ООО «Газинформсервис»

УТВЕРЖДАЮ
Заместитель генерального директора –
технический директор
ООО «Газинформсервис»

_____Н.В. Нашивочников

«____» _____ 20___ г.

ПРОГРАММНЫЙ КОМПЛЕКС SafeERP

Описание применения

ЛИСТ УТВЕРЖДЕНИЯ

643.72410666.00038-01 31 01-ЛУ

Представители предприятия-разработчика

Руководитель проекта/Начальник отдела РБППО

_____С.В. Устенко

Исполнитель

_____В.К. Павлова

Нормоконтролер

_____И.Л.Крылова

2020

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

Изм.	Подп.	Дата

Литера

ООО «Газинформсервис»

Утвержден
643.72410666.00038-01 31 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС SafeERP

Описание применения

643.72410666.00038-01 31 01

Листов 13

2020

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

Изм.	Подп.	Дата

Литера

АННОТАЦИЯ

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

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПК SAFEERP

ПК SafeERP предназначен для функционирования в интеграционной платформе SAP NetWeaver, разработанной компанией SAP SE. ПК SafeERP интегрируется в действующие SAP-системы и реализует следующие функциональные возможности:

- регистрацию изменений целостности программного обеспечения (изменение контрольных сумм программных объектов);
- регистрацию уязвимостей информационной системы (поиск и регистрация небезопасного состояния программного кода ABAP, небезопасного состояния настроек программного обеспечения и средств защиты);
- определение событий безопасности, подлежащих регистрации, и их состава (выбор программных объектов для постановки на контроль);
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности (отображение событий информационной безопасности в рабочей области оператора ПК SafeERP в удобном виде и формирования отчетов по полученным результатам в файлы формата «xlsx» или «doc» для дальнейшего анализа).

Применение ПК SafeERP позволяет достичь следующих производственно-экономических показателей:

- автоматизировать процесс получения информации о событиях информационной безопасности (ИБ) SAP-систем;
- оптимизировать процессы обработки событий ИБ;
- снизить трудозатраты на мониторинг и обработку событий ИБ;
- сократить сроки и расходы на проектирование мер защиты по обеспечению безопасности SAP-систем.

2. УСЛОВИЯ ПРИМЕНЕНИЯ ПК SAFEERP

2.1. Область применения ПК SafeERP

ПК SafeERP функционирует в составе версий с SAP NetWeaver не ниже 7.52.

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

2.2. Состав ПК SafeERP

ПК SafeERP состоит из следующих компонентов:

- сервер управления;
- ABAP-агент (агент для систем SAP NetWeaver на ABAP-стеке);
- Java-агент (агент для систем SAP NetWeaver на Java-стеке);
- BO-агент (агент для систем SAP Business Objects);
- HANA-агент (агент для систем SAP HANA).

Серверная часть ПК SafeERP устанавливается на SAP-систему, где будут работать оператор или администратор ПК SafeERP. 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 ПК SafeERP устанавливается на SAP-систему, программные 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 функциональные модули ПК SafeERP 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 и администратора ПК SafeERP, должны иметь характеристики не ниже:

- процессор Intel с частотой не менее 1,5 ГГц;
- оперативное запоминающее устройство с объемом памяти не менее 1 Гбайт;
- жесткий диск объемом не менее 150 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 необходима платформа SAP NetWeaver AS ABAP не ниже версии 7.52 с установленным компонентом SAP FIORI FRONT-END SERVER не ниже версии 5.0 SP1.

Для работы агентов необходимы платформы:

- для ABAP-агента – SAP NetWeaver AS ABAP не ниже версии 7.0;
- для Java-агента – SAP NetWeaver AS Java не ниже версии 7.31;
- для BO-агента – SAP BusinessObject BI не ниже версии 4.1;
- для HANA-агента – SAP HANA не ниже версии 1.0.

На автоматизированные рабочие места оператора и администратора ПК SafeERP должны быть установлены: SAP GUI for Windows не ниже версии 7.50 и Microsoft Office – для формирования и просмотра отчетов.

2.5. Требования и условия организационного, технического и технологического характера

Администрирование ПК осуществляет администратор ПК SafeERP. Функциональные модули ПК SafeERP интегрируются в действующие системы SAP NetWeaver. Системному программисту (далее – администратор SAP-систем) сначала

необходимо произвести установку комплекса, установить агенты на те системы SAP, контроль над которыми необходимо осуществлять. Правила установки ПК SafeERP приведены в документе «Руководство системного программиста по установке и удалению компонентов комплекса» 643.72410666.00038-01 32 01.

На этапе установки сервера управления и агентов ПК администратор ПК SafeERP должен получить у администратора SAP-систем необходимые исходные данные для установки значений некоторых параметров и заранее определить значения ряда параметров устанавливаемых компонентов ПК. Состав параметров, значения которых необходимо согласовать, приведен в документе «Руководство администратора» 643.72410666.00038-01 90 01.

Перед созданием нового пользователя ПК администратор ПК SafeERP должен настроить параметры функциональных подсистем ПК и только затем зарегистрировать нового пользователя в соответствии с разработанным в организации порядком, получить необходимые исходные данные:

- состав SAP-систем, которые будут контролироваться оператором ПК SafeERP;
- состав контролируемых параметров для каждой SAP-системы.

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

- взаимодействия администратора ПК SafeERP с администраторами SAP-систем (получение необходимых исходных данных и осуществление настроек SAP-систем);
- взаимодействия администратора ПК SafeERP с оператором ПК SafeERP (регистрация новых пользователей, модификация настроек, удаление пользователей ПК);
- реагирования администратора ПК SafeERP и оператора ПК SafeERP на факты выявленных нарушений ИБ в контролируемых SAP-системах.

3. ОПИСАНИЕ ЗАДАЧ

ПК SafeERP позволяет решать задачи основных требований по регистрации событий безопасности:

- регистрация изменений целостности программного обеспечения;
- регистрация уязвимостей информационной системы;
- определение событий безопасности, подлежащих регистрации, и их состава;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

3.1. Регистрация изменений целостности программного обеспечения

ПК SafeERP реализует задачу регистрации изменений целостности программного обеспечения путем контроля изменений объектов репозитория SAP-систем.

Контроль изменения целостности осуществляется путем расчета эталонного значения характеристики объекта при постановке его на контроль, расчета текущего значения характеристики объекта в соответствии с заданным расписанием и сравнения рассчитанного значения с эталонным значением.

В качестве характеристики объекта могут выступать:

- значение хэш-функции, рассчитанное по алгоритму, описанному в ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» – размер значения хэш-функции 256 бит;
- значение хэш-функции, рассчитанное по встроенному алгоритму систем SAP NetWeaver (MD5 – Message Digest 5) – размер значения хэш-функции 128-бит.

Выбор алгоритма расчета значения хэш-функции осуществляется на этапе установки сервера управления.

Расписание проверки целостности программных объектов задается администратором ПК SafeERP.

В случае обнаружения нарушения целостности контролируемых программных объектов в рабочей области оператора ПК SafeERP появляется индикация, информирующая о наличии изменений.

Оператор, контролирующий SAP-систему с помощью ПК SafeERP, может утвердить новое эталонное значение характеристики объекта, целостность которого была нарушена.

3.2. Регистрация уязвимостей информационной системы

ПК SafeERP реализует задачу регистрации уязвимостей в SAP-системах путем анализа и контроля:

- участков с недостатками ABAP-кода, отвечающих за безопасность использования прикладного программного обеспечения;
- уязвимостей, связанных с некорректной установкой и настройкой программного обеспечения.

ПК SafeERP реализует задачу анализа уязвимостей в SAP-системах путем применения сравнительных алгоритмов оценки, основанных на шаблонах сценариев возможных ошибок кода и шаблонных (безопасных) значениях параметров установки и настройки SAP-систем.

ПК SafeERP реализует задачу контроля уязвимостей в SAP-системах путем настройки запуска фоновых заданий для периодической проверки кода и параметров настройки. Период (расписание) проверки задается администратором ПК SafeERP .

Для маркировки результатов анализа используются индикаторы, отображающие статус критичности найденных уязвимостей. Так же в ПК SafeERP реализовано информирование о способах устранения выявленных уязвимостей.

3.3. Определение событий безопасности, подлежащих регистрации, и их состава

ПК SafeERP реализует задачу определения событий безопасности, подлежащих регистрации, путем предварительного выбора контролируемых объектов. Выбор программных объектов осуществляет администратор ПК SafeERP.

В ПК SafeERP реализовано определение следующих событий безопасности:

- изменение целостности программных объектов;
- доступ к объектам информации ограниченного доступа.

Возможный состав программных объектов для постановки на контроль целостности:

- ABAP-агент: пакеты, группы функций, параметры функциональных модулей, интерфейсы, логическая база данных, пакетный интерфейс, программы, классы;
- Java-агент: файлы, объекты EP, объекты MII;
- BO-агент: объекты инструментов Universe, CrystalRep, WebIntel;
- HANA-агент: объекты репозитория базы данных;

Возможный состав программных объектов для постановки на контроль доступа (только для ABAP-агента):

- транзакции;
- рабочие книги BI-системы;
- Java-приложения, связанные с данной ABAP-системой

3.4. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

ПК SafeERP реализует задачу просмотра результатов регистрации событий безопасности путем отображения собранных и обработанных данных в рабочей области оператора ПК SafeERP. Для способа маркировки событий используются индикаторы, отображающие статус проверки. Так же есть возможность отобразить (развернуть) более подробную информацию о полученных результатах. Состав отображаемых данных определяет администратор ПК SafeERP. (Оператору ПК SafeERP доступны только данные, собранные с контролируемых им SAP-систем).

После проведения системного анализа полученных результатов можно осуществить оперативные действия по реагированию на выявленные инциденты. Полученные результаты можно выгружать в файлы формата «docx» или «xlsm» и оперативно передавать ответственным лицам для дальнейшего анализа и устранения угроз.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными для ПК SafeERP являются:

- значения управляющих параметров, задаваемых администратором ПК SafeERP;
- данные, собираемые агентами с контролируемых SAP-систем, состав которых определяется произведенными настройками управляющих параметров функциональных модулей ПК SafeERP.

Формат, описание и способ кодирования значений управляющих параметров функциональных модулей ПК SafeERP описан в документе «Руководство администратора» 643.72410666.00038-01 90 01.

Выходными данными для ПК SafeERP являются:

- данные, отображаемые в рабочей области оператора ПК SafeERP, состав которых определяется значениями управляющих параметров функциональных модулей ПК SafeERP;
- данные, экспортируемые подсистемой отображения собранных данных, в файлы формата «docx» или «xlsm» по запросам оператора ПК SafeERP.

Формат, описание и способы отображения выходных данных в рабочей области оператора ПК SafeERP описаны в документе «Руководство оператора» 643.72410666.00038-01 34 01.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ИБ	–	информационная безопасность
ПК	–	программный комплекс

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

Изм.	Подп.	Дата