ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по предотвращению реализации угроз безопасности информации при применении SAP-систем в условиях прекращения их технической поддержки и распространения обновлений на территории Российской Федерации

2026

1. Произвести инвентаризацию и обеспечить актуальность установленных компонентов SAP и применяемых пакетов обновлений в соответствии с пунктом 1 приложения к настоящим рекомендациям:

провести анализ состояния установленных компонентов и пакетов обновлений;

проверить наличие неустановленных SAP Security Notes и устаревших версий ядра и модулей (установку SAP Security Notes, а также обновление устаревших версий ядра и модулей необходимо осуществлять в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г.);

провести аудит активированных сервисов и интерфейсов, доступных через SAP NetWeaver, SAP HANA и других компонентов системы;

обеспечить своевременное обновление операционных систем, баз данных и внешних библиотек, от которых зависит корректное функционирование SAP-системы (в случае невозможности установки обновлений системного и прикладного программного обеспечения рекомендуется принять компенсирующие меры, представленные разработчиками указанного системного и прикладного программного обеспечения);

произвести изоляцию уязвимых компонентов, обеспечив ограничение их сетевой доступности, минимизацию количества взаимодействующих с ними сервисов и пользователей, а также исключение доступа из недоверенных сегментов;

обеспечить регистрацию попыток эксплуатации уязвимостей с использованием автоматизированных средств обнаружения и реагирования, организовав их работу в режиме реального времени с контролем поведения сервисов, отслеживанием характерных последовательностей действий и обнаружением аномальных обращений к уязвимым компонентам. При выявлении попыток эксплуатации обеспечить реализацию автоматизированных мер реагирования, в том числе блокировку трафика, ограничение сеансов, временную изоляцию хоста или уведомление ответственных специалистов для оперативного принятия решений.

2. Произвести инвентаризацию учетных записей пользователей и сервисных записей, включая системные учетные записи SAP (SAP*, SAPSTAR, DDIC, SAPCPIC, EARLYWATCH), технические учетные записи интеграционных модулей и администраторов приложений в соответствии с пунктом 2 приложения к настоящим рекомендациям:

для всех обнаруженных учетных записей установить надежные пароли, учитывая что длина пароля должна быть не менее 15 символов, пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), специальные символы (например, !, », №, %, *, /) в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов);

заблокировать неиспользуемые учетные записи и исключить их из групп с административными правами, кроме того, обеспечить блокировку учетных записей пользователей, которые не осуществляли авторизацию в системе более 6 месяцев;

обеспечить отключение учетной записи SAP* (SAPSTAR) путем изменения параметров таблицы RZ10, кроме того обеспечить мониторинг изменений параметров указанной таблицы;

обеспечить мониторинг создания и действий пользователей, имеющих профиль полномочий SAP_ALL, SAP_NEW;

обеспечить использование технических учетных записей только системными задачами и обеспечить контроль их действий внедрением механизмов журналирования.

3. Обеспечить ограничение доступа к неиспользуемым веб-сервисам, интерфейсам и компонентам SAP, а также провести отключение всех встроенных механизмов и сервисов, которые не задействованы в бизнес-процессах организации, обеспечив их недоступность из внешних и внутренних сегментов в соответствии с пунктом 3 приложения к настоящим рекомендациям:

проверить активные сервисы ICF (включая ITS, WebDynpro, мобильные сервисы и вспомогательные веб-интерфейсы) и отключить все, которые не используются;

проверить наличие активных сервисов и модулей AS Java (Portal, UME, SQL Dispatcher, диагностические компоненты и другие подсистемы) и остановить неиспользуемые компоненты;

проверить активные компоненты SAP HANA XS Engine, XS Classic и XS Advanced, включая контейнеры приложений и вспомогательные сервисы, и отключить неиспользуемые движки и функциональные модули;

проверить активные BI-сервисы (Web Intelligence, Crystal Reports, Analysis Services, BIP-сервисы) и отключить все компоненты, не применяемые в работе организации;

проверить зарегистрированные RFC-функции, внешние интерфейсы интеграции и Web Services Repository, исключив доступ ко всем интерфейсам,

не используемым в текущих сценариях взаимодействия;

ограничить RFC-подключение к функциональным модулям системы путем настройки объекта полномочий S_RFC.

4. Обеспечить ограничение доступа к административным интерфейсам и сервисам SAP, а также провести проверку всех доступных административных компонентов с целью исключения несанкционированных подключений и минимизации поверхности атаки в соответствии с пунктом 4 приложения к настоящим рекомендациям:

проверить доступность SAPControl, SAPHostControl, Message Server, Gateway, Web Dispatcher, SAPRouter и иных административных сервисов и ограничить их вызов только доверенными хостами;

проверить настройки консольных и веб-интерфейсов администрирования SAP HANA (включая HANA Cockpit и HANA Studio) и обеспечить их доступность исключительно из закрытых административных сегментов;

ограничить доступ к административным компонентам SAP Business Objects (CMC, BI LaunchPad и сопутствующим сервисам), исключив возможность их вызова из внешних сетей;

проверить наличие и корректность файлов ACL и других механизмов ограничений доступа к административным интерфейсам, запретив использование универсальных разрешений вида «*», в том числе в таблице SAPRouttab;

обеспечить применение аутентификации и авторизации для всех интерфейсов удаленного администрирования, путем использования механизмов аутентификации, таких как Kerberos/SPNEGO, SAML 2.0, OAuth 2.0, сертификатную аутентификацию X.509 и SNC и авторизации на ролевой модели SAP (например, с использованием PFCG в ABAP, UME в SAP Java), предусматривая минимально необходимые привилегии, включая разрешения OData/Fiori и политики безопасности SAP HANA.

5. Провести анализ конфигурации параметров безопасности профиля SAP-систем в соответствии с пунктом 5 приложения к настоящим рекомендациям:

проверить параметры, регулирующие политику паролей, ограничения неудачных попыток входа, контроля времени действия паролей, требования к длине и сложности, а также настройку допустимых способов аутентификации;

исключить использование параметров, допускающих обход аутентификации или выполнение операций без проверки авторизации;

установить безопасные значения параметров профиля, обеспечивающих сетевое взаимодействие, контроль доступа к интерфейсам и ограничение

регистрации внешних программ;

произвести настройку инструмента для контроля конфигураций SAP Configuration Validation (при наличии);

произвести настройку инструмента SAP Security Self Service, для контроля безопасности SAP-систем.

6. Проверить наличие и корректность настройки механизмов шифрования и защиту всех каналов передачи данных между компонентами SAP и внешними системами в соответствии с пунктом 6 приложения к настоящим рекомендациям:

обеспечить использование протоколов SSL/TLS и SNC для всех HTTP-, RFC-, DIAG-, JDBC-, ODBC-, SOAP- и OData-соединений;

проверить настройки STRUST (ABAP) и NWA/Key Storage (Java) и обеспечить корректную загрузку сертификатов, задействованных в каналах связи, включая Web Dispatcher, ICM/ICF и встроенные Java-серверы;

ограничить использование устаревших криптографических алгоритмов и протоколов (например, SSL 2.0/3.0, TLS 1.0/1.1, RC4, DES, 3DES), разрешив только современные алгоритмы и версии TLS;

проверить настройки шифрования SAP HANA (студия, Cockpit, SQL-клиенты, внутренние сервисы), обеспечив включение параметров tls, sslvalidate, internal communication encryption и шифрования для SAP HANA System Replication;

обеспечить применение механизма SNC для взаимодействия SAP GUI и ABAP-серверов, задав минимально допустимые криптографические параметры и запретив незашифрованный DIAG-трафик;

проверить настройки SM59 и NWA для RFC-интерфейсов (ABAP — ABAP, ABAP — Java, ABAP — HANA), обеспечив обязательное использование шифрования и отключив «No encryption» в профилях соединений;

проверить наличие шифрования для интерфейсов администрирования (SAPControl, SAPHostControl, Web Dispatcher admin UI, HANA Cockpit, BO CMC и прочих), исключив доступ по незащищенным каналам.

7. Провести инвентаризацию прав доступа в соответствии с пунктом 7 приложения к настоящим рекомендациям:

определить критичные полномочия, предоставляющие возможность выполнения операций с правами администратора, изменения параметров безопасности и доступа к функциям, влияющим на целостность данных и бизнес-процессов;

обеспечить функционирование системы контроля критичных полномочий, предусматривающей постоянный мониторинг использования административных функций, регистрацию и анализ попыток их применения, а также автоматическое ограничение действий при выявлении несанкционированных или отклоняющихся от установленных политик операций;

реализовать процедуру регулярной проверки актуальности предоставленных прав, обеспечив документирование результатов контроля и оперативное реагирование на выявленные отклонения.

8. Проверить наличие доверенных соединений и связей между SAP-системами, в том числе RFC-назначений с сохраненными учетными данными и конфигурациями доверенных систем в соответствии с пунктом 8 приложения к настоящим рекомендациям:

использовать доверенное соединение только с системами с сопоставимым уровнем защиты;

исключить неиспользуемые и устаревшие связи, а также удалить сохраненные пароли из назначений;

обеспечить строгую изоляцию и отсутствие двусторонних доверенных отношений для систем, функционирующих в разных средах (например, исследовательский стенд, тестовая зона информационной системы («песочница»), информационная система, функционирующая в штатном режиме).

9. Обеспечить включение и регулярный контроль механизмов журналирования и аудита событий безопасности в соответствии с пунктом 9 приложения к настоящим рекомендациям:

активировать ведение системных журналов безопасности (Security Audit Log, Read Access Logging, Business Transformation Log) для регистрации действий пользователей, операций входа и изменения параметров системы;

включить ведение журналов HTTP-запросов, журналов шлюза и событий на уровне базы данных;

осуществлять в защищенном виде хранение журналов и регулярную проверку со стороны администраторов безопасности указанного процесса для выявления признаков несанкционированной активности.

10. Обеспечить безопасность данных в SAP-системах:

запретить использование транзакции SE16N (прямое ведение таблиц в промышленных системах);

запретить в промышленных системах использование транзакций SE38, SA38

(запуск программ и функциональных модулей напрямую);

запретить транзакцию PFCG и SU01 всем пользователям, кроме администраторов (администраторов безопасности);

запретить использование доступа ко всем таблицам системы: для объекта S_TABU_DIS значений «*» и «&NC&», для объекта S_TABU_NAM значения «*».

11. Регламентировать процессы управления доступом и безопасной разработки путем разработки и утверждения в органе (организации) концепции полномочий и управления доступом в SAP-системах, требований к ведению безопасной разработки в SAP-системах.

12. Обеспечить безопасность в процесса безопасной разработки в SAP-системах путем запрета использования отладчика в режиме DEBUG (ACTVT = 01.02) (функция подмены переменных в режиме отладки). Для изменения промышленных систем, применять только конвейер DEVOps, используя транспортную систему SAP (STMS). Кроме того, необходимо обеспечить проведение статического анализа кода автоматизированными средствами или вручную.

Приложение 1

Перечень параметров, ролей, сервисов и учетных записей, подлежащих контролю и приведению к безопасным значениям в SAP-системах

№ п/п	Наименование параметра/роли/сервиса	Действие	Безопасное значение/результат	Продукт SAP
1. Управление обновлениями				
1.1	Установленные SAP Security Notes	Проверить наличие и применить все актуальные обновления безопасности	Актуальный уровень SAP Security Notes установлен	ABAP / Java/ S/4HANA
1.2	Версия ядра (Kernel)	Сверить с последней доступной версией	Используется последняя версия ядра	ABAP / Java
1.3	Версии HANA DB	Проверить актуальность релиза	Установлены последние SAP HANA Revision и обновления ОС	HANA / S/4HANA
1.4	Уровень патчей BI-платформы	Проверить наличие обновлений	Применены последние FixPack / SP	Business Objects
2. Учетные записи и пароли по умолчанию				
2.1	SAP*, DDIC, SAPCPIC, EARLYWATCH	Проверить наличие и состояние	Аккаунты заблокированы или пароли изменены	ABAP / S/4HANA
2.2	Administrator, Guest	Проверить наличие стандартных пользователей	Пароли изменены, гостевой доступ отключен	Java / Business Objects
2.3	SYSTEM, _SYS_REPO, XSA_ADMIN	Проверить пароли системных пользователей	Сложные пароли, ограниченный доступ	HANA
3. Неиспользуемый функционал и сервисы				
3.1	ICF-сервисы (ITS, WebDynpro, mobile)	Проверить активность	Неиспользуемые сервисы отключены	ABAP / S/4HANA
3.2	J2EE-сервисы (Portal, SQL Dispatcher)	Проверить наличие	Неиспользуемые сервисы остановлены	Java
3.3	XS Engine, контейнеры HANA	Проверить активные компоненты	Отключены неиспользуемые движки	HANA
3.4	BI-сервисы Web Intelligence, Crystal Reports	Проверить активность	Отключены, если не используются	Business Objects
4. Открытые интерфейсы и администрирование				
4.1	SAPControl, SAPHostControl	Проверить доступность извне	Доступ ограничен доверенными IP	ABAP / Java / S/4HANA

№ п/п	Наименование параметра/роли/ сервиса	Действие	Безопасное значение/результат	Продукт SAP
4.2	Message Server, Gateway	Проверить списки ACL	Установлены ACL-файлы, отсутствует «*»	ABAP / S/4HANA
4.3	HANA Cockpit, Web Dispatcher	Проверить каналы доступа	Доступ только через HTTPS / VPN	HANA
4.4	CMC (Central Management Console)	Проверить доступ	Доступ только по SSL, ограниченные пользователи	Business Objects
5. Параметры профиля и конфигурации безопасности				
5.1	login/min_password_lng	Установить минимальную длину пароля	⩾ 15 символов	ABAP / S/4HANA
5.2	login/ min_password_digits	Требовать цифры в пароле	⩾ 1	ABAP / S/4HANA
5.3	login/ min_password_letters	Требовать буквы	⩾ 1	ABAP / S/4HANA
5.4	login/ min_password_specials	Требовать спецсимволы	⩾ 1	ABAP / S/4HANA
5.5	login/ password_expiration_time	Настроить срок действия пароля	⩽ 90 дней	ABAP / S/4HANA
5.6	login/ password_history_size	Включить историю паролей	⩾ 5 предыдущих паролей	ABAP / S/4HANA
5.7	login/fails_to_user_lock	Установить лимит неудачных попыток входа	5 или меньше	ABAP / S/4HANA
5.8	login/ disable_multi_gui_login	Запретить множественные одновременные сессии	Значение = 1	ABAP / S/4HANA
5.9	login/ password_max_idle_productive	Ограничить срок неиспользуемых учетных записей	⩽ 30 дней	ABAP / S/4HANA
5.10	login/ password_downwards_compatibility	Отключить старые алгоритмы хеширования	Значение = 0	ABAP / S/4HANA
5.11	icm/HTTP/auth_*	Ограничить методы аутентификации в HTTP	Отключены слабые/анонимные методы	ABAP / S/4HANA
5.12	rfc/login_security_mode	Усилить аутентификацию RFC	Значение = 1 (требовать защищенное подключение)	ABAP / S/4HANA

№ п/п	Наименование параметра/роли/ сервиса	Действие	Безопасное значение/результат	Продукт SAP
5.13	gw/acl_mode	Включить контроль ACL для Gateway	Значение = 1 (ACL включен)	ABAP / S/4HANA
5.14	gw/sec_info	Настроить файл разрешенных программ	Явный список разрешенных программ (без «*»)	ABAP / S/4HANA
5.15	gw/reg_info	Ограничить регистрацию внешних программ	Только конкретные, авторизованные программы	ABAP / S/4HANA
5.16	gw/reg_no_conn_info	Запретить выдачу информации о подключенных программах	Значение = 1 — скрытие информации о внешних RFC-программах	ABAP / S4HANA
5.17	gw/monitor	Отключить незащищенный доступ к Gateway Monitor	Значение = 0 (доступ запрещен)	ABAP / S/4HANA
5.18	rdisp/gui_auto_login	Запретить автоматический SAP GUI логин	Значение = 0	ABAP / S/4HANA
5.19	login/ no_automatic_user_sapstar	Запретить обход аутентификации SAP*	Значение = 1	ABAP / S/4HANA
5.20	login/ disable_password_logon	Запретить вход с паролем там, где используется SSO	Значение = 1	ABAP / Java
5.21	icm/server_port_0	Запретить порты без TLS	Только HTTPS-порты; HTTP отключен	ABAP / S/4HANA
5.22	icm/HTTPS/ verify_client	Включить проверку клиента при необходимости	Проверка активна	ABAP / S/4HANA
5.23	login/accept_sso2_ticket	Контролировать прием SSO2 Ticket	Включено только при использовании SSO2; при отсутствии SSO — отключено	ABAP / S4HANA
5.24	login/ accept_sso2_ticket_only	Ограничить способы аутентификации	Использовать только при обязательном SSO (значение = 1); иначе = 0	ABAP / S4HANA
5.25	snc/enable	Включить использование SNC	Значение = 1	ABAP / S4HANA
5.26	snc/identity/as	Задать SNC-идентификатор сервера	Корректно настроенный SNC-name	ABAP / S4HANA

№ п/п	Наименование параметра/роли/ сервиса	Действие	Безопасное значение/результат	Продукт SAP
5.27	snc/identity/dn	Задать Distinguished Name для SNC	DN соответствует сертификату SNC	ABAP / S4HANA
5.28	auth/saml2*	Настроить параметры SAML 2.0	SAML2 включен при использовании SSO, корректная конфигурация IdP и сертификатов	ABAP / Java / S4HANA
5.29	ssl/client_ciphersuites	Ограничить наборы шифров для SSL-клиентов	Только современные шифры (PFS, AES-GCM, TLS1.2/1.3)	ABAP / S4HANA
5.30	ssl/ciphersuites	Ограничить cipher-suites SSL-сервера	Исключить RC4, DES, 3DES, разрешить современные шифры	ABAP / S4HANA
5.31	ume.logon.security_policy.password_min_length	Настроить минимальную длину пароля	⩾ 15	Java / UME
5.32	ume.logon.security_policy.password_max_length	Задать максимальную длину пароля	72+ символов	Java / UME
5.33	ume.logon.security_policy.password_min_digits	Требовать цифры	⩾ 1	Java / UME
5.34	ume.logon.security_policy.password_min_letters	Требовать буквы	⩾ 1	Java / UME
5.35	ume.logon.security_policy.password_min_specials	Требовать спецсимволы	⩾ 1	Java / UME
5.36	ume.logon.security_policy.password_history_size	Включить историю паролей	⩾ 5 последних паролей	Java / UME
5.37	ume.logon.security_policy.password_expiration_period	Задать срок действия пароля	⩽ 90 дней	Java / UME
5.38	ume.logon.security_policy.password_change_required	Требовать смену пароля при первом входе	Значение = TRUE	Java / UME
5.39	ume.logon.security_policy.lockout_threshold	Установить лимит ошибок входа	5 или меньше	Java / UME
5.40	ume.logon.security_policy.lockout_duration	Задать время блокировки	⩾ 15 минут	Java / UME
5.41	ume.logon.security_policy.lockout_reset_timeout	Интервал сброса счетчика	15–30 минут	Java / UME

№ п/п	Наименование параметра/роли/ сервиса	Действие	Безопасное значение/результат	Продукт SAP
5.42	ume.configuration.security.single_signon.enabled	Включить/отключить SSO	Включено при централизованном SSO; отключено при отсутствии SSO	Java / UME
5.43	ume.configuration.security.assertion_ticket.enabled	Управлять Assertion Tickets	Включено только при использовании SAP Logon Tickets	Java / UME
5.44	ume.configuration.security.spnego.enabled	Включить SPNEGO/Kerberos	TRUE — если используется Kerberos; иначе FALSE	Java / UME
5.45	ume.configuration.security.saml2.enabled	Включить SAML2	TRUE при наличии IdP; иначе FALSE	Java / UME
5.46	ume.configuration.security.default_authentication	Определить разрешенные методы входа	Только безопасные методы (SPNEGO / SAML2 / пароль с политикой сложности)	Java / UME
5.47	ume.configuration.security.login_module_stack	Ограничить используемые LoginModules	Только проверенные модули аутентификации (без custom insecure stacks)	Java / UME
5.48	ume.logon.security.enforce_security	Применить строгие правила входа	Значение = TRUE	Java
5.49	auth/ enable_password_logon	Запретить слабые способы входа	Значение = FALSE (если используется SSO)	Java
5.50	BOE Authentication settings	Ограничить допустимые методы	Только LDAP/SAML/Windows AD или сильные SAP-учетные записи	SAP BusinessObjects
5.51	enforce_strong_passwords	Включить строгую политику паролей	Enabled	SAP BusinessObjects
5.52	password_policy.min_length	Задать длину пароля	⩾ 15	SAP HANA
5.53	password_policy.max_password_lifetime	Определить срок действия пароля	⩽ 90 дней	SAP HANA
5.54	password_policy.minimum_digit_count	Требовать цифры	⩾ 1	SAP HANA
5.55	password_policy.minimum_uppercase_count	Требовать заглавные буквы	⩾ 1	SAP HANA
5.56	password_policy.history_size	Включить историю паролей	⩾ 5	SAP HANA

№ п/п	Наименование параметра/роли/ сервиса	Действие	Безопасное значение/результат	Продукт SAP
5.57	password_policy.lockout _threshold	Установить лимит ошибок входа	⩽ 5	SAP HANA
6. Шифрование и защита каналов связи				
6.1	com.sap.engine.services. ssl.enabled	Включить SSL-сервисы в Java-движке	Значение = true (SSL включен для сервисов Java)	Java
6.2	communication	Включить шифрование внутренних сервисов	encr = Вся внутренняя коммуникация зашифрована	SAP HANA
6.3	enabledCipherSuites	Ограничить набор разрешенных шифров (cipher suites)	Указан жесткий список современных шифров, допускающих TLS 1.2/1.3 (только устойчивые ECDHE- и AEAD-алгоритмы)	Java / BO / другие Java-компоненты
6.4	sslvalidate	Включить проверку сертификатов	true = Проверка сертификатов обязательна	SAP HANA
6.5	icm/HTTPS/cipher_suite	Ограничить cipher-suite для ICM/HTTPS	Установлен перечень шифров, допускающих только TLS 1.2+ и современные безопасные наборы (например, ECDHE_AES_GCM)	ABAP / S/4HANA
6.6	icm/HTTPS/enabled	Включить поддержку HTTPS в ICM	TRUE — активация HTTPS	ABAP
6.7	icm/HTTPS/ ssl_protocols	Ограничить допустимые TLS-протоколы	Только TLSv1.2,TLSv1.3	ABAP
6.8	icm/HTTPS/ verify_client	Включить/настроить проверку клиента (при необходимости)	Включено при использовании клиентских сертификатов; в случае использования — проверка строгая	ABAP / S/4HANA
6.9	icm/server_port_HTTPS	Обеспечить наличие и корректную настройку HTTPS-порта	HTTPS-порт задан и активен, доступ по HTTP запрещен или перенаправлен на HTTPS	ABAP / S/4HANA

№ п/п	Наименование параметра/роли/сервиса	Действие	Безопасное значение/результат	Продукт SAP
6.10	keystore/truststore	Обеспечить корректное хранение ключей и сертификатов	Хранилища защищены, пароли надежны, доступ ограничен	Java / BO / HANA / ABAP (при использовании хранилищ)
6.11	OData/REST сервисы	Обеспечить шифрование сервисов Fiori/OData	Все сервисы доступны по HTTPS	SAP S/4HANA
6.12	RFC-профили SM59	Запретить незашифрованные RFC	Все RFC с использованием SNC/TLS, без «No encryption»	ABAP
6.13	SAP PO/PI/CPI: WS Security	Включить WS-Security	SOAP / Web Services только через TLS	SAP PO / CPI
6.14	snc/accept_insecure_gui	Запретить нешифрованный DIAG-трафик	0 - Нешифрованные соединения SAP GUI недопустимы	ABAP
6.15	snc/data_protect	Установить максимальную защиту SNC-трафика	3 - Максимальная защита целостности и конфиденциальности	ABAP
6.16	snc/data_protection	Обеспечить защиту данных с помощью SNC (контроль целостности/конфиденциальности)	Значение = 1 (включена защита данных)	ABAP / S/4HANA
6.17	snc/enable	Включить механизм SNC для защиты соединений	Значение = 1 (SNC включено) — все поддерживаемые RFC/GUI-каналы защищены	ABAP / S/4HANA
6.18	snc/identity/as	Настроить SNC-идентификатор сервера	Корректный SNC-идентификатор для SAP-сервера	ABAP
6.19	ssl.clientAuth	Включение требования клиентской аутентификации при необходимости	Включено для административных интерфейсов / по требованию политики — clientAuth=required	Java / BO
6.20	ssl/ciphersuites	Назначить стойкие наборы шифров	Высокая стойкость; исключены RC4, DES, 3DES	ABAP
6.21	ssl/client_ciphersuites	Установить современные наборы шифров	135:PFS:HIGH::EC Современные PFS-алгоритмы	ABAP

№ п/п	Наименование параметра/роли/сервиса	Действие	Безопасное значение/результат	Продукт SAP
6.22	ssl/ssl_lib	Указать и использовать SAP криптографическую библиотеку для SSL/SNC	Установлена SAPCryptolib (или другая сертифицированная библиотека), путь задан корректно	ABAP / S/4HANA
6.23	ssl/ssl_provider	Указать провайдера SSL для Java-движка	Провайдер SSL включен и настроен (поставщик реализует TLS 1.2+)	Java (NetWeaver Java)
6.24	STRUST (сертификаты)	Проверить корректность PSE и сертификатов	Актуальные сертификаты, корректные цепочки доверия	ABAP
6.25	tlsEnabled	Активировать использование TLS в соответствующих компонентах	Значение = true (используется TLS 1.2 или выше)	Java / BO / S/4HANA
6.26	wdisp/ssl_auth	Настроить проверку сертификатов	Аутентификация клиента включена при необходимости	SAP S/4HANA / Web Dispatcher
6.27	wdisp/ssl_cred	Настроить креденшелы для SSL	Корректные SSL-учетные данные Web Dispatcher	SAP S/4HANA / Web Dispatcher
6.28	wdisp/ssl_encrypt	Включить шифрование трафика Web Dispatcher → backend	Полное шифрование backend-трафика	SAP S/4HANA / Web Dispatcher
7. Контроль доступа и разделение полномочий				
7.1	Роли с SAP_ALL, SAP_NEW	Проверить наличие	Удалены или ограничены	ABAP / S/4HANA
7.2	Административные группы J2EE	Проверить наличие	Только уполномоченные пользователи	Java
7.3	Привилегии HANA (SELECT, ADMIN)	Проверить распределение	Минимальные необходимые привилегии	HANA
7.4	Роли CMC (Administrator, ContentAdmin)	Проверить полномочия	Роли разделены по функциям	Business Objects
8. Доверенные соединения и RFC				

№ п/п	Наименование параметра/роли/ сервиса	Действие	Безопасное значение/результат	Продукт SAP
8.1	RFC-назначения с сохраненными паролями	Проверить наличие	Используются технические пользователи с ограничениями	ABAP / S/4HANA
8.2	TRUSTED-системы	Проверить доверенные связи	Только между равнозначными системами	ABAP / Java
8.3	OAuth/SAML доверия	Проверить внешние интеграции	Устаревшие записи удалены	Java / BO / S/4HANA
9. Логирование и аудит				
9.1	rsau/enable	Проверить включение	Значение = 1 (активен Security Audit Log)	ABAP / S/4HANA
9.2	icm/HTTP/logging_<n>	Проверить активность логов	Значение = ALL	ABAP / S/4HANA
9.3	HANA Audit Policy	Проверить состояние	Активна для системных событий	HANA
9.4	Audit Log в CMC	Проверить включение	Включено, хранение в защищенной базе данных	Business Objects