ООО «НОВЫЕ ОБАЛЧНЫЕ ТЕХНОЛОГИИ»

УТВЕРЖДЕН
501410.2914487-2016-01 34 01 ЛУ

Программное обеспечение «Комплекс средств защиты платформы МойОфис»

Руководство оператора

501410.2914487-2016-01 34 01

Листов 21

Москва, 2017

Подпись и дата | Инв. № дубл. | Взам. инв. № | Подпись и дата | Инв. № подл.

СОДЕРЖАНИЕ

АННОТАЦИЯ

Настоящий документ содержит руководство для оператора по работе с программным обеспечением «Комплекс средств защиты платформы МойОфис» (далее – Изделие, КСЗ МойОфис). Назначением документа является описание процесса настройки параметров доступа и отправки запросов пользователями программного обеспечения КСЗ МойОфис.

Документ разработан согласно ГОСТ 19.ххх Единая система программной документации (ЕСПД).

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Назначение программы

Изделие входит в состав программного комплекса «МойОфис» и предназначено для защиты информации от несанкционированного доступа исключительно в программном комплексе «МойОфис».

Изделие применяется для идентификации и аутентификации субъектов и объектов доступа, управления доступом субъектов доступа к объектам доступа, предотвращения ошибочных действий пользователей программного комплекса «МойОфис».

1.2 Функции программы

Субъектами доступа программного комплекса «МойОфис», контролируемыми Изделием, являются все внешние пользователи программного комплекса «МойОфис». Изделие выполняет идентификацию и аутентификацию указанных субъектов доступа при входе их в систему (программный комплекс «МойОфис»).

Объектами доступа программного комплекса «МойОфис», контролируемыми Изделием, являются файлы и папки, создаваемые (загружаемые) пользователями программного комплекса «МойОфис».

Изделие контролирует доступ наименованных субъектов к наименованным объектам доступа, указанным выше. Для каждой пары (субъект - объект) в программном комплексе «МойОфис» средствами Изделия задаются явные и недвусмысленные перечисления допустимых типов доступа (чтение, запись, удаление) данного субъекта к объекту.

Контроль доступа со стороны Изделия применим к каждому объекту и каждому субъекту (пользователю либо группе пользователей) программного комплекса «МойОфис».

Права изменять правила разграничения доступа предоставляются выделенным субъектам:

1) администраторам – в части формирования и ведения групп пользователей программного комплекса «МойОфис»;
2) пользователям, являющимся владельцами объектов доступа, - в части санкционирования доступа к объектам, созданным данными пользователями.

Изделие обеспечивает предотвращение ошибочных действий пользователей программного комплекса «МойОфис»: при попытке выполнения недопустимого действия пользователь получает сообщение об ошибке.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Требования к необходимым техническим средствам

В состав необходимых технических (аппаратных) средств для обеспечения функционирования Изделия должны входить:

1) Процессор – в соответствии с требованиями ОС, установленной на компьютер;
2) ОЗУ – не менее 1 Гб;
3) ЖМД – не менее 2 Гб, рекомендуется 4 Гб.

2.2 Требования к другим программам

КСЗ МойОфис применяется для защиты от несанкционированного доступа к информации, обрабатываемой с использованием следующих программных средств из состава программного обеспечения (ПО) «МойОфис»:

1) МойОфис Профессиональный (минимальная версия 2016.02);
2) МойОфис Частное Облако (минимальная версия 2016.02);
3) МойОфис Почта (минимальная версия 2016.02);
4) МойОфис Хранилище (минимальная версия 2016.02).

Также в состав необходимых программных средств для обеспечения функционирования Изделия необходимы:

1) Одна из двух операционных систем:
   - Red Hat Enterprise Linux Server 7.2;
   - CentOS 7.2.
2) Система управления базами данных (СУБД) PostgreSQL (Postgresql.org) версии 9.3.10, либо более новой версии начиная с версии 9.4.5 (открытая лицензия PostgreSQL);
3) Redisserver версии 2.8.21, либо более новой версии начиная с версии 3.0.2 (открытая лицензия BSD).
4) Стандартные библиотеки Perl (www.perl.org), включенные в версию 5.10.1-136.el6.x86_64 (открытая лицензия Artistic), указанные в Таблице 1.

Таблица 1 – Библиотеки Perl, необходимые для функционирования Изделия

№	Библиотека		Файлы библиотеки	
	Название	**Версия**	**Название**	**Размещение при эксплуатации**
1	Cache::Memcached	1.28	GetParser.pm	/usr/share/perl5/Cache/Memcached
			Memcached.pm	/usr/share/perl5/Cache
2	Carp	1.36	Carp.pm	/usr/share/perl5/

№	Библиотека		Файлы библиотеки	
	Название	Версия	Название	Размещение при эксплуатации
			Heavy.pm	/usr/share/perl5/Carp
3	Cassandra::Lite	0.4.0	Cassandra.pm	/usr/local/share/perl5/Cassandra
			Lite.pm	/usr/local/share/perl5/Cassandra
			Types.pm	/usr/local/share/perl5/Cassandra
4	ClamAV::Client	0.11	Client.pm	/usr/share/perl5/vendor_perl/ClamAV
			Config.pm	/usr/share/perl5/vendor_perl/ClamAV
5	Config::File	1.50	File.pm	/usr/local/share/perl5/Config
6	Crypt::CBC	2.29	CBC.pm	/usr/share/perl5/Crypt
7	Crypt::OpenSSL::AES	0.02	AES.pm	/usr/lib64/perl5/vendor_perl/Crypt/OpenSSL
			AES.so	/usr/lib64/perl5/vendor_perl/auto/Crypt/OpenSSL/AES
8	Data::Compare	1.2102	Compare.pm	/usr/share/perl5/vendor_perl/Data
			Properties.pm	/usr/share/perl5/vendor_perl/Data/Compare/Plugins/Scalar
9	Data::UUID	1.217	UUID.pm	/usr/local/lib64/perl5/Data
			UUID	/usr/local/lib64/perl5/auto/Data
			UUID.so	/usr/local/lib64/perl5/auto/Data/UUID
10	DateTime	1.19	DateTime.pm	/usr/lib64/perl5/vendor_perl
			Duration.pm	/usr/lib64/perl5/vendor_perl/DateTime
			Helpers.pm	/usr/lib64/perl5/vendor_perl/DateTime
			Infinite.pm	/usr/lib64/perl5/vendor_perl/DateTime
			LeapSecond.pm	/usr/lib64/perl5/vendor_perl/DateTime
			PP.pm	/usr/lib64/perl5/vendor_perl/DateTime
			PPExtra.pm	/usr/lib64/perl5/vendor_perl/DateTime
			DateTime.so	/usr/lib64/perl5/vendor_perl/auto/DateTime
11	DBD::Pg	2.15.1	Pg.pm	/usr/lib64/perl5/vendor_perl/Bundle/DBD
			Pg.pm	/usr/lib64/perl5/vendor_perl/DBD
			Pg.so	/usr/lib64/perl5/vendor_perl/auto/DBD/Pg
12	DBI	1.609	dbilogstrip	/usr/bin
			dbiprof	/usr/bin
			dbiproxy	/usr/bin
			DBI.pm	/usr/lib64/perl5/Bundle
			DBM.pm	/usr/lib64/perl5/DBD
			ExampleP.pm	/usr/lib64/perl5/DBD
			File.pm	/usr/lib64/perl5/DBD
			Gofer.pm	/usr/lib64/perl5/DBD
			Base.pm	/usr/lib64/perl5/DBD/Gofer/Policy
			classic.pm	/usr/lib64/perl5/DBD/Gofer/Policy
			pedantic.pm	/usr/lib64/perl5/DBD/Gofer/Policy
			rush.pm	/usr/lib64/perl5/DBD/Gofer/Policy
			Base.pm	/usr/lib64/perl5/DBD/Gofer/Transport
			null.pm	/usr/lib64/perl5/DBD/Gofer/Transport
			pipeone.pm	/usr/lib64/perl5/DBD/Gofer/Transport
			stream.pm	/usr/lib64/perl5/DBD/Gofer/Transport

№	Библиотека		Файлы библиотеки	
	Название	Версия	Название	Размещение при эксплуатации
			NullP.pm	/usr/lib64/perl5/DBD
			Proxy.pm	/usr/lib64/perl5/DBD
			Sponge.pm	/usr/lib64/perl5/DBD
			DBI.pm	/usr/lib64/perl5
			Changes.pm	/usr/lib64/perl5/DBI
			GetInfo	/usr/lib64/perl5/DBI/Const
			ANSI.pm	/usr/lib64/perl5/DBI/Const/GetInfo
			ODBC.pm	/usr/lib64/perl5/DBI/Const/GetInfo
			GetInfoReturn.pm	/usr/lib64/perl5/DBI/Const
			GetInfoType.pm	/usr/lib64/perl5/DBI/Const
			DBD.pm	/usr/lib64/perl5/DBI
			Metadata.pm	/usr/lib64/perl5/DBI/DBD
			FAQ.pm	/usr/lib64/perl5/DBI
			Execute.pm	/usr/lib64/perl5/DBI/Gofer
			Request.pm	/usr/lib64/perl5/DBI/Gofer
			Response.pm	/usr/lib64/perl5/DBI/Gofer
			Base.pm	/usr/lib64/perl5/DBI/Gofer/Serializer
			DataDumper.pm	/usr/lib64/perl5/DBI/Gofer/Serializer
			Storable.pm	/usr/lib64/perl5/DBI/Gofer/Serializer
			Base.pm	/usr/lib64/perl5/DBI/Gofer/Transport
			pipeone.pm	/usr/lib64/perl5/DBI/Gofer/Transport
			stream.pm	/usr/lib64/perl5/DBI/Gofer/Transport
			Profile.pm	/usr/lib64/perl5/DBI
			ProfileData.pm	/usr/lib64/perl5/DBI
			ProfileDumper	/usr/lib64/perl5/DBI
			ProfileDumper.pm	/usr/lib64/perl5/DBI
			Apache.pm	/usr/lib64/perl5/DBI/ProfileDumper
			ProfileSubs.pm	/usr/lib64/perl5/DBI
			ProxyServer.pm	/usr/lib64/perl5/DBI
			PurePerl.pm	/usr/lib64/perl5/DBI
			Roadmap.pm	/usr/lib64/perl5/DBI
			Nano.pm	/usr/lib64/perl5/DBI/SQL
			CacheMemory.pm	/usr/lib64/perl5/DBI/Util
			_accessor.pm	/usr/lib64/perl5/DBI/Util
			DBI.so	/usr/lib64/perl5/auto/DBI
			DBIXS.h	/usr/lib64/perl5/auto/DBI
			Driver.xst	/usr/lib64/perl5/auto/DBI
			Driver_xst.h	/usr/lib64/perl5/auto/DBI
			dbd_xsh.h	/usr/lib64/perl5/auto/DBI
			dbi_sql.h	/usr/lib64/perl5/auto/DBI
			dbipport.h	/usr/lib64/perl5/auto/DBI
			dbivport.h	/usr/lib64/perl5/auto/DBI
			dbixs_rev.h	/usr/lib64/perl5/auto/DBI

№	Библиотека		Файлы библиотеки	
	Название	Версия	Название	Размещение при эксплуатации
			dbixs_rev.pl	/usr/lib64/perl5
13	Digest::SHA	5.47	shasum	/usr/bin
			SHA.pm	/usr/lib64/perl5/Digest
			SHA.so	/usr/lib64/perl5/auto/Digest/SHA
14	File::Spec	0.7	Spec.pm	/usr/local/share/perl5/File
			Functions.pm	/usr/local/share/perl5/File/Spec
			Mac.pm	/usr/local/share/perl5/File/Spec
			OS2.pm	/usr/local/share/perl5/File/Spec
			Unix.pm	/usr/local/share/perl5/File/Spec
			VMS.pm	/usr/local/share/perl5/File/Spec
			Win32.pm	/usr/local/share/perl5/File/Spec
15	IO::String	1.08	String.pm	/usr/share/perl5/IO
16	IPC::Run	0.84	Run.pm	/usr/share/perl5/vendor_perl/IPC
			Debug.pm	/usr/share/perl5/vendor_perl/IPC/Run
			IO.pm	/usr/share/perl5/vendor_perl/IPC/Run
			Timer.pm	/usr/share/perl5/vendor_perl/IPC/Run
17	JSON::XS	2.27	json_xs	/usr/bin
			XS.pm	/usr/lib64/perl5/JSON
			Boolean.pm	/usr/lib64/perl5/JSON/XS
			XS.so	/usr/lib64/perl5/auto/JSON/XS
18	Mail::Sender	0.8.23	Sender.pm	/usr/share/perl5/vendor_perl/Mail
			Ext.pm	/usr/share/perl5/vendor_perl/Mail/Sender/CType
19	Module::Build	0.3500	config_data	/usr/bin
			Build.pm	/usr/share/perl5/Module
			Base.pm	/usr/share/perl5/Module/Build
			Compat.pm	/usr/share/perl5/Module/Build
			Config.pm	/usr/share/perl5/Module/Build
			ConfigData.pm	/usr/share/perl5/Module/Build
			Cookbook.pm	/usr/share/perl5/Module/Build
			Dumper.pm	/usr/share/perl5/Module/Build
			ModuleInfo.pm	/usr/share/perl5/Module/Build
			Notes.pm	/usr/share/perl5/Module/Build
			PPMMaker.pm	/usr/share/perl5/Module/Build
			Amiga.pm	/usr/share/perl5/Module/Build/Platform
			Default.pm	/usr/share/perl5/Module/Build/Platform
			EBCDIC.pm	/usr/share/perl5/Module/Build/Platform
			MPEiX.pm	/usr/share/perl5/Module/Build/Platform
			MacOS.pm	/usr/share/perl5/Module/Build/Platform
			RiscOS.pm	/usr/share/perl5/Module/Build/Platform
			Unix.pm	/usr/share/perl5/Module/Build/Platform
			VMS.pm	/usr/share/perl5/Module/Build/Platform
			VOS.pm	/usr/share/perl5/Module/Build/Platform
			Windows.pm	/usr/share/perl5/Module/Build/Platform

№	Библиотека		Файлы библиотеки	
	Название	Версия	Название	Размещение при эксплуатации
			aix.pm	/usr/share/perl5/Module/Build/Platform
			cygwin.pm	/usr/share/perl5/Module/Build/Platform
			darwin.pm	/usr/share/perl5/Module/Build/Platform
			os2.pm	/usr/share/perl5/Module/Build/Platform
			PodParser.pm	/usr/share/perl5/Module/Build
			Version.pm	/usr/share/perl5/Module/Build
			YAML.pm	/usr/share/perl5/Module/Build
20	Module::Info	0.31	module_info	/usr/bin
			pfunc	/usr/bin
			BUtils.pm	/usr/share/perl5/B
			Info.pm	/usr/share/perl5/B/Module
			Info.pm	/usr/share/perl5/Module
21	Module::Load::Conditional	0.30	Conditional.pm	/usr/share/perl5/Module/Load
22	Mouse	0.58	Mouse.pm	/usr/lib64/perl5/vendor_perl
			Exporter.pm	/usr/lib64/perl5/vendor_perl/Mouse
			Attribute.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta
			Class.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta
			Method.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta
			Accessor.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta/Method
			Constructor.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta/Method
			Delegation.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta/Method
			Destructor.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta/Method
			Module.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta
			Role.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta
			Composite.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta/Role
			Method.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta/Role
			TypeConstraint.pm	/usr/lib64/perl5/vendor_perl/Mouse/Meta
			Object.pm	/usr/lib64/perl5/vendor_perl/Mouse
			PurePerl.pm	/usr/lib64/perl5/vendor_perl/Mouse
			Role.pm	/usr/lib64/perl5/vendor_perl/Mouse
			Spec.pm	/usr/lib64/perl5/vendor_perl/Mouse
			Tiny.pm	/usr/lib64/perl5/vendor_perl/Mouse
			TypeRegistry.pm	/usr/lib64/perl5/vendor_perl/Mouse
			Util.pm	/usr/lib64/perl5/vendor_perl/Mouse
			MetaRole.pm	/usr/lib64/perl5/vendor_perl/Mouse/Util
			TypeConstraints.pm	/usr/lib64/perl5/vendor_perl/Mouse/Util
			Squirrel.pm	/usr/lib64/perl5/vendor_perl
			Role.pm	/usr/lib64/perl5/vendor_perl/Squirrel
			Mouse.pm	/usr/lib64/perl5/vendor_perl/Test
			Mouse.bs	/usr/lib64/perl5/vendor_perl/auto/Mouse
			Mouse.so	/usr/lib64/perl5/vendor_perl/auto/Mouse
			ouse.pm	/usr/lib64/perl5/vendor_perl

№	Библиотека		Файлы библиотеки	
	Название	Версия	Название	Размещение при эксплуатации
23	Net::RabbitMQ	0.2.0-1	RabbitMQ.pm	/usr/local/lib64/perl5/Net
			RabbitMQ.so	/usr/local/lib64/perl5/auto/Net/RabbitMQ
24	Readonly	1.03	Readonly.pm	/usr/share/perl5
24	Redis	1.978	Redis.pm	/usr/share/perl5/vendor_perl
			Hash.pm	/usr/share/perl5/vendor_perl/Redis
			List.pm	/usr/share/perl5/vendor_perl/Redis
			Sentinel.pm	/usr/share/perl5/vendor_perl/Redis
26	String:: HexConvert	0.01-1	HexConvert.pm	/usr/local/share/perl5/String
27	Test::Simple	1.001014	Builder.pm	/usr/share/perl5/vendor_perl/Test
			Scalar.pm	/usr/share/perl5/vendor_perl/Test/Builder/IO
			Module.pm	/usr/share/perl5/vendor_perl/Test/Builder
			Tester	/usr/share/perl5/vendor_perl/Test/Builder
			Tester.pm	/usr/share/perl5/vendor_perl/Test/Builder
			Color.pm	/usr/share/perl5/vendor_perl/Test/Builder/Tester
			More.pm	/usr/share/perl5/vendor_perl/Test
			Simple.pm	/usr/share/perl5/vendor_perl/Test
			Tester.pm	/usr/share/perl5/vendor_perl/Test
			Capture.pm	/usr/share/perl5/vendor_perl/Test/Tester
			CaptureRunner.pm	/usr/share/perl5/vendor_perl/Test/Tester
			Delegate.pm	/usr/share/perl5/vendor_perl/Test/Tester
			ok.pm	/usr/share/perl5/vendor_perl/Test/use
			ok.pm	/usr/share/perl5/vendor_perl
28	Time::HiRes	1.9721	HiRes.pm	/usr/lib64/perl5/Time
			HiRes.so	/usr/lib64/perl5/auto/Time/HiRes
29	URI::Escape::XS	0.08	XS.pm	/usr/lib64/perl5/vendor_perl/URI/Escape
			XS.bs	/usr/lib64/perl5/vendor_perl/auto/URI/Escape/XS
			XS.so	/usr/lib64/perl5/vendor_perl/auto/URI/Escape/XS
30	version	0.9912	vxs.so	/usr/lib64/perl5/vendor_perl/auto/version/vxs
			version.pm	/usr/lib64/perl5/vendor_perl
			regex.pm	/usr/lib64/perl5/vendor_perl/version
			vpp.pm	/usr/lib64/perl5/vendor_perl/version
			vxs.pm	/usr/lib64/perl5/vendor_perl/version

2.3 Условия применения в информационных системах

КСЗ МойОфис предназначен для защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и может применяться:

- в государственных информационных системах до 1 класса защищенности (включительно) в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных

информационных системах» (утверждены приказом ФСТЭК России от 11.02.2013 г. № 17 от 11.02.2013 г.);

- для обеспечения до 1 уровня защищенности (включительно) персональных данных в информационных системах персональных данных в соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены Приказом ФСТЭК России № 21 от 18.02.2013 г. № 21).

Эксплуатация КСЗ МойОфис в информационных системах персональных данных и государственных информационных системах должна осуществляться при условии принятия в указанных системах технических мер, определенных приказом ФСТЭК России от 18 февраля 2013 № 21 и приказом ФСТЭК России от 11 февраля 2013 г. № 17, по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При использовании КСЗ МойОфис в составе системы защиты информационной системы персональных данных 1 и 2 уровня защищенности и/или системы защиты информации государственной информационной системы 1 и 2 класса защищенности для обеспечения указанных выше мер должны применятся:

- межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 5 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;
- средства вычислительной техники не ниже 5 класса.

2.4 Настройка безопасной конфигурации среды функционирования

2.4.1 Подготовка целевой операционной системы

1) CentOS

- инсталлировать минимальный вариант CentOS рекомендуемой версии:
- настроить имя хоста, параметры сети.
- перевести SELinux в состояние Disabled.
- сконфигурировать внешний DNS. Убедиться, что ресолвится и доступен SMTP сервер FS (smtp.domain) и MAIL сервер (mail.domain).

2) Scientific Linux

- инсталлировать минимальный вариант Scientific Linux рекомендуемой версии;
- аналогично CentOS, настроить сетевые интерфейсы, hostnames;
- перевести SELinux в состояние Disabled.

2.4.2 Руководство по настройке безопасной конфигурации операционной системы

В данном подразделе представлен порядок настройки безопасной конфигурации операционной системы (ОС), используемой в качестве операционной платформы сервера МойОфис.

3) Выполнить установку ОС.

4) В настройках BIOS исключить загрузку ОС, кроме как с жесткого диска сервера, на который она была установлена. Принять меры по исключению вхождения пользователей в режим конфигурирования BIOS (например, с использованием парольной защиты).

5) Запустить менеджер пакетов и удалить следующие пакеты (с опцией --nodeps):

- gcc-4.4.7-4.el6.[x86_64/s390x].rpm
- gcc-c++-4.4.7-4.el6.[x86_64/s390x].rpm
- gcc-gfortran-4.4.7-4.el6.[x86_64/s390x].rpm
- gcc-gnat-4.4.7-4.el6.[x86_64/s390x].rpm
- gcc-java-4.4.7-4.[x86_64/s390x].rpm
- gcc-objc++-4.4.7-3.el6.x86_64.rpm
- gcc-objc-4.4.7-3.el6.x86_64.rpm
- gdb-7.2-60.el6.[x86_64/s390x].rpm
- gdb-gdbserver-7.2-60.el6.[x86_64/s390x].rpm.

Принять организационные меры по недопущению инсталляции указанных выше пакетов в операционной среде сервера.

6) Выполнить настройку сетевых сервисов.

```
cd /etc/sysconfig/network-scripts
vi ifcfg-eth0
vi ifcfg-eth1
```

7) Выполнить настройку учетных записей субъектов доступа:

а) Создать пользователя admin

```
useradd admin –u 500 -g users
```

б) Установить права администратора в ОС:

```
echo 'admin ALL=(ALL) NOPASSWD: ALL' >> /etc/sudoers
```

в) Для обеспечения защиты СУБД Postgresql следует использовать подключаемые модули аутентфикации (pam), которые предоставляет.

Разграничения прав доступа на уровне СУБД достигается ограничением среды функционирования – СУБД Postgresql. СУБД используется эксклюзивно, т.е содержит только базу метаданных МойОфис и предоставляет возможность обслуживания запросов:

- от имени служебного пользователя МойОфис – postges,
- локальных запросов.

Для конфигурирования следует отредактировать файл /etc/pam.d/postgresql должен включив следующие строки:

```
auth include password-auth
account include password-auth
```

Детально настройка безопасной конфигурации СУБД приведена в разделе 2.4.3.

8) Настроить подсистему регистрации и учета событий безопасности, используя правила настройки подсистемы регистрации событий безопасности.

При этом принять следующий рабочий перечень объектов и субъектов доступа:

Субъекты:

- Пользователь АЗИ,
- Выделенный пользователь СУБД potrges,

Объекты:

- Программа PostgreSQL.

9) сформировать файл правил аудита, обеспечивающий регистрацию следующих событий:

- вход (выход), а также попытки входа субъектов доступа на сервер;
- попытки загрузки (останова) операционной системы;

- подключение машинных носителей информации и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач) МойОфис;
- попытки доступа программных средств к каталогам и файлам МойОфис.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности:

- типа события безопасности,
- даты и времени события безопасности,
- идентификационная информация источника события безопасности,
- результат события безопасности (успешно или неуспешно),
- субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности

10) Выполнить скрытие файлов регистрации системных событий.

11) Настроить подсистему разграничения доступа, очистку внешней памяти в соответствии с руководством ОС.

12) Настроить подсистему контроля целостности.

а) Выполнить инсталляцию программы AIDE (Advanced Intrusion Detection Environment -- Среда для Обнаружения Вторжений с Расширенными Возможностями), предназначенной для подсчёта фактических контрольных сумм всех файлов операционной среды. Установка aide осуществляется выполнением команды:

```
yum install aide
```

б) Создать в системе конфигурационный файл aide.conf , скопировав файл, поставляемый в составе дистрибутива:

```
cp /usr/local/etc/aide.conf.sample /var/db/aide/aide.conf
```

в) Выполнить инициализацию базы данных aide:

```
aide –init
```

г) Проверить целостность файловой системы по построенной ранее базе данных с получением развёрнутого отчёта командой:

```
aide --compare
```

д) Подтвердить легитимность состояния файловой системы:

```
aide –update
```

2.4.3 Руководство по настройке безопасной конфигурации системы управления базами данных

В данном подразделе представлен порядок настройки безопасной конфигурации СУБД PostgreSQL, используемой для обеспечения работы сервера МойОфис.

Установку произвести в следующем порядке:

а) Путем набора команд в терминале (здесь и далее все указанные команды следует выполнять в терминале ELK) выполнить следующие команды:

```
useradd -d /var/lib/pgsql -s /dev/null -c PostgreSQL -u 88 postgres
cd /директория_содержащая_дистрибутив_СУБД
```

б) После чего выполнить последовательно команды:

```
chmod +x install.sh
./install.sh
```

в) Выполнить инициализацию БД:

```
sudo -u postgres initdb -D /var/lib/pgsql/data --locale=ru_RU.utf8
```

г) Настроить postgres, отредактировать конфигурационный файл

```
mcedit /var/lib/pgsql/data/postgresql.conf
listen_addresses = '*'
```

д) Настроить правила доступа к СУБД, отредактировав файл конфигурации postgresql (pg_hba.conf):

```
# TYPE DATABASE USER CIDR-ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all postgres pam
# IPv4 local connections:
# IPv6 local connections:
```

е) Запустить СУБД:

```
service postgresql start
```

ж) Создать роль admin в СУБД:

```
psql -U postgres -c "CREATE ROLE \"admin\" SUPERUSER CREATEROLE LOGIN;"
```

з) Установить драйвер QT:

```
rpm -ivh /opt/distr/qt46-postgresql-4.6.3-vniins2.i386.rpm –nodeps
```

и) Добавить запуск сервиса синхронизации времени и даты в автозапуск системы. Отредактировать файл конфигурации mcedit /etc/ntp.conf:

```
chkconfig ntpd on
```

а) Запустить сервис синхронизации времени и даты

```
service ntpd start
```

3 ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 Настройка времени блокировки пользователя

Настройка времени, в течение которого пользователь переходит в статус «заблокирован» и не имеет возможности осуществления входа в систему от своего имени, производится в файле `config.inc.default` в подзаголовке `# FailAttempts`.

Необходимо отредактировать значение параметра

```
fail_timeout = 300
```

где 300 – количество секунд, в течение которого пользователь находится в статусе «заблокирован».

3.2 Настройка интервала отслеживания неуспешных действий пользователя

Настройка времени, в течение которого система отслеживает совершение пользователем неуспешных действий, производится в файле `config.inc.default` в подзаголовке `# FailAttempts`.

Необходимо отредактировать значение параметра

```
fail_life_time = 3600
```

где 3600 – количество секунд, в течение которого система отслеживает совершение пользователем неуспешных действий.

3.3 Настройка числа неуспешных попыток авторизации

Число неуспешных (подряд) попыток авторизации, после которых пользователю предлагается ввести код CAPTCHA, производится в следующем файле:

```
/usr/local/lib64/perl5/PSync/API/.config.inc
```

Необходимо отредактировать значение параметра

```
fail_captcha_start = 1000000
```

где 1000000 – редактируемое число попыток авторизации.

Также данная настройка может быть выполнена в файле `config.inc.default` в подзаголовке `# FailAttempts`. Система считает оба конфигурационных файла, сначала `config.inc.default`, а затем `.config.inc` (если существует). Если параметр `fail_captcha_start` задан в обоих конфигурационных файлах, приоритетным является значение, заданное в файле `.config.inc`.

3.4 Настройка числа попыток входа в систему

Настройка максимально допустимого числа попыток входа в систему в течение периода, заданного параметром `fail_life_time`, производится в следующем файле:

`/usr/local/lib64/perl5/PSync/API/.config.inc`

Необходимо отредактировать значение параметра

```
fail_max_attempts = 10000000
```

где 10000000 – редактируемое число попыток авторизации.

Также данная настройка может быть выполнена в файле `config.inc.default` в подзаголовке `# FailAttempts`. Система считает оба конфигурационных файла, сначала `config.inc.default`, а затем `.config.inc` (если существует). Если параметр `fail_max_attempts` задан в обоих конфигурационных файлах, приоритетным является значение, заданное в файле `.config.inc`.

3.5 Настройка исключения блокировки доступа для внутренних адресов

Настройка адресов, являющихся для системы внутренними, доступ с которых не подлежит блокировке, производится в файле `config.inc.default` в подзаголовке `# FailAttempts`.

Необходимо отредактировать значение параметра

```
fail_ip_skip = 10.20.
```

где `10.20` – маска исключения адресов.

3.6 Настройка числа запросов за период с одного ip-адреса

Настройка допустимого числа запросов в течение `ddos_period` секунд с одного ip-адреса производится в файле `config.inc.default` в подзаголовке `# FailAttempts`.

Необходимо отредактировать значение параметра

```
ddos_attempts = 6000
```

где `6000` – число запросов в течение `ddos_period` секунд с одного ip-адреса.

3.7 Настройка допустимого периода получения запросов с одного ip-адреса

Параметр `ddos_period` означает период времени, в течение которого, при условии, что значение параметра `ddos_attempts` превысило допустимый лимит, получение запросов с

данного ip-адреса блокируется на `fail_timeout` секунд. Настройка данного параметра производится в файле `config.inc.default` в подзаголовке `# FailAttempts`.

Необходимо отредактировать значение

```
ddos_period = 3000
```

где `3000` – количество секунд, в течение которого система подсчитывает значение параметра `ddos_attempts`.

3.8 Настройка числа неверных попыток доступа с одного ip-адреса

Настройка допустимого числа неверных попыток доступа в течение `bruteforce_period` времени с одного ip-адреса производится в файле `config.inc.default` в подзаголовке `# FailAttempts`.

Необходимо отредактировать значение параметра

```
bruteforce_attempts = 3000
```

где `3000` – количество неверных попыток доступа в течение `bruteforce_period` времени с одного ip-адреса.

3.9 Настройка допустимого периода попыток доступа с одного ip-адреса

Параметр `bruteforce_period` означает период времени, в течение которого, при условии, что значение параметра `bruteforce_attempts` превысило допустимый лимит, доступ с данного ip-адреса блокируется на `fail_timeout` секунд. Настройка данного параметра производится в файле `config.inc.default` в подзаголовке `# FailAttempts`.

Необходимо отредактировать значение

```
bruteforce_period = 1000
```

где `1000` – количество секунд, в течение которого система подсчитывает значение параметра `bruteforce_attempts`.

3.10 Настройка аудита

Журнал аудита расположен в файле /var/log/fsapi.*

В конфигурации можно блокировать сессию. Кроме того, каждому пользователю можно указать его статус через административный вебинтерфейс, при помощи нашего api (set_user_status) или напрямую в БД postgresql.

Например, при помощи sql можно блокировать идентификаторы пользователей следующим образом:

```
su - postgres; psql -d fs_fedbst -c 'update users set status='606' where last_activity < 2678400'
```

Статусы:

```
USER_STATUS_CREATED    => 600;
USER_STATUS_ACTIVE        => 107;
USER_STATUS_SUSPENDED    => 606;
USER_STATUS_MARK_DELETED    => 111;
USER_STATUS_DELETED    => 666;
USER_STATUS_PROMISED    => 500;
USER_STATUS_DEBTOR        => 501;
USER_STATUS_PASSWORD_EXPIRED => 502;
```

4 СООБЩЕНИЯ ОПЕРАТОРУ

В процессе редактирования конфигурационных файлов оператор не получает сообщений от КСЗ. Сведения по результатам контроля ошибочных действий пользователей по вводу и передаче информации и предупреждение пользователей об ошибочных действиях осуществляется на формах Web-приложения.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводи-тельного документа	Под-пись	Дата
	изме-ненных	Заме-ненных	новых	Аннулиро-ванных					