X-Role

Описание системы

Руководство администратора

Системный интегратор	Центр противодействия кибератакам IZ SOC
+7 495 980 23 45	+7 495 980 23 45
market@infosec.ru	izsoc@infosec.ru
www.infosec.ru	www.izsoc.ru
Сервисный центр	Центр противодействия мошенничеству
+7 495 981 92 22 +7 495 980 23 45 доб. 06	+7 495 980 23 45
support@itsoc.ru	Пресс служба
www.itsoc.ru	pr@infosec.ru

Оглавление

Глоссарий

ИС	Информационная система
ЦС / Целевая Система	Информационная система, в которой управление учетными записями и правами доступа автоматизируется системой X-Role
БД	База данных
ОШС	Организационно-штатная структура, загруженная в систему X-Role. ОШС X-Role состоит из Подразделений, Должностей и Сотрудников
Подразделение	Структурная единица ОШС, например, «Отдел продаж» или «Отдел бухгалтерского учёта»
Должность	Структурная единица ОШС. Например, «Специалист в отделе продаж» или «Руководитель отдела бухгалтерского учёта»
Сотрудник	Физическое лицо, назначенное на определенную Должность. Например, «Петров Сергей на Должности Специалист в отделе продаж»
Учётная запись	В настоящем документе это объект системы X-Role, хранящий информацию об учетной записи пользователя в Целевой системе
Группа учетных записей	В настоящем документе это объект системы X-Role, хранящий информацию об объектах Целевых систем, которые группируют учетным записи в этих системах и могут предоставлять групповой доступ к ресурсам Целевых систем. Например, Группа учетных записей может хранить информацию о таких объектах ЦС как «Учетная запись группы» в Active Directory или «Роль» в SAP ERP
Ресурс	Объект системы X-Role, хранящий описание ресурсов Целевой системы, доступ к которым управляется или контролируется Системой X-Role Ресурсы могут объединяться в категории Ресурсов для упрощения их поиска и настройки
Тип ресурса	Признак, объединяющий Ресурсы одной Целевой системы, используемый в системе X-Role для группировки, фильтрации и поиска. Для каждой Целевой системы существует свой перечень Типов ресурсов. Например, система «Домен Active Directory» содержит Тип Ресурса - «Подразделение AD», система «Почтовый домен MS Exchange» - «Почтовый ящик» и «Почтовый домен», система «Сервер Windows» - «Сервер», «Каталог», «Файл», «Принтер», «Разделяемый каталог», «Разделяемый принтер», «Разделяемое устройство»
Субъект доступа	Учетная запись или Группа учетных записей
Организационная единица	Объект системы X-Role, хранящий описание каталога учетных записей в Целевых системах Например, Организационная единица может хранить информацию об объекте «Организационная единица» в Active Directory
Право доступа	Объект системы X-Role, хранящий информацию об определенном праве доступа к ресурсу Целевой системы. Для каждого Типа ресурсов существует свой перечень Прав доступа Например, для Типа ресурса «Каталог» по умолчанию существуют следующие Права доступа: «Чтение атрибутов», «Создание файла», «Выполнение файла» и другие
Агент/ Коннектор	Программный модуль системы X-Role, обеспечивающий контроль изменения объектов Целевой Системы и прав доступа к ним Агенты состоят из «серверной части», которая является подключаемым модулем сервера X-Role, и «выносной части», устанавливаемой как отдельное программное обеспечение Для некоторых Целевых Систем, требуется выполнять установку Агента на сервер Целевой Системы Агенты могут быть организованны в иерархию, в соответствии с которой могут использоваться Учетные записи нижестоящего Агента

IIS	Веб-сервер, который используется пользовательским веб-приложением и сервером X-Role для связи с Java коннектор-сервером и агентами
Java коннектор-сервер	Компонент системы X-Role. Обеспечивает программную среду для работы конекторов целевых систем, разработанных на языке Java

Введение

Данный документ предназначен для администраторов продукта X-Role. В документе изложено общее описание и возможности системы X-Role.

Возможности системы

Аналитическая система X-Role реализует управление безопасностью в различных информационных системах. Система предоставляет решения по анализу и управлению неструктурированными данными компании.

Система обеспечивает:

- визуальное отображение организационно-штатной структуры (ОШС) компании;
- предоставление актуальной информации о текущих правах доступа пользователей;
- контроль за изменениями в структуре ОШС и доступе сотрудников;
- выявление подозрительного доступа и ошибок в предоставлении доступа сотрудникам;
- рассылка уведомлений при получении пользователями подозрительного доступа к ресурсам;
- возможность создавать и тестировать ролевые модели доступа;
- оценка готовности компании к внедрению IDM системы.

Использование системы позволит:

- проводить ревизию прав пользователей;
- снизить риски, вызванные наличием избыточного доступа;
- выполнять требования регуляторов по контролю доступа и прав в информационных системах;
- хранить историю доступов и прав в информационных системах;
- оптимизировать выдаваемые доступы.

Принцип работы

Настройка системы

Работа с системой X-Role начинается с импорта информационных данных, доступ к которым будет контролироваться, и организационно-штатной структуры (ОШС) компании.

Система X-Role позволяет загружать информационные данные и данные ОШС из следующих источников и информационных систем:

- данные ОШС:
  - система "1С: Предприятие";
  - система SAP.
- информационные данные:
  - ресурсы Active Directory, Windows Server и Exchange;
  - система SharePoint;
  - система "1С: Предприятие";
  - система SAP.

Информационные данные импортируются в систему X-Role с помощью специализированных агентов и коннекторов.

Система X-Role позволяет импортировать следующие данные:

- данные учетных записей сотрудников: ФИО сотрудников;
- данные сотрудников: подразделение, должность, руководитель;
- данные групп учетных записей: системное наименование группы, область действия, тип группы;
- информация о контролируемых ресурсах:
  - права доступа к ресурсам;
  - тип ресурса;
  - путь к ресурсу;
  - владелец ресурса.

Импорт возможен в двух режимах:

- инкрементальный: системе X-Role передаются только изменения произошедшие в информационной системе с момента предыдущего импорта;
- полный: системе X-Role передаются все актуальные данные.

После загрузки информационных данных и данных ОШС, система X- Role устанавливает связи между сотрудниками компании и учетными записями.

Сопоставление учетных записей с сотрудниками может выполняться как в автоматическом режиме, так и в ручном или с помощью заранее подготовленного текстового файла (см. подробнее в документе "Руководство по установке и настройке", глава "Связывание сотрудников с учетными записями сотрудников").

Работа с системой

После загрузки и сопоставления информационных данных и ОШС, на главной странице пользовательского веб-приложения X-Role отобразится сводная информация по количеству загруженных информационных данных и данных ОШС:

- общее количество загруженных информационных данных: учетных записей, групп учетных записей и ресурсов;
- общее количество данных ОШС: подразделений и сотрудников;
- количество неиспользуемых ресурсов;
- статистика по ОШС:
  - количество сотрудников, не связанных с учетными записями;
  - количество учетных записей, не связанных с сотрудниками;
  - наличие незаблокированных учетных записей уволенных сотрудников.

На странице с описанием текущей модели доступа отображаются структуры ОШС и информационных ресурсов.

ОШС отображается в виде иерархического дерева от названия компании к подразделениям и сотрудникам подразделений. Поиск сотрудников можно производить как с помощью различных фильтров (например, по части ФИО), так и путем нахождения сотрудника в иерархическом дереве ОШС. При выборе сотрудника отображаются ресурсы, к которым сотрудник имеет доступ. Выбор нескольких сотрудников позволяет сравнивать их доступ.

Ресурсы отображаются в виде иерархического дерева от названий информационных систем, которым принадлежат ресурсы, к самим ресурсам. Поиск ресурсов происходит аналогично поиску сотрудников. При выборе ресурса отображаются сотрудники, которые имеют доступ к ресурсу, и их права доступа.

На странице с описанием текущей модели ОШС при выборе сотрудника отображаются учетные записи, с которыми связан сотрудник.

Построение ролевой модели доступа

Ролевая модель доступа служит для оптимизации предоставления доступа сотрудникам, имеющих схожие права доступа к ресурсам. Оптимизация достигается путем замены индивидуального доступа сотрудников на доступ через роли.

Ролевая модель создается на основе набора ролей, сформировываемых автоматически при указаний правил, по которым будет осуществляться поиск идентичного доступа сотрудников (например, «более 75% сотрудников подразделения X имеют доступ к ресурсу Y»). Полученная ролевая модель может редактироваться администратором, например, путем редактирования ролей или добавлением ролей из других ролевых моделей.

После построения ролевой модели на главной странице веб-приложения отображается информация о количестве ресурсов, доступ к которым предоставляется через роли.

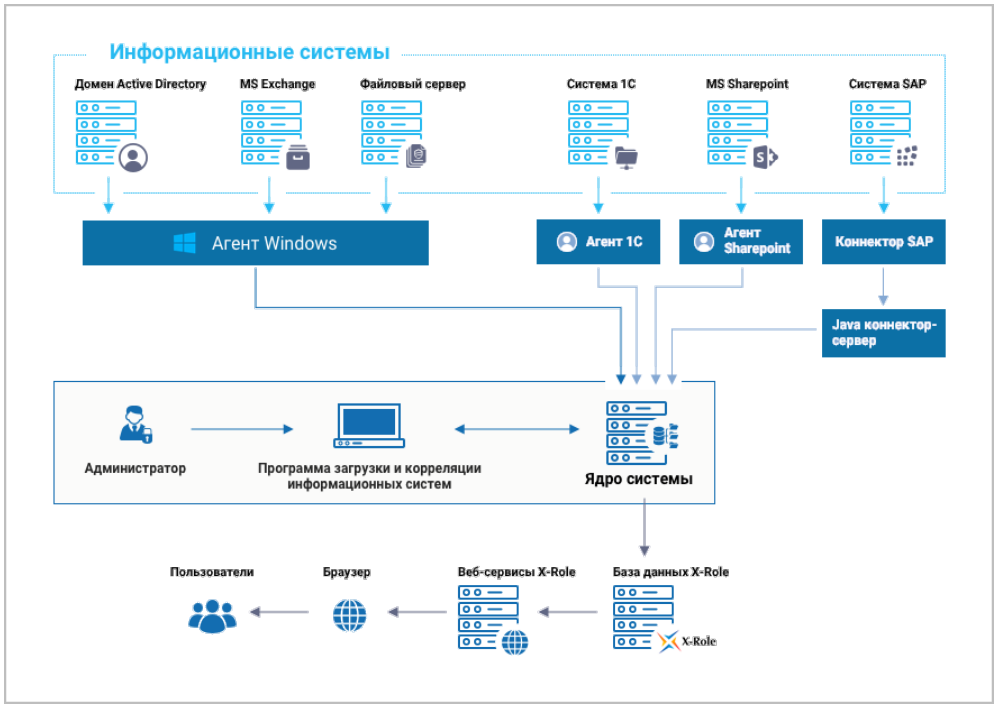
Сравнение ролевых моделей доступа

Система X-Role позволяет проводить сравнение разных ролевых моделей с одинаковым набором ресурсов.

При сравнении ролевых моделей указываются различия между ролевыми моделями в доступе к информационным ресурсам, а так же ресурсы и сотрудники, у которых существуют различия ролевого доступа.

Архитектура системы

Архитектура системы X-Role представлена на рисунке:



Система X-Role состоит из следующих компонентов:

- ядро системы;
- база данных;
- программа загрузки и корреляции данных информационных систем;
- пользовательское веб-приложение;
- агенты и коннекторы информационных систем.

Ядро системы и база данных

Ядро системы X-Role координирует работу остальных компонентов системы и обеспечивает обмен данными между ними.

Информация об объектах ИС и системы X-Role хранится в базе данных. Доступ к базе данных обеспечивается централизованно через ядро системы.

В ядре системы при помощи агентов и коннекторов обрабатывается информация о структуре ОШС контролируемой системы.

Программа загрузки и корреляции данных ИС

Программа загрузки и корреляции данных ИС представляет собой Windows-приложение, предназначенное для загрузки ОШС из кадровых источников и настройки системы X-Role. Доступ к приложению имеют только администраторы системы X-Role.

Пользовательское веб-приложение

Пользовательское веб-приложение – приложение на веб-сервере IIS. Пользователи осуществляют доступ к веб-приложению X-Role со своих рабочих мест через Web-интерфейс.

Веб-приложение предназначено для:

- отображения информации об организационно-штатной структуры компании:
  - ФИО сотрудников;

    - подразделения компании;
    - учетные записи и группы учетных записей сотрудников;
    - учетные записи, не связанные с сотрудниками и связанные с уволенными сотрудниками компании;
    - сотрудники, не связанные с учетными записями.
- отображения информации об информационных ресурсах компании:
    - текущий доступ сотрудников к ресурсам;
    - подозрительный доступ сотрудников к ресурсам;
    - ресурсы, к которым сотрудники не имеют доступа.
- контроля за изменениями в структуре ОШС и доступе сотрудников;
- генерации ролевых моделей доступа;
- сравнения созданных ролевых моделей доступа;
- создания различных отчетов о доступе сотрудников.

Агенты и коннекторы

Агенты и коннекторы — это программные модули, которые обеспечивают получение информации об объектах информационных систем и правах доступа к ним.

Для каждой информационной системы необходимо зарегистрировать соответствующий агент или коннектор.

Агент устанавливается как непосредственно на сервер целевой системы, так и на любой сервер сети, в зависимости от возможностей программного интерфейса целевой системы и архитектуры агента.

Коннектор устанавливается на Java коннектор-сервере. Java коннектор- сервер включает в себя сервер приложений, который обеспечивает программную среду для работы конектора, и СУБД для хранения данных коннектора.

Агент Windows

Агент Windows предназначен для контроля доступа к ресурсам Active Directory, объектам почтовой системы Exchange и серверов под управлением ОС Windows 2008/2012.

Агент имеет собственную локальную БД, в которой хранится информация о контролируемых объектах.

Контролируемая номенклатура объектов ИС

Субъекты и объекты доступа, контролируемые агентом, разделены по платформам "Сервер Windows", Active Directory и дочерним агентом Exchange.

Субъекты доступа — кому предоставляется доступ.

Объекты доступа — к чему предоставляется доступ.

Платформа "Сервер Windows"

К субъектам доступа платформы Сервер Windows относятся:

- встроенные и локальные группы серверов Windows;
- локальные пользователи серверов Windows.

Объектами доступа являются следующие ресурсы ИС:

- серверы Windows;
- кластеры серверов Windows;
- локальные каталоги серверов Windows;
- разделяемые каталоги серверов Windows;
- локальные принтеры;
- разделяемые принтеры;
- разделяемые устройства серверов Windows.

Платформа Active Directory

К субъектам доступа платформы Active Directory относятся:

- встроенные, локальные, глобальные и универсальные группы домена Active Directory;
- специальные контекстные группы пользователей;
- пользователи домена Active Directory.

Объектами доступа являются подразделения Active Directory.

Агент может контролировать как полностью домен Active Directory, так и отдельные контейнеры Active Directory.

На серверах, в том числе контроллерах домена, контролируются файлы и папки, а при использовании файловой системы NTFS — и права доступа к ним (дескриптор безопасности). По умолчанию контролируются только папки, к которым предоставлен общий доступ по сети.

Почтовая система MS Exchange

В качестве субъектов доступа используются следующие категории объектов Active Directory:

- пользователи домена (Domain users);
- группы (Groups);
- контакты (Contacts).

Объектами доступа для пользователей домена могут быть как почтовые ящики, так и адреса электронной почты. Для двух других категорий объектами доступа могут быть только адреса электронной почты.

Агент 1С

Агент 1С предназначен для контроля над правами доступа пользователей к объектам метаданных системы "1С: Предприятие" (далее — системы). Агент выполняет следующие функции:

- получение данных о доступе пользователей к объектам метаданных системы;
- контроль прав доступа пользователей системы к объектам метаданных.

В соответствии с настраиваемым расписанием агент получает от системы следующие данные:

- роли;
- учетные записи пользователей и их роли;
- объекты метаданных;
- права доступа ролей к объектам метаданных.

Права доступа к различным типам объектов метаданных системы и их ограничение задаются ролями. Субъектом доступа являются учетные записи пользователей. В зависимости от типа используемой платформы "1С: Предприятие" контролируемый набор прав доступа к какому-либо объекту может изменяться.

Агент SharePoint

Агент предназначен для контроля над правами доступа пользователей к ресурсам прикладной системы MS Office SharePoint Server версий 2007, 2010, 2013.

Агент выполняет следующие основные функции:

- получение данных о доступе пользователей к объектам системы SharePoint;
- контроль прав доступа пользователей системы SharePoint:
  - предоставление ролей SharePoint структурам ОШС. В качестве ОШС могут выступать учетные записи и группы AD или собственная ОШС системы SharePoint. При использовании в качестве ОШС учетных записей и групп AD необходимо установить агент Windows.

- права доступа ролей SharePoint к ресурсам системы SharePoint.

Для контроля и управления доступом к ресурсам системы SharePoint используются субъекты и объекты доступа.

Субъектами доступа являются:

- доменные учетные записи пользователя;
- доменные группы учетных записей.

Объектами доступа являются ресурсы следующих типов:

- сайты;
- списки;
- папки;
- элементы списка;
- файлы.

Коннектор SAP

Коннектор SAP предназначен для контроля доступа к объектам системы SAP ABAP.

Коннектор выполняет следующие функции:

- получение данных о доступе пользователей к объектам системы SAP ABAP;
- контроль прав доступа пользователей в системе SAP ABAP.

Коннектор SAP обеспечивает загрузку данных о пользователях, ролях и связи пользователей с ролями системы SAP ABAP.

В случае если у пользователя в системе SAP ABAP есть групповые (composite role) и дочерние им роли, то при загрузке в систему пользователям присваиваются только групповые роли.

Соответствие объектов системы SAP ABAP и системы X-Role:

Объект системы SAP ABAP	**Объект системы X-Role**
Имя пользователя (поле User)	Системное имя учетной записи
Имя роли (поле Role)	Системное имя роли

Коннектор устанавливается на Java коннектор-сервере. Java коннектор-сервер включает в себя сервер приложений, который обеспечивает программную среду для работы конектора и СУБД для хранения данных коннектора.

В комплект поставки Java коннектор-сервера входит:

- сервер приложений JBoss Enterprise Application Server версии 6.2.0;
- настроенная СУБД H2;
- набор библиотек для разработки новых коннекторов;
- документация для разработчика (JavaDoc);
- коннектор SAP (включая исходные коды).