Ankey IDM

Ключевые особенности и интересные детали реализованных проектов

Иван Корешков, менеджер по продукту

GIS
ГАЗИНФОРМ
СЕРВИС

Санкт-Петербург +7 (812) 677-20-53 sales@gaz-is.ru www.gaz-is.ru

Покрытие ряда требований регуляторов

- **Стандарт ГОСТ:** Р 57580.1-2017 (ЗИ)
- **ФЗ:** №149, 152, 187 (ЗИ, ИСПДн)
- **Указ Президента РФ:** №166 об обеспечении технологического суверенитета

- **Приказы ФСТЭК:** №17, 21, 31, 239

- **ISO 27001 / ГОСТ 27001:** контроль предоставления полномочий и их пересмотр;

- **В реестре отечественного ПО**
- **Сертификат ФСТЭК №4107**

- **PCI DSS / СТО БР ИББС:** контроль создания, изменений и удаления данных ID; отзыв и пересмотр прав доступа

Покрываемые меры приказов ФСТЭК

АНЗ.5: Парольные политики, разграничение доступа

АУД.0: Политика аудита безопасности

АУД.10, АУД.11: Проведение аудитов безопасности

ИАФ.0, ИАФ.5, ИАФ.6: Идентификация и аутентификация пользователей

ИАФ.6: Идентификация внешних пользователей

УПД.1, УПД.2, УПД.4, УПД.5: Управление доступом, реализация модели доступа, разделение полномочий, назначение минимальных наборов прав

	Приказы			
	№17	№21	№31	№239
АНЗ.5	✓	✓		
АУД.0			✓	✓
АУД.10, АУД.11			✓	✓
ИАФ.0, ИАФ.5, ИАФ.6			✓	✓
ИАФ.6	✓	✓		
УПД.1, УПД.2, УПД.4, УПД.5	✓	✓	✓	✓

Покрываемые меры ГОСТ 57580.1-2017

Безопасность финансовых (банковских) операций.
Защита информации финансовых организаций.

Комплекс Ankey IDM покрывает 27 мер УЗП (ГОСТ 57580.1),

в т.ч. обязательных

Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.1	Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями	Т	Т	Т
УЗП.2	Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа	О	О	Т
УЗП.3	Контроль отсутствия незаблокированных учетных записей: - уволенных работников; - работников, отсутствующих на рабочем месте более 90 календарных дней; - работников внешних (подрядных) организаций, прекративших свою деятельность в организации	О	О	Т

Ключевые отличия комплекса Ankey IDM

Поддержка множественных трудоустройств

и сопровождение минимальных прав доступа для автоматизации назначения/отзыва доступов при совместительстве

Самообслуживание, аудит и сертификация доступов призваны обеспечить управление и контроль доступов гибким и удобным для пользователей и администраторов систем

Поддержка доменной аутентификации и иных средств

и возможность использования систем и служб Identity Provider для реализации единой точки входа

Обширные возможности интеграции

со смежными ИТ и ИБ системами:

SIEM, ITSM, SSO, PAM, Vault, NAC, SOAR для реализации «купола» безопасности

Поддержка популярного ПО

1С
ALD Pro
NAUMEN
DIRECTUM
АЙТИБАСТИОН
Identity Blitz
Битрикс24

Microsoft Active Directory
Exchange
Jira Software
БОСС КАДРОВИК
INDEED ID
SAPERION
Jatoba
VK WorkMail

CommuniGate Pro
Docsvision
CHECK POINT
opentext
Skype for Business
Red Hat Enterprise Linux
ASTRA LINUX
KEYCLOAK

SAP
MDaemon
BELSOFT
SafeERP
MAIL.RU ДЛЯ БИЗНЕСА
360
РЕДОС
alt linux

Универсальные коннекторы

SQL
{ REST:API }
PowerShell
SSH
SOAP
OpenICF

Не нашли систему на этом слайде – напишите нам: sales@gaz-is.ru

Любые корпоративные службы каталогов

Альт Домен

Microsoft Active Directory

В Active Directory поддерживаем мультидоменность

ALD Pro

Ankey IDM сертифицирован для работы с ALD Pro

РЕДАДМ

А также поддерживаем решения, реализованные на популярных протоколах:

SAMBA

Включая AD DC

OpenLDAP

FreeIPA

Партнеры IAM-сферы

Identity Blitz — Технологический партнер (SSO, MFA, ЕСИА)

MULTIFACTOR — Сертификат совместимости (SSO, MFA)

АЙТИБАСТИОН — Сертификат совместимости (PAM)

INDEED ID — Сертификат совместимости (ESSO)

Не нашли систему на этом слайде – напишите нам: sales@gaz-is.ru

Реализованные проекты

Программный комплекс Ankey IDM установлен более чем в 40 компаниях России и СНГ со штатом сотрудников от 720 до 300 000 человек

Показатели на реализованных проектах (на одну инсталляцию):

Максимальное количество подключенных информационных систем: более 1 100 систем

Максимальное количество сотрудников под управлением: около 300 000

Максимальное количество сформированных ролей: свыше 1 500 000

Максимальное число оформленных заявок в системе за сутки: 58 000 заявок

Максимальный простой системы: 8 часов (проведение регламентных работ)

Бизнес-кейсы, #1

CVE-2022–26923 – повышение привилегий user вплоть до domain admin

Требуется времени на закрепление и эксплуатацию – около 7 минут

Время обнаружение SIEM-ом – в пределах 1-2 минут

Время реагирования (блокировка УЗ, шлюзов) , сессий – 2-5 минут с момента обнаружения

Время обнаружения и реагирования IDM – 3 минуты, включая блокировку УЗ, отзыв сессий (Kerberos), и передачу информации об инциденте в ИБ

Бизнес-кейсы, #2

Компрометация УЗ – ведущий менеджер в отпуске

Системы класса IDM – не использовались

Компрометация УЗ облачной почты

Сбор информации о стиле переписок, сбор шаблонов документов

Ведущий менеджер в отпуске с оповещением ключевых заказчиков контрагента

*«Вы интересовались этим решением – при оплате до конца недели скидка **60%**, обновленный счет с ограниченным сроком действия - во вложении»*

Прямой ущерб порядка 60 млн. рублей. Принято решение о закупке и внедрении Ankey IDM

Бизнес-кейсы, #3

Крупная инсталляция – около 300 тысяч данных о сотрудниках

Система класса IDM - *** IM**

Скорость первичной обработки кадровых источников около 5 суток

Риски, связанные с «западностью» вендора

В ходе тестирования Ankey IDM показал сроки
обработки аналогичного объема данных – **около 5 часов**

Принято решение о переходе на Ankey IDM

Скорость, оптимизация, российское ПО и надежный вендор

Бизнес-кейсы, #4

Многолетняя инсталляция с **** IM, многое реализовано силами внутренней разработки**

«Тормоза» и зависание решения, большая нагрузка на ИТ-службу сопровождения

Срок обследования, уточнения функциональностей и добавления модулей в Ankey IDM – около 1,5 лет

В ходе проекта тестирования создан один из самых высокопроизводительных IDM-проектов в РФ. Отказоустойчивость N+2

«Наконец-то мы видим, что система работает без визуальных «зависаний»

Принято решение о переводе системы управления УЗ и доступами на Ankey IDM

Ankey IDM разворачивается на любом уровне инфраструктуры (от «все в одном» до контейнеризации)

Бизнес-кейсы, #5

Проект международной зоны *«Нам нужен IDM, но компетенций недостаточно»*

1,5 года сбора требований, основной объем напоминает популярное решение ******** IDM

Результатом совместного взаимодействия между вендором и интегратором - проект запущен. После полугода уточнений и совещаний – в ходе разработки Ankey IDM реализуется дорожная карта с учетом всех пожеланий заказчика, интегратор проводит имплементацию решения в инфраструктуре Заказчика

Более 80 объективно-полезных фич принято в дорожную карту Ankey IDM
И общих пожеланий к текущей функциональности – более 200

Плотное взаимодействие вендор-интегратор, отзывчивость вендора

Вопрос-ответ?

Ankey IDM

СПАСИБО ЗА ВНИМАНИЕ

+7 (812) 677-20-53

sales@gaz-is.ru