения функционирования информационной системы путем мониторинга работоспособности компонентов и обработки данных в соответствии с инструкцией администратора. |  | Убедиться, что в согласованном документе Инструкция администратора описан порядок контроля безотказного функционирования. | В документе Инструкция администратора описан порядок контроля безотказного функционирования.  Документ согласован | Не пройдено | В ИА не описан порядок контроля безотказного функционирования ИС.  Критичность несоответствия: средняя |
| **ЗАЩИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ, ЕЕ СРЕДСТВ, СИСТЕМ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ (3ИС)** | | | | | | |
|  | ЗИС.3 Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | | | | | |
|  | **Специальными средствами:**  Все компоненты СОРИБ размещены в отдельных сегментах внутренней ДМЗ. Доступ к внутренним ДМЗ из сетей, не соответствующих требованиям Положения Компании «Требования к защите локальных вычислительных сетей Компании, подключаемых в единую корпоративную телекоммуникационную систему ПАО «НК «Роснефть» № П3-11.01 Р-0123, введенного в действие 26.12.2016 г, возможен только с использованием ПКЗИ. Для взаимодействия с веб-интерфейсами СОРИБ используется протокол SSL. Для администрирования серверов СОРИБ используются протоколы SSH. |  | Выполнить подключение по HTTPS к веб-интерфейсу ППО любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Администратор СОРИБ.  В адресной строке открыть информацию о подключении.  Открыть информацию о сертификате SSL.  Убедиться, что SSL-сертификат выдан инфраструктурным УЦ домена «rosneft.ru». | SSL-сертификат выдан инфраструктурным УЦ домена «rosneft.ru». | Пройдено | Испытания проводились на Сервер приложений и СУБД (основной сервер) sib-cdc-irp-s1.rosneft.ru (10.192.91.101).  Под УЗ iyukuznetsov\_adm\_cdc с ролью Администратор СОРИБ  Файл 0.8.1.1.1 – 0.8.1.1.3 |
| **УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ И СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (УКФ)** | | | | | | |
|  | УКФ.1 Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных | | | | | |
|  | Выполняется организационными мерами: лица, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных, определены в Техническом паспорте СОРИБ |  | Убедиться, что в согласованном документе Технический паспорт описан перечень работников, которым разрешены действия по внесению изменений в конфигурацию ИС. | В документе Технический паспорт описан перечень работников, которым разрешены действия по внесению изменений в конфигурацию ИС.  Документ согласован. | Пройдено | Раздел 4 ТПс |
|  | УКФ.2 Управление изменениями конфигурации информационной системы и системы защиты персональных данных | | | | | |
|  | Выполняется организационными мерами: Порядок обновления и изменения СОРИБ определён в документе «Руководство по обеспечению непрерывности» в разделе 2.2. |  | Убедиться, что в согласованном документе Руководство по обеспечению непрерывности описан порядок обновления и изменения Системы. | В документе Руководство по обеспечению непрерывности описан порядок обновления и изменения Системы.  Документ согласован | Пройдено | Раздел 3.2 РОН |
| ДОПОЛНИТЕЛЬНЫЕ МЕРЫ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ УТВЕРЖДЕННЫМИ ПРИКАЗОМ ФСБ РОССИИ ОТ 10 ИЮЛЯ 2014 Г. № 378 | | | | | | |
|  | Утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей | | | | | |
|  | Утвержден документ «Перечень должностных лиц, которым необходим доступ к обрабатываемым в ИСПДн персональным данным» |  | У руководителя проектом запросить утвержденный документ «Перечень должностных лиц, которым необходим доступ к обрабатываемым в ИСПДн персональным данным». | Документ «Перечень должностных лиц, которым необходим доступ к обрабатываемым в ИСПДн персональным данным» предоставлен.  Документ утвержден. | Пройдено | Приложение 4 к РПД\_Перечень лиц, которым необходим доступ к ПДН, 1154 ЛС\_РПД\_v1.2\_korch |
|  | Обеспечение поддержания в актуальном состоянии документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей | | | | | |
|  | Обеспечивается действующими в Компании процедурами предоставления доступа к Системе в соответствии с утвержденным Регламентом предоставления доступа |  | Убедиться, что в согласованном документе Регламент предоставления доступа описан порядок поддержания в актуальном состоянии документа, которым необходим доступ к персональным данным | В документе Регламент предоставления доступа описан порядок поддержания в актуальном состоянии документа, которым необходим доступ к персональным данным.  Документ согласован. | Пройдено | Раздел 5 РПД |

**Таблица 3   
Объем испытаний реализации требований Профиля ИБ ОС Astra Linux SE 1.6**

| **№  п/п** | **Реализация требования ИБ** | **№  п/п** | **Описание методики испытания** | **Критерий успешного прохождения испытания** | Результат испытания | Примечание  **(ссылка на свидетельство)** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА (ИАФ)** | | | | | | |
| 17  (15.5.2) | Доступ пользователей к консоли должен быть отключен |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить следующие команды:  systemctl is-enabled astra-console-lock  Убедиться, что параметр astra-console-lock имеет значение enable. | Для astra-console-lock установлено enable | Не пройдено | sib-cdc-irp-cl3.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  p.17.1  Отсутствует доступ на выполнение команды  Критичность несоответствия: высокая |
| 18 | Системные учетные записи должны быть заблокированы |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить следующие команду cat /etc/passwd  Убедиться, что для учетных записей установлены следующие параметры:   * daemon – заблокирована; * bin – заблокирована; * mail – заблокирована; * news – заблокирована; * nobody – заблокирована; * wwwrun – заблокирована; * sshd – установлен запрет на вход; * lp – заблокирована; * uucp – заблокирована. | Для учетных записей установлены следующие параметры:   * daemon – заблокирована; * bin – заблокирована; * mail – заблокирована; * news – заблокирована; * nobody – заблокирована; * wwwrun – заблокирована; * sshd – установлен запрет на вход; * lp – заблокирована; * uucp – заблокирована. | Не пройдено | sib-cdc-irp-cl3.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  p.18.1  параметры УЗ не соответствуют требованию  Критичность несоответствия: высокая |
| 21  (15.2.2) | Режим киоска для пользователей должен быть включен и настроен |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команду: cat /parsecfs/mode\_mask  Убедиться, что установлено значение маски отличное от 0000. | В конфигурацонном файле /parsecfs/mode\_mask установлено значение маски отличное от 0000 | Не пройдено | sib-cdc-irp-cl3.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  p.21.1  значение маски не соответствует требования  Критичность несоответствия: высокая |
| 22  (15.4) | Системные ограничения для пользователей должны быть включены |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команду: systemctl is-enabled astra-ulimits-control  Убедиться, что для параметра astra-ulimits-control установлено значение enable | Для параметра astra-ulimits-control установлено значение enable | Не пройдено | sib-cdc-irp-cl3.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  p.22.1  Отсутствует доступ на выполнение команды  Критичность несоответствия: высокая |
| 23  (15.5.6) | Использование клавиши SysRq должно быть запрещено |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команду: /etc/sysctl.conf  Убедиться, что для параметра kernel.sysrq установлено значение 0 | Для параметра kernel.sysrq установлено значение 0 | Не пройдено | sib-cdc-irp-cl3.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  p.23.1  Значение параметра не соответствует требования  Критичность несоответствия: высокая |
| 24  (15.5.3) | Исполнение модулей Python с расширенным функционалом должно быть заблокировано |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команду: find /usr/lib/python\* -type f -name "\_ctype\*"  Зафиксировать права на все файлы из вывода команды.  Убедиться, что право на исполнение отображенных файлов запрещено. | Исполнение модулей Python с расширенным функционалом запрещено | Пройдено | sib-cdc-irp-cl3.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  p.24.1 |
| 25 | Все неиспользуемые службы должны быть отключены |  | Выполнить подключение по SSH к любому серверу любой среды согласно Таблице 8 ПиМИ от имени УЗ с ролью Системный администратор.  Выполнить команды:  systemctl is-enabled,  netstat –ntulp  Зафиксировать результаты выполнения команд.  Убедиться, что в результатах вывода неиспользуемые службы отключены. | Все неиспользуемые службы отключены | Не пройдено | sib-cdc-irp-cl3.rosneft.ru  УЗ aiurentsev\_adm\_cdc  Файл  p.25.1  Отсутствует доступ на выполнение команды systemctl  Критичность несоответствия: высокая |

**Таблица 4   
Серверы Системы**

| **№** | **предназначение оборудования** | **FQDN, IP-адрес** | **Примечание** |
| --- | --- | --- | --- |
| **1** | **2** | **3** | **3** |
| **Продуктивная среда** | | | |
|  | Сервер приложений и СУБД  (основной сервер) | sib-cdc-irp-s1.rosneft.ru  IP-адрес: 10.192.91.101 | Astra Linux SE 1.6;  R-Vision IRP;  Postgres Pro Enterprise Certified;  Veritas NetBackup 8.2 Agent;  Kaspersky Security для Linux |
|  | Сервер приложений и СУБД  (резервный сервер) | sib-cdc-irp-s2.rosneft.ru  IP-адрес: 10.192.91.102 | Astra Linux SE 1.6;  R-Vision IRP;  Postgres Pro Enterprise Certified;  Veritas NetBackup 8.2 Agent;  Kaspersky Security для Linux |
|  | Коллектор реагирования #1 | sib-cdc-irp-cl1.rosneft.ru  IP-адрес: 10.192.91.103 | Astra Linux SE 1.6;  Veritas NetBackup 8.2 Agent;  Kaspersky Security для Linux |
|  | Коллектор реагирования #2 | sib-cdc-irp-cl2.rosneft.ru  IP-адрес: 10.192.91.104 | Astra Linux SE 1.6;  Veritas NetBackup 8.2 Agent;  Kaspersky Security для Linux |
|  | Коллектор реагирования #3 | sib-cdc-irp-cl3.rosneft.ru  IP-адрес: 10.192.91.105 | Astra Linux SE 1.6;  Veritas NetBackup 8.2 Agent;  Kaspersky Security для Linux |
| **Предпродуктивная среда** | | | |
|  | Сервер приложений и СУБД | sib-cdc-pirpsrv.rosneft.ru  IP-адрес: 10.192.80.28 | Astra Linux SE 1.6;  R-Vision IRP;  Postgres Pro Enterprise Certified;  Veritas NetBackup 8.2 Agent;  Kaspersky Security для Linux |
|  | Коллектор инвентаризации | sib-cdc-pirpcol.rosneft.ru  IP-адрес: 10.192.80.30 | Astra Linux SE 1.6;  Veritas NetBackup 8.2 Agent;  Kaspersky Security для Linux |

**Специалисты, проводившие испытания:**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Уренцев А.И. | Ведущий эксперт отдела оценки эффективности информационной безопасности Управления архитектуры информационной безопасности ООО ИК «СИБИНТЕК» |  |
|  |  |  | Подпись |
| 2. | Волков С.А. | Главный менеджер отдела оценки эффективности информационной безопасности Управления архитектуры информационной безопасности ООО ИК «СИБИНТЕК» |  |
|  |  |  | Подпись |
| 3. | Кузнецов И.Ю. | Ведущий эксперт отдела оценки эффективности информационной безопасности Управления архитектуры информационной безопасности ООО ИК «СИБИНТЕК» |  |
|  |  |  | Подпись |
| 4. | Хайруллин Ш.Х. | Эксперт отдела оценки эффективности информационной безопасности Управления архитектуры информационной безопасности ООО ИК «СИБИНТЕК» |  |
|  |  |  | Подпись |
| 5. | Жарова А.С. | Эксперт отдела оценки эффективности информационной безопасности Управления архитектуры информационной безопасности ООО ИК «СИБИНТЕК» |  |
|  |  |  | Подпись |
| 6 | Мягких А.А. | Эксперт отдела оценки эффективности информационной безопасности Управления архитектуры информационной безопасности ООО ИК «СИБИНТЕК» |  |
|  |  |  | Подпись |
| 7. | Ковалев Т.А. | Главный специалист отдела оценки эффективности информационной безопасности Управления архитектуры информационной безопасности ООО ИК «СИБИНТЕК» |  |
|  |  |  | Подпись |

**Документ согласован:**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Захаренко А.А. | Главный менеджер Управления по проектной деятельности  Дирекции по реализации проектов ООО «СИБИНТЕК-СОФТ» |  |
|  |  |  | Подпись |

Приложение 1

Скрипт выполняемых команд на уровне ОС Astra Linux 1.6 SE «Смоленск»

#!/bin/bash

date

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IP ХОСТА\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

hostname

hostname -I

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ВЕРСИЯ ОС\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

cat /etc/lsb-release

uname -a

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*АУДИТОР\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

auditor=$(whoami)

echo $auditor

id=$(id -u)

echo "UID $id"

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ДОМЕН\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*KRB5\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

cat /etc/krb5.conf

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*HOSTS\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

cat /etc/hosts

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*SSSD\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

sudo cat /etc/sssd/sssd.conf

echo

echo "\*\*\*\*\*ПАРОЛЬНАЯ ПОЛИТИКА\*\*\*\*\*"

date > com\_pass.txt

hostname >> com\_pass.txt

cat /etc/pam.d/common-password >> com\_pass.txt

grep PASS /etc/login.defs

grep LOGIN /etc/login.defs

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*УЗ БЕЗ ПАРОЛЯ\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

sudo getent shadow | grep '^[^:]\*:.\?:' | cut -d: -f1

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*KLIST\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

klist

echo

#ГРУПП и УЗ

date > passwd.txt

hostname >> passwd.txt

cat /etc/passwd >> passwd.txt

date > group.txt

hostname >> group.txt

cat /etc/group >> group.txt

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*WHEEL|SSH|SUDO|SU\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

sudo cat /etc/pam.d/su | grep wheel

date > pamd\_su.txt

hostname >> pamd\_su.txt

sudo cat /etc/pam.d/su >> pamd\_su.txt

getent group wheel

date > sudoers.txt

hostname >> sudoers.txt

sudo cat /etc/sudoers >> sudoers.txt

sudo grep PermitRootLogin /etc/ssh/sshd\_config

date > securetty.txt

hostname >> securetty.txt

sudo cat /etc/securetty >> securetty.txt

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*SUDODOERS.D\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

sudo ls -l /etc/sudoers.d

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*SU\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

sudo su

echo

#NETSTAT

date > netstat.txt

hostname >> netstat.txt

sudo netstat -na >> netstat.txt

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*РЕГИСТРАЦИЯ ВХОДА/ВЫХОДА\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

sudo grep $auditor /var/log/auth.log | tail -n 20

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*FDISK\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

#FDISK

sudo lsblk -f

sudo fdisk -l

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*LS\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

ls -al /

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*PS\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

ps -au

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*МАТРИЦА (ОБЪЕКТЫ ЗАЩИТЫ)\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

getfacl /var/log

echo

sudo getfacl /var/log/auth.log

echo

sudo getfacl /etc/fstab

echo

sudo getfacl /etc/passwd

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*НАСТРОЙКА АУДИТА\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

date > getfaud.txt

hostname >> getfaud.txt

getfaud -sR / >> getfaud.txt

echo

getfaud /etc/fstab

echo

getfaud /etc/passwd

echo

getfaud /var/log/auth.log

#РОТАЦИЯ ЖУРНАЛОВ

date > logrotate.txt

hostname >> logrotate.txt

cat /etc/logrotate.d/rsyslog >> logrotate.txt

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*РЕГИСТРАЦИЯ ЗАПУСКА\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

#ЗАПУСК ПРОГРАММ

sudo kernlog | grep $id | tail -n 20

echo

sudo /usr/sbin/kernlog | grep $id | grep cat

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*РЕГИСТРАЦИЯ ДОСТУПА К ЗАЩИЩАЕМОМУ ОБЪЕКТУ\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

#РЕГИСТРАЦИЯ ДОСТУПА К ЗАЩИЩАЕМОМУ ОБЪЕКТУ

date > fstab.txt

hostname >> fstab.txt

cat /etc/fstab >> fstab.txt

date > auth\_log.txt

hostname >> auth\_log.txt

cat /var/log/auth.log | head -n 20 >> auth\_log.txt

echo

sudo kernlog -x $id | grep fstab

sudo kernlog -x $id | grep auth.log

sudo kernlog -x $id | grep passwd

echo

sudo /usr/sbin/kernlog | grep $id | grep cat

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*SWAP\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

cat /etc/parsec/swap\_wiper.conf

echo

#НАСТРОЙКИ AFICK, ЕСЛИ ИСПОЛЬЗУЕТСЯ

date > afick.txt

hostname >> afick.txt

sudo cat /etc/afick.conf >> afick.txt

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*CRON.DAILY\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

sudo ls /etc/cron.daily

echo

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*КАСПЕРСКИЙ\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

sudo /opt/kaspersky/klnagent64/bin/klnagchk

echo

echo

sudo /opt/kaspersky/kesl/bin/kesl-control --app-info

#УСТАНОВЛЕННЫЕ ПАКЕТЫ

echo

date > packets.txt

hostname >> packets.txt

sudo dpkg –l >> packets.txt

#IPTABLES, ЕСЛИ ИСПОЛЬЗУЕТСЯ

date > iptables.txt

hostname >> iptables.txt

sudo iptables -L -v -n --line-numbers >> iptables.txt

sudo iptables -t filter -L >> iptables.txt

1. Далее проверка хранения событий в течение последних 90 дней в журнале /var/log/auth.log повторно не проводится [↑](#footnote-ref-1)
2. Далее проверка ротации и архивации журналов /var/log/auth.log и /var/log/audit/audit.log на уровне ОС повторно не проводится [↑](#footnote-ref-2)
3. Далее проверка резервного копирования журналов событий ОС с серверов Системы повторно не проводится [↑](#footnote-ref-3)
4. Далее проверка описания процедуры создания архивов журналов событий ОС в Инструкции администратора повторно не проводится [↑](#footnote-ref-4)
5. Далее описание процедуры создания архивов журналов событий СУБД в Инструкции администратора повторно не проверяется [↑](#footnote-ref-5)
6. Далее проверка регистрации действий привилегированных пользователей средствами СКДПП ЦОД на уровне ОС повторно не проводится [↑](#footnote-ref-6)
7. Далее проверка регистрации действий привилегированных пользователей средствами СКДПП ЦОД на уровне ППО повторно не проводится [↑](#footnote-ref-7)
8. Далее проверки настройки отправки и присутствия событий входа (выхода), запуска (завершения) программ и процессов, попыток доступа на изменение к защищаемым томам, каталогам, файлам в СМСИБ на уровне ОС повторно не проводятся [↑](#footnote-ref-8)