ООО «Газинформсервис»

УТВЕРЖДАЮ
Заместитель генерального директора –
технический директор
ООО «Газинформсервис»

_____Н.В. Нашивочников

«____» _____ 20___ г.

ПРОГРАММНЫЙ КОМПЛЕКС
SAFEERP CODE SECURITY

Описание применения
ЛИСТ УТВЕРЖДЕНИЯ

643.72410666.00050-01 31 01-ЛУ

Представители предприятия-разработчика

Руководитель проекта

__ _____М.А. Татаренко

Руководитель группы защиты ППО SAP

_____С.В. Устенко

Исполнитель

_____В.К. Павлова

Нормоконтролер

_____И.Л.Крылова

2015

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

ООО «Газинформсервис»

Утвержден
643.72410666.00050-01 31 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС
SAFEERP CODE SECURITY

Описание применения

643.72410666.00050-01 31 01

Листов 13

2015

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

АННОТАЦИЯ

Настоящий документ содержит описание назначения и условий применения программного комплекса (ПК) SafeERP Code Security, описание решаемых им задач, входных и выходных данных. Описание применения ПК SafeERP Code Security ориентировано на пользователей, осуществляющих работу с программным обеспечением, а также руководителей, определяющих целесообразность применения данного программного обеспечения.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

ПК SafeERP Code Security предназначен для функционирования в интеграционной платформе SAP NetWeaver, разработанной компанией SAP. ПК SafeERP Code Security интегрируется в действующие системы SAP NetWeaver и предназначен для:

- анализа кода прикладного программного обеспечения SAP с целью контроля безопасного состояния программного кода ABAP в SAP-системах;
- повышения информационной безопасности (ИБ) и эффективности работы SAP-систем.

Областью контроля ПК SafeERP Code Security является язык программирования ABAP.

Применение ПК SafeERP Code Security позволяет достичь следующих производственно-экономических показателей:

- автоматизировать процесс получения информации о фактах нарушения ИБ и эффективности работы прикладного программного обеспечения систем, реализованных на платформе SAP NetWeaver;
- оптимизировать процессы и снизить трудозатраты на поиск опасных участков ABAP-кода в собственных и сторонних разработках.

2. УСЛОВИЯ ПРИМЕНЕНИЯ ПРОГРАММНОГО КОМПЛЕКСА

2.1. Область применения программного комплекса

ПК SafeERP Code Security функционирует в составе версий SAP NetWeaver не ниже 7.0.

Операционные системы и базы данных, на которых функционирует система SAP с интегрированным ПК SafeERP Code Security, должны соответствовать требованиям, указанным в эксплуатационной документации на систему SAP NetWeaver.

2.2. Состав программного комплекса

ПК SafeERP Code Security состоит из следующих компонентов:

- сервер управления ПК;
- ABAP-агент ПК (агент для систем SAP NetWeaver на ABAP-стеке).

Серверная часть устанавливается на SAP-систему, где будет работать оператор ИБ. Серверная часть содержит функционал для анализа объектов SAP-системы на безопасность. Для получения данных о проверяемом объекте серверная часть посылает запрос агентской части. Агентская часть устанавливается на SAP-систему, объекты которой необходимо анализировать. Агентская часть содержит набор функций, которые по запросу собирают данные о проверяемом объекте и передают их на серверную часть для анализа на безопасность.

2.3. Требования к техническим средствам

Так как программные компоненты ПК SafeERP Code Security интегрируются в заранее установленную и развернутую систему SAP NetWeaver, то технические средства должны соответствовать требованиям, указанным в эксплуатационной документации на систему SAP NetWeaver.

Технические характеристики компьютеров, на базе которых созданы автоматизированные рабочие места оператора ИБ, должны иметь характеристики не ниже:

- процессор Intel с частотой не менее 1,5 ГГц;
- оперативное запоминающее устройство с объемом памяти не менее 512 Мбайт;
- жесткий диск объемом не менее 1 Гбайт;
- встроенный SVGA-адаптер с объемом памяти не менее 32 Мбайт;
- жидкокристаллический монитор с размером экрана не менее 15 дюймов и разрешением не менее 1024x768 пикселей;
- встроенный сетевой адаптер.

В комплектность компьютера также должно входить следующее оборудование: клавиатура, мышь и источник бесперебойного питания.

2.4. Требования к программным средствам

Для работы сервера управления необходим сервер SAP NetWeaver AS ABAP не ниже версии 7.0.

На агенте SAP-системы необходим сервер SAP NetWeaver AS ABAP не ниже версии 7.0.

На автоматизированное рабочее место оператора ИБ должны быть установлены: SAP GUI for Windows не ниже версии 7.30 и Microsoft Office Excel – для формирования и просмотра отчетов.

Исходный код для ПК должен быть реализован на языке программирования ABAP/4.

2.5. Требования и условия организационного, технического и технологического характера

Программные компоненты ПК интегрируются в действующие системы SAP NetWeaver. Системному программисту (далее – администратор SAP-систем) сначала необходимо произвести установку комплекса, установить агенты на те системы SAP, на которых необходимо произвести комплексную проверку прикладного

программного обеспечения SAP (ABAP-кода). Правила установки ПК приведены в документе «Руководство системного программиста по установке и удалению компонентов ПК» 643.72410666.00050-01 32 01.

Рекомендуется в организации разработать организационно-распорядительные документы, в которых должны быть описаны процедуры:

- взаимодействия оператора ИБ с администраторами SAP-систем для передачи отчета о выявленных уязвимых участках в прикладном программном обеспечении;
- взаимодействия администраторов SAP-систем с разработчиками прикладного программного обеспечения SAP для устранения выявленных фактов нарушения в контролируемых SAP-системах.

3. ОПИСАНИЕ ЗАДАЧ

ПК Code Platform Security позволяет решать следующие основные задачи:

- обнаруживать уязвимые участки ABAP-кода по категории «безопасность»;
- обнаруживать уязвимые участки ABAP-кода по категории «производительность»;
- отображать собранные данные в окне панели управления ПК и экспортировать выбранные оператором ИБ данные в файлы формата «xlsm» или «pdf» (подсистема отображения собранных данных).

3.1. Подсистема обнаружения уязвимых участков ABAP-кода по категории «безопасность»

Подсистема обнаружения уязвимых участков ABAP-кода по категории «безопасность» предназначена для выявления опасных фрагментов ABAP-кода, отвечающих за безопасность использования прикладного программного обеспечения.

Основные области потенциальных уязвимостей, по которым осуществляется проверка кода в данной категории:

- программные закладки;
- критичные системные вызовы;
- вызов методов ABAP Kernel;
- критичные запросы к системе управления базами данных;
- критичный доступ к операционной системе;
- динамический вызов ABAP-кода;
- переполнение буфера в ABAP-коде;
- инъекция SQL;
- проверки авторизации;
- изменение хода выполнения (жестко запрограммированные проверки);
- использование таблиц базы данных без авторизационных групп;

– уязвимость команд HTML страниц.

Все потенциально уязвимые участки кода по категории «безопасность» маркируются своим уровнем критичности и отображаются в панели оператора ИБ и в отчете в следующих группах:

– высокая критичность;
– средняя критичность;
– низкая критичность;
– информация.

Собранные данные сохраняются в базе данных сервера управления.

3.2. Подсистема обнаружения уязвимых участков ABAP-кода по категории «производительность»

Подсистема обнаружения уязвимых участков ABAP-кода по категории «производительность» предназначена для выявления опасных фрагментов ABAP-кода, отвечающих за производительность в использовании прикладного программного обеспечения.

Основные области потенциальных уязвимостей, по которым осуществляется проверка кода в данной категории:

– обход буферизированных таблиц;
– неэффективное использование полей индекса таблиц;
– неэффективное использование команд внутри циклов;
– неэффективные запросы к базе данных;
– неэффективное использование памяти.

Все потенциально уязвимые участки кода по категории «производительность» маркируются своим уровнем критичности и отображаются в панели оператора ИБ и в отчете в следующих группах:

– высокая критичность;
– низкая критичность;
– информация.

Собранные данные сохраняются в базе данных сервера управления.

3.8. Подсистема отображения собранных данных

Подсистема отображения собранных данных осуществляет вывод данных, сохраненных в таблицу базы данных, в окно панели управления оператора ИБ и экспорт данных в файлы формата «xlsm» или «pdf». Состав отображаемых и экспортируемых данных определяет оператор ИБ. Оператору ИБ доступны только данные, собранные с контролируемых им систем SAP NetWeaver.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными для ПК SafeERP Code Security являются данные, собираемые агентами с контролируемых систем SAP NetWeaver, состав которых определяется настройками ПК SafeERP Code Security (настроенные системными программистами RFC-соединения при установке ПК).

Формат постановки систем SAP на контроль и установки ПК описан в документе «Руководство системного программиста по установке и удалению компонентов ПК» 643.72410666.00050-01 32 01.

Выходными данными для ПК SafeERP Code Security являются:

- данные, отображаемые в окне панели управления ПК оператора ИБ;
- данные, экспортируемые подсистемой отображения собранных данных, в файлы формата «xlsm» или «pdf»по запросам оператора ИБ.

Формат, описание и способы отображения выходных данных в окне панели управления оператора ИБ описаны в документе «Руководство оператора» 643.72410666.00050-01 34 01.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ИБ – информационная безопасность

ПК – программный комплекс

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	Номер докум.	Входящий № сопроводитель-ного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннули-рованных					

№ изменения:_____	Подпись отв. лица:_____	Дата внесения изм.:_____