ВИЗОР

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

описание программного обеспечения

Аннотация

Настоящий документ содержит общее описание Системы защиты информации (СЗИ) «Визор» версии **2016.Q2.R1** (далее - программный продукт).

Документ содержит сведения о назначении программного продукта, функциональных возможностях и технических и программных средствах, обеспечивающих функционирование программного продукта.

Содержание

Термины и определения

Автоматизированная информационная система – комплекс программных и технических средств, предназначенных для сбора, хранения, поиска и выдачи информации по запросам.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторизация – предоставление определённому субъекту или группе субъектов прав на выполнение определённых действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

Администратор информационной безопасности – сотрудник организации, которому предоставлены полномочия на управление системой обеспечения информационной безопасности.

Аудит – анализ накопленной Службой управления событиями безопасности информации о событиях, произошедших в информационных ресурсах организации, проводимый оперативно, в реальном времени или периодически.

Аутентификация – процедура проверки принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Безопасность информации (информационная безопасность) – состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования и т.п.

Генератор событий – реализуемый разработчиком программный компонент, выполняющий в информационном ресурсе задачи генерации событий и их регистрации посредством взаимодействия со Службой управления событиями безопасности.

Действия пользователя – завершенная последовательность взаимосвязанных автоматических действий модуля, связанных с обработкой информации, инициатором которой является пользователь.

Доступ к информации – получение субъектом возможности обработки информации, в частности, ознакомление, копирование или уничтожение, в том числе с помощью технических средств.

Журнал событий – входящее в состав Службы управления событиями безопасности централизованное хранилище зарегистрированных в хронологическом порядке событий, произошедших в информационном ресурсе в результате действий пользователей или технологических операций программных процессов.

Защита информации – комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

Защищаемый контур – среда функционирования одного или нескольких информационных ресурсов, к которым предъявляются требования по обеспечению информационной безопасности.

Идентификатор – уникальная последовательность символов, позволяющая однозначно идентифицировать субъекта в информационной ресурсе, предварительно присвоенная ему при прохождении процедуры регистрации.

Идентификация – процедура, в результате выполнения которой для субъекта доступа выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе.

Инициатор события – субъект, инициировавший в источнике выполнение последовательности действий, по результатам которых генерируется событие.

Контекст – набор уточняющих значений, которые (в случае необходимости) могут применяться для дополнительного ограничения области действия функции.

Информационный ресурс – см. Автоматизированная информационная система, Автоматизированная система.

Пароль – фактор аутентификации, обычно представляющий собой секретное слово или набор символов и используемый для подтверждения подлинности субъекта при его доступе к защищаемым данным.

Политика безопасности – совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

Протоколирование – процесс сбора и накопления Службой управления событиями безопасности информации о событиях, произошедших в информационных ресурсах, которые явным или косвенным образом могут влиять на нарушение конфиденциальности, целостности или доступности информации, обрабатываемой в этих информационных ресурсах.

Разрешение – подтверждение со стороны Службы управления доступом на выполнение субъектом в информационном ресурсе определенной функции (действия) в рамках обозначенной области действия (области действия, дополнительно ограниченной контекстом).

Роль – логическое объединение реализуемых в информационном ресурсе действий (функций), необходимых для выполнения субъектом взаимосвязанного круга задач.

Ролевая модель (модель безопасности модуля) – xml-документ, содержащий формализованное описание модели разграничения доступа к информационному ресурсу.

Сессия – временной промежуток, в течении которого разрешения субъекта считаются актуальными.

Событие – зафиксированный в некоторый момент времени результат действий пользователя или технологических операций, включая информационное взаимодействие с внешними системами, связанных с успешной или неуспешной обработкой информации, хранящейся в информационных ресурсах организации.

Субъект – пользователь (человек) или программный компонент (модуль, информационная система), осуществляющий доступ к информационным ресурсам, входящих в защищаемый контур.

Технологическая операция – завершенная последовательность взаимосвязанных автоматических действий модуля, связанных с обработкой информации, инициатором которой является сам модуль (внутренняя технологическая операция), другой модуль (внутреннее информационное взаимодействие) или внешняя система (внешнее информационное взаимодействие).

Фактор аутентификации – определенный вид информации, предоставляемый субъектом доступа для подтверждения своей подлинности при прохождении процедуры аутентификации.

Функция (действие) – завершенная последовательность автоматических операций, реализуемая в информационном ресурсе в рамках обозначенной области действия и направленная на достижение полезной для субъекта цели.

Назначение

Система защиты информации (СЗИ) «Визор» представляет собой набор служб безопасности, реализующих функции обеспечения информационной безопасности при организации контролируемого, коллективного доступа субъектов к информационным ресурсам организации, содержащих информацию ограниченного использования.

СЗИ «Визор» обеспечивает снижение рисков утечки информации ограниченного использования, а также минимизацию последствий, связанных с возможной утечкой информации, и предназначена для использования всеми информационными ресурсами, включенными в защищаемый контур, в качестве единого, централизованного механизма обеспечения информационной безопасности.

В зависимости от требований, предъявляемых в организации к обеспечению информационной безопасности информации ограниченного доступа, СЗИ «Визор» может быть, как единственным компонентом безопасности, так и входить в состав системы безопасности организации (например, Систем защиты персональных данных).

Функциональные возможности

Управление идентификационными данными:

- учет сведений о сотрудниках с сохранением истории изменений и возможностью прикрепления документов, на основе которых произведены изменения;
- поддержка групповых операций над сотрудниками;
- автоматическая блокировка учетных записей после достижения установленного количества дней неактивности пользователя;
- управление правами доступа сотрудников к информационным ресурсам на основе ролевой модели управления доступом;
- поддержка прав доступа сотрудников на время;
- управление служебными расследованиями в отношении сотрудников;
- управление жизненным циклом ролевой модели информационных ресурсов;
- работа с электронными заявками на доступ;
- управление политикой генерации идентификаторов учетных записей;
- ведение справочников организационной структуры, должностей, званий;
- управление паролями, включая возможность определения единой политики паролей;
- автоматическая синхронизация данных с Active Directory;
- возможность конфигурированию ролевой модели доступа к службам информационной безопасности без программирования;
- экспорт отчетов.

Управление доступом к информационным ресурсам:

- идентификация и аутентификация пользователей при доступе к информационным ресурсам по идентификатору и паролю;
- предотвращение доступа не идентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;

- блокирование учетной записи пользователя при превышении установленного числа попыток доступа;
- поддержка функции однократной аутентификации (Single Sign-On);
- разграничение доступа пользователей к информационным ресурсам в зависимости от назначенных прав доступа;
- сопряжение сведений о сотруднике с учетной записью субъекта, от имени которой он осуществляет доступ к информационным ресурсам;
- поддержка ограничения доступа в соответствии с графиком доступа;
- защита сетевых коммуникаций с использованием протокола SSL;
- протоколирование успешных и неуспешных попыток доступа пользователей к информационным ресурсам;
- принудительное завершение действия сессий безопасности пользователей.

Управление событиями безопасности:

- предоставление интерфейса для протоколирования событий, связанных с действиями пользователей в информационных ресурсах, а также в рамках информационного взаимодействия между системами;
- ведение журнала зарегистрированных событий;
- управление заданиями очистки журнала от событий, потерявших актуальность;
- предоставление пользовательских интерфейсов для поиска и аудита накопленной информации;
- экспорт отчетов.

Условия применения

Комплекс программно-технических средств программного продукта состоит из серверной части, рабочих мест пользователей и обслуживающего персонала.

Взаимодействие пользователей с программным продуктом осуществляется по технологии тонкого клиента.

Требования к серверной части

Требования к аппаратному обеспечению

Ниже представлены рекомендуемые требования к аппаратному обеспечению серверной части:

- сервер контроллера домена:
  - два процессора Pentium 4 с частотой 3 ГГц или выше;
  - 4 Гб ОЗУ;
  - 80 ГБ свободного места на жестком диске;
  - сетевой адаптер для подключения сервера к ЛВС по протоколам стека TCP/IP с полосой пропускания 1 Гбит/с;
- сервер приложений / баз данных:
  - процессор Intel Xeon ® E5-2680 2.7ГГц или аналогичный;
  - 8 Гб ОЗУ;
  - 300 ГБ свободного места на жестком диске;
  - сетевой адаптер для подключения сервера к ЛВС по протоколам стека TCP/IP с полосой пропускания 1 Гбит/с;

Вышеперечисленные средства вычислительной техники могут быть представлены виртуальными машинами с аналогичными характеристиками.

Требования к программному обеспечению

Ниже представлены рекомендуемые требования к программному обеспечению серверной части:

- сервер контроллера домена:
  - операционная система Microsoft Windows Server 2008 R2 Standard SP1, 64bit;
  - рекомендуется файловая система NTFS;
- сервер приложений / баз данных:
  - операционная система Microsoft Windows Server 2008 R2 Standard SP1, 64bit;
  - комплект разработчика приложений Oracle Java Development Kit версии 8u77, 64bit;
  - СУБД PostgreSQL версии 9.5.1;
  - Apache HTTPD версии 9.5.1;
  - Apache ActiveMQ 5.11.1;
  - WildFly AS 9.0.2.

Требования к рабочему месту пользователя

Требования к аппаратному обеспечению

Ниже представлены рекомендуемые требования к аппаратному обеспечению рабочего места пользователя:

- процессор Intel i3, 2GHz или аналогичный;
- 4 Гб ОЗУ;
- 50 ГБ свободного места на жестком диске;
- сетевой адаптер для подключения рабочей станции к ЛВС по протоколам стека TCP/IP с полосой пропускания не менее 100 Мбит/с;
- графический SVGA монитор с разрешением экрана 1280x1024x24bit;
- клавиатура и мышь.

Требования к программному обеспечению

Ниже представлены рекомендуемые требования к программному обеспечению рабочего места пользователя:

- операционная система Microsoft Windows 7 и выше;
- интернет-браузер Internet Explorer версии 11 и выше, либо Google Chome версии 44 и выше, Firefox Mozilla версии 39 и выше;
- программа просмотра документации в pdf–формате Adobe Acrobat Reader версии 9.0 и выше;
- программа для работы с электронными таблицами Microsoft Office Excel 2007 и выше.

Уровень подготовки пользователя

Пользователи должны обладать следующими навыками и знаниями:

- базовые навыки работы на персональном компьютере;
- навыки работы в операционной системе Windows;
- навыки работы с одним из браузеров: Internet Explorer, Google Chome, Mozilla Firefox;
- навыки работы с программой Microsoft Office Excel;
- знать предметную область.

Перед началом работы с программным продуктом пользователю рекомендуется ознакомиться с настоящим руководством.