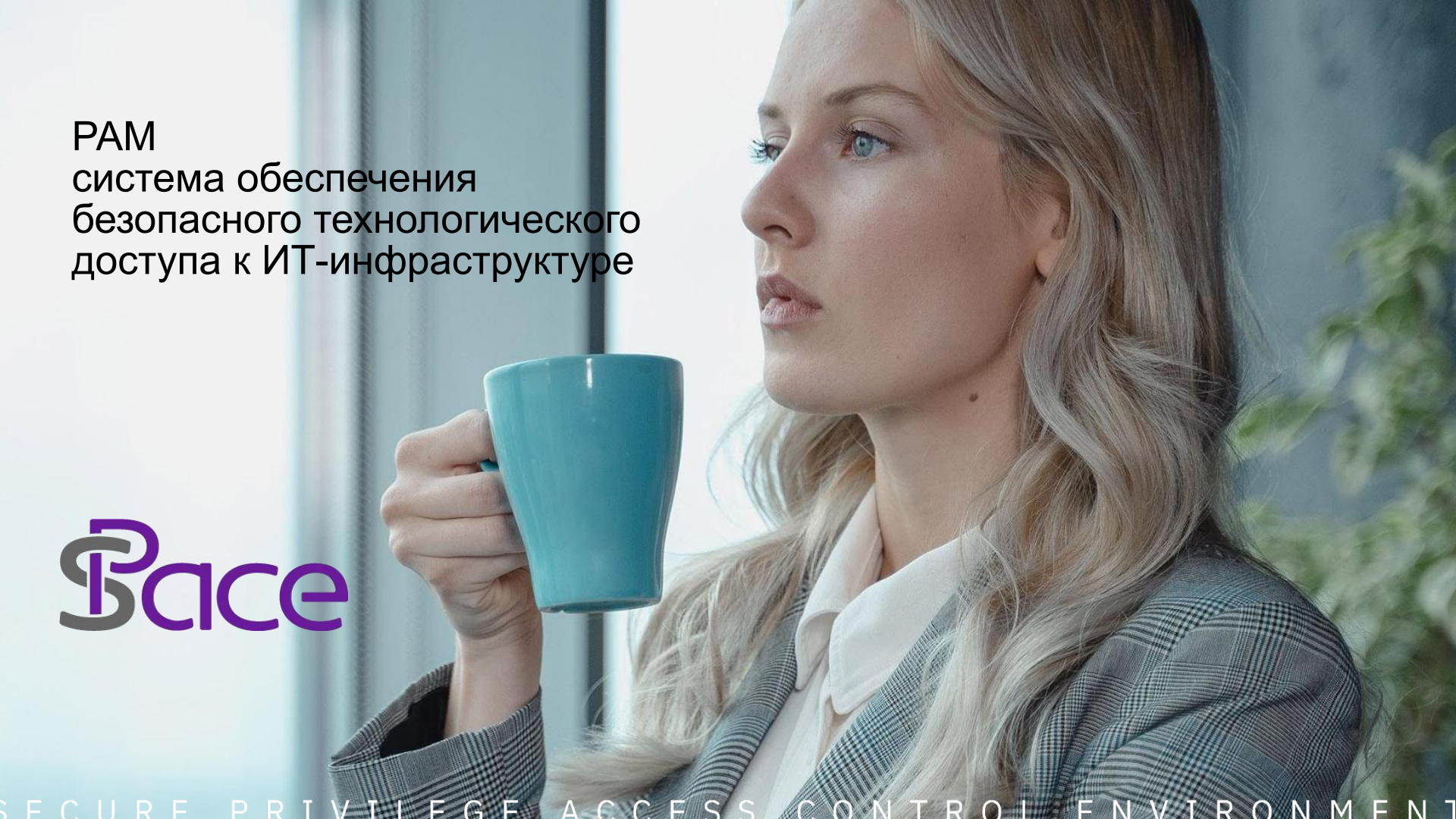
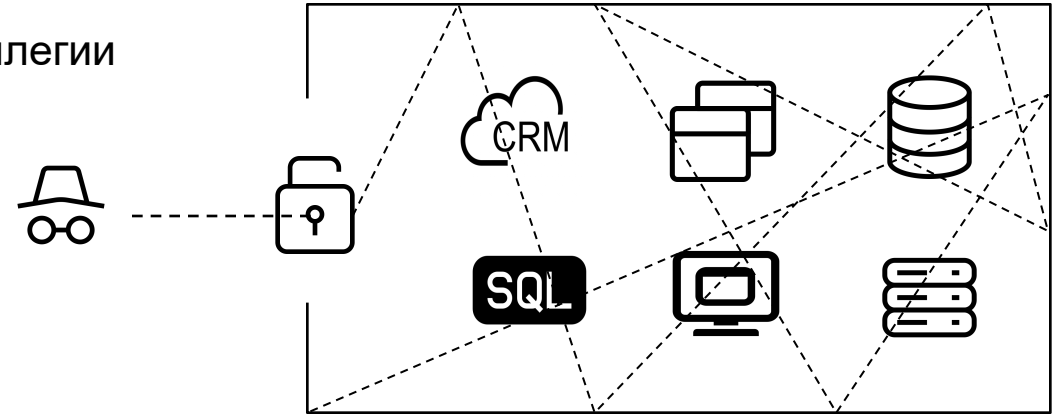

PAM
система обеспечения
безопасного технологического
доступа к ИТ-инфраструктуре
Pace
SECURE PRIVILEGE ACCESS CONTROL ENVIRONMENT

Главная точка атаки
киберпреступников –
неконтролируемые привилегии



Основные цели атаки - информация и контроль над ИТ-инфраструктурой

ИТ-инфраструктура - объект кибератак

Рост ИТ-инфраструктуры рождает новые цели и открывает новые пути для кибератак

On-Premises

- Административные Учетные Записи
- Desktops (Windows, Mac)
- Серверы (Unix, Linux, Windows)
- Промышленные Системы Управления
- Безопасность и Сетевая инфраструктура
- Приложения и БД
- Учетные данные машин (App to App)
- Гипервизоры и Виртуальные машины

Cloud & Hybrid Cloud

- Облачные Платформы Управления (AWS, Azure)
- Виртуальная среда (VMWare, MSFT)
- Виртуальные Машины (Unix, Linux, Windows)
- SaaS-Приложения (Facebook, LinkedIn, Custom)

Internet of Things

- Роуминг Рабочих Станций
- BYOD
- Видеокамеры
- Аппаратура наблюдения
- Принтеры
- Любое устройство со встроенным подключением к интернету

Dev Ops

- DevOps & SecDevOps Tools
- Dynamic Virtual окружение
- Containers
- Microservers

Неконтролируемый привилегированный доступ к ИТ-системам приводит к росту доли успешных кибератак

Следствием этого является утеря данных, утечка конфиденциальной информации, финансовые и репутационные потери компаний

В большинстве компаний никто не может быть уверен в безопасности привилегированных учетных данных

Требования регуляторов

Компаниям необходимо соблюдать требования регуляторов

ГОСТ 57580 ЦБ РФ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.1— 2017

Безопасность финансовых (банковских) операций

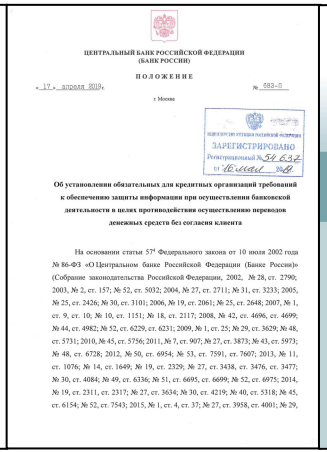
ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Базовый состав организационных и технических мер

Издание официальное

Москва Стандартинформ 2020

Положение 683 ЦБ РФ



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

ПОЛОЖЕНИЕ

«17» апреля 2019 г. № 683-П

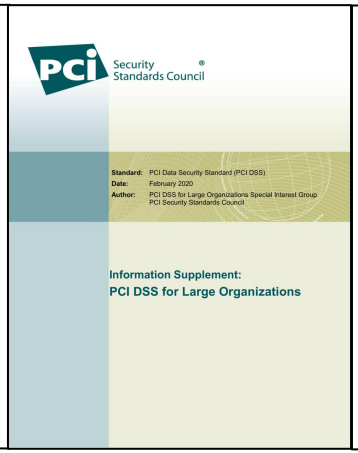
г. Москва

ЗАРЕГИСТРИРОВАНО Регистрационный № 54637 от 16 мая 2019

Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента

На основании статьи 57[4] Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 25, ст. 2426; № 30, ст. 3101; 2006, № 19, ст. 2061; № 25, ст. 2648; 2007, № 1, ст. 9, ст. 10; № 10, ст. 1151; № 18, ст. 2117; 2008, № 42, ст. 4696, ст. 4699; № 44, ст. 4982; № 52, ст. 6229, ст. 6231; 2009, № 1, ст. 25; № 29, ст. 3629; № 48, ст. 5731; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 27, ст. 3873; № 43, ст. 5973; № 48, ст. 6728; 2012, № 50, ст. 6954; № 53, ст. 7591, ст. 7607; 2013, № 11, ст. 1076; № 14, ст. 1649; № 19, ст. 2329; № 27, ст. 3438, ст. 3476, ст. 3477; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695, ст. 6699; № 52, ст. 6975; 2014, № 19, ст. 2311, ст. 2317; № 27, ст. 3634; № 30, ст. 4219; № 40, ст. 5318; № 45, ст. 6154; № 52, ст. 7543; 2015, № 1, ст. 4, ст. 37; № 27, ст. 3958, ст. 4001; № 29,

Требования PSI DSS

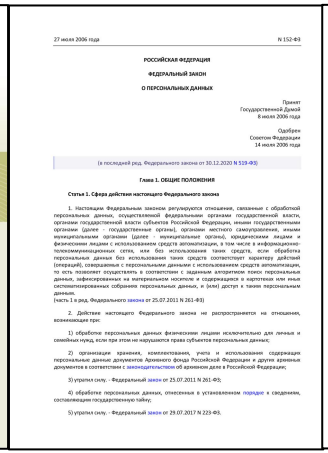


PCI Security Standards Council

Standard: PCI Data Security Standard (PCI DSS)
Date: February 2020
Author: PCI DSS for Large Organizations Special Interest Group
PCI Security Standards Council

Information Supplement:
PCI DSS for Large Organizations

Федеральный закон 152-ФЗ



27 июля 2006 года N 152-ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О ПЕРСОНАЛЬНЫХ ДАННЫХ

Принят Государственной Думой 8 июля 2006 года

Одобрен Советом Федерации 14 июля 2006 года

(в последней ред. Федерального закона от 30.12.2020 N 519-ФЗ)

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеке или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

(часть 1 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

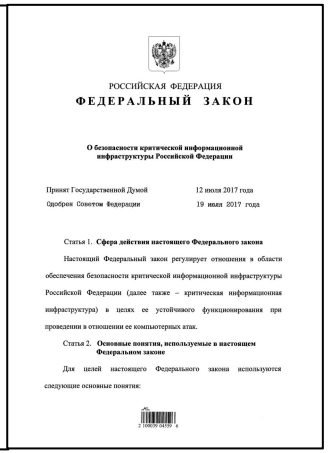
2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) утратил силу. - Федеральный закон от 25.07.2011 N 261-ФЗ;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

5) утратил силу. - Федеральный закон от 29.07.2017 N 223-ФЗ.

Федеральный закон 187-ФЗ



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

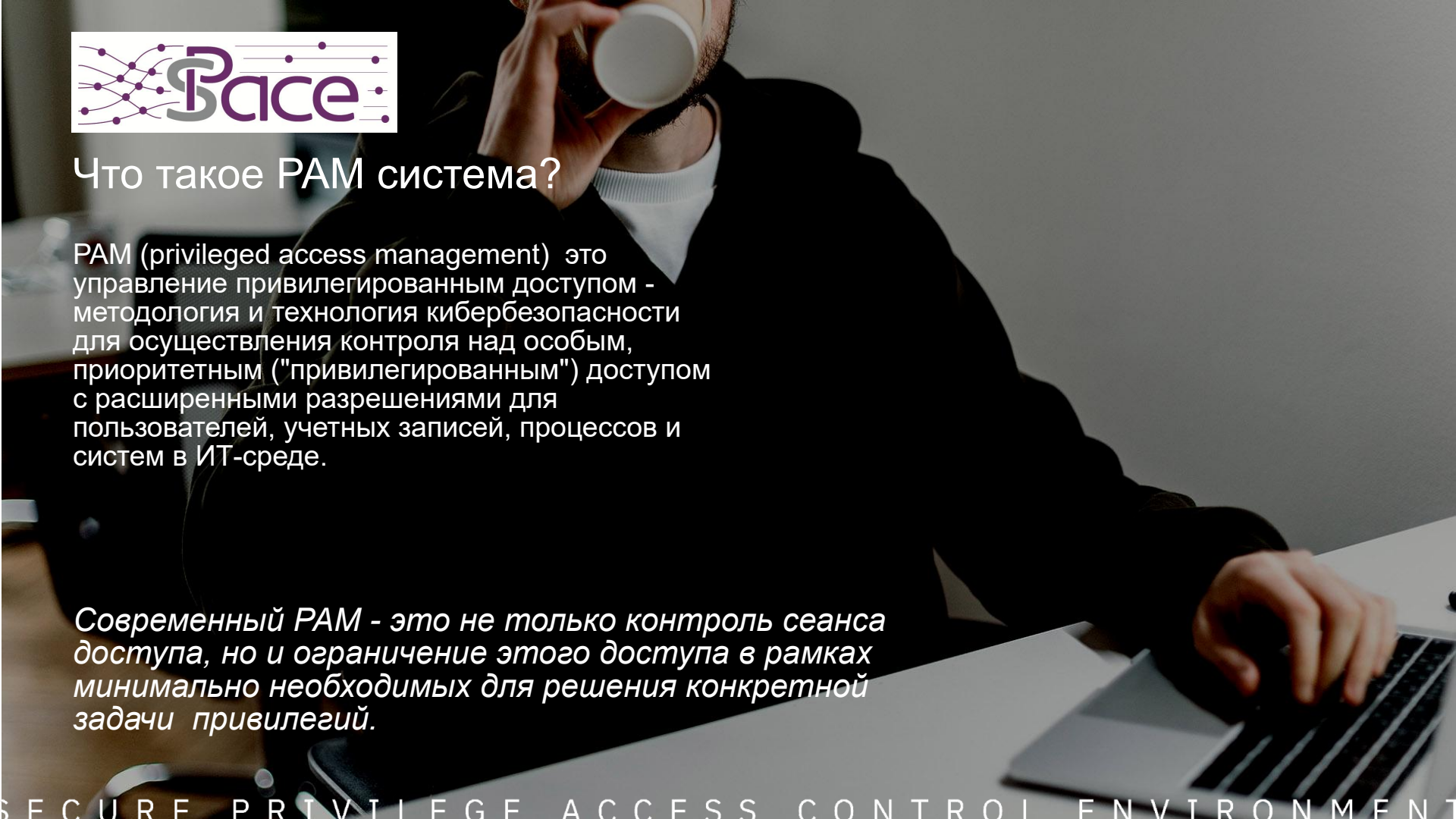
Одобрен Советом Федерации 19 июля 2017 года

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:



Что такое PAM система?

PAM (privileged access management) это управление привилегированным доступом - методология и технология кибербезопасности для осуществления контроля над особым, приоритетным ("привилегированным") доступом с расширенными разрешениями для пользователей, учетных записей, процессов и систем в ИТ-среде.

Современный PAM - это не только контроль сеанса доступа, но и ограничение этого доступа в рамках минимально необходимых для решения конкретной задачи привилегий.

SECURE PRIVILEGE ACCESS CONTROL ENVIRONMENT

Почему PAM система нужна вам именно сейчас?

- Значительный рост числа сотрудников и внешних подрядчиков которым нужен удаленный доступ
- Лавинообразный рост количества и интенсивности кибератак
- Новые штрафы и угроза уголовной ответственности за киберинциденты
- Уход с нашего рынка иностранных производителей высокопроизводительных PAM систем

PAM-система - важнейший и действенный инструмент для предупреждения кибератак

Gartner

К 2024 году 50% организаций внедрят привилегированный доступ

Внедрение PAM - «приоритет №1» в проектах безопасности на ближайшие годы

kuppingercole ANALYSTS

Рынок PAM-решений вырастет вырастет с 2,2 млрд.$ в 2020 до 4,5 млрд.$ к 2025

- Традиционные PAM - системы это прежде всего системы хранения и обеспечения жизненного цикла привилегированных учетных записей.
- Они ориентированы на работу в основном с администраторами ИТ-систем, контроль их действий и расследования инцидентов связанных с компрометацией привилегированного доступа.
- Они имеют ограниченный набор поддерживаемых «из коробки» контролируемых ИТ систем.

Внедрение PAM это длительный трудоемкий процесс который не всегда удается довести до конца.

«Идеальный PAM» глазами заказчиков

- *Наличие необходимого функционала*
- *Поддержка всех ИТ систем в организации*
- *Безопасность*
- *Простота внедрения*
- *Простота использования*

Не только безопасный, но и простой в использовании

Затраты на сопровождение и масштабировани е минимальны, сотрудников не нужно обучать работать с системой

Можно использовать с другими ИБ-решениями.

Основной функционал по управлению привилегиями работает надежно

Система настолько проста, что с ней могут работать не только ИТ-специалисты, но и бизнес-пользователи

Просто развертывать и быстро внедряется

Просто интегрировать новые объекты администрирования

sPACE - система организации контролируемого доступа привилегированных пользователей, обеспечивающая не только безопасность, но и простоту внедрения и эксплуатации

- Защита привилегированных учетных данных и снижение рисков кибератак, вызванных их компрометацией
- «Демократизация» PAM - снижение порога «вхождения» и минимизация уровня пользовательского опыта, необходимого для работы с PAM
- Обеспечение контролируемого доступа не только для администраторов, но и для любого критичного доступа к ИТ системам
- Автоматизация управления доступом и повышение продуктивности сотрудников

SECURE PRIVILEGE ACCESS CONTROL ENVIRONMENT

Что дает sPACE

Защиту

критически важных ИТ систем и снижение риска кибератак, вызванных компрометацией привилегированных учетных данных

Минимизацию

финансовых потерь и штрафов регуляторов из-за неконтролируемых привилегий

Автоматизацию

управления привилегированным доступом и повышение продуктивности сотрудников

Контроль доступа

не только для ИТ-специалистов, но и для бизнес-пользователей, работающих с «чувствительной» информацией

PAM система sPACE

Управление

Согласование доступа

Ролевая модель

Условия и график доступа

Управление привилегированным и учетными данными

Контроль

Единая точка входа

Прерывание подозрительных сессий

Соответствие парольной политике

Расследование

Контроль активных сеансов

Мониторинг состояния системы

Просмотр завершенных сеансов

Почему вам нужен именно sPACE?

- ветераны рынка сформировались на рубеже веков, когда ИТ-инфраструктура была совсем другой, наша система создавалась для современных реалий
- высокая стоимость этих систем обусловлена большим количеством наследованного функционала, который не всегда нужен в современных условиях

sPACE – масштабируемая пластичная система, которая благодаря кластерной архитектуре и гибкому механизму подключения к инфраструктуре удовлетворит любого заказчика.

Основные подходы к пректированию sPACE

Policy-Based Access Control (PBAC) – управление доступом на основе политик

Zero Standing Privileges (ZSP) – нулевые постоянные привилегии

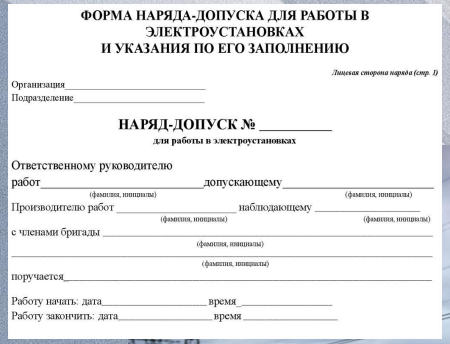
Security by Design – безопасность по природе

Реализация ZSP и PBAC в sPACE

- Привилегированный доступ предоставляется для решения определенной Задачи в конкретной целевой системе
- Доступ предоставляется по запросу с использованием механизма согласования Нарядов-Допусков.
- В случае отсутствия согласованного и действующего Наряда-Допуска доступ Пользователя к целевым системам невозможен
- sPACE позволяет гранулировать доступ и предоставлять разные права для решения различных задач в конкретной целевой системе
- Доступ к конкретной задаче предоставляется путем запуска Сценариев

Наряд - Допуск

Задача + Пользователь + Полномочия + Период действия



ФОРМА НАРЯДА-ДОПУСКА ДЛЯ РАБОТЫ В ЭЛЕКТРОУСТАНОВКАХ
И УКАЗАНИЯ ПО ЕГО ЗАПОЛНЕНИЮ

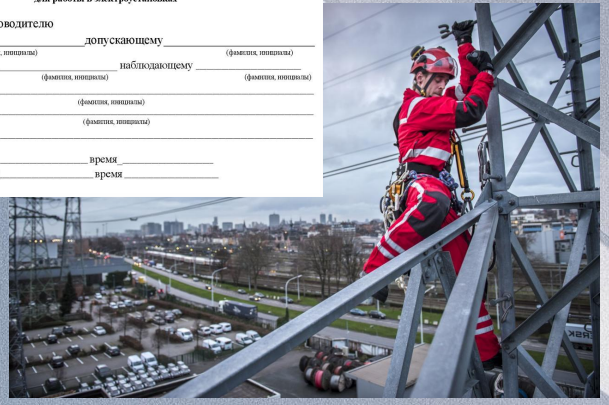
Лицевая сторона наряда (стр. 1)

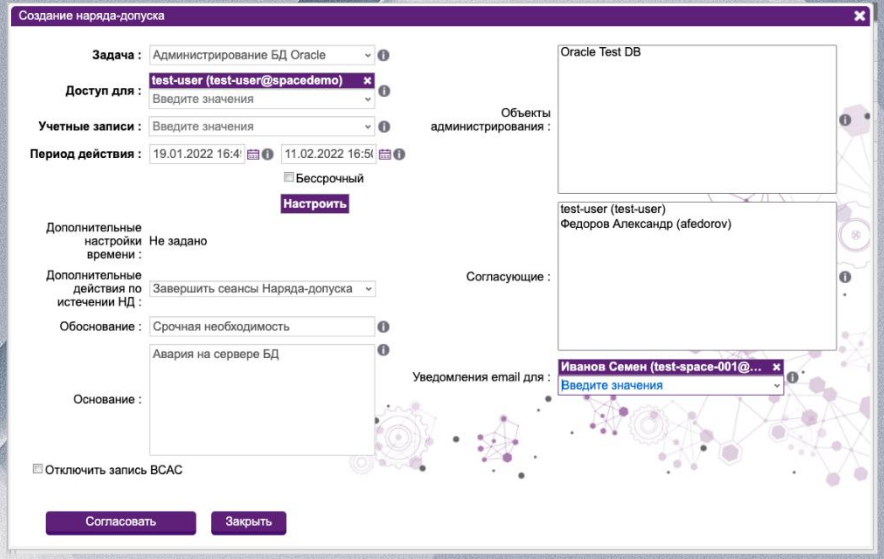
Организация_____
Подразделение_____

НАРЯД-ДОПУСК № _____
для работы в электроустановках

Ответственному руководителю
работ_____допускающему_____
(фамилия, инициалы) (фамилия, инициалы)
Производителю работ _____ наблюдающему _____
(фамилия, инициалы) (фамилия, инициалы)
с членами бригады _____
(фамилия, инициалы)
_____
(фамилия, инициалы)
поручается_____

Работу начать: дата_____время_____
Работу закончить: дата_____время_____





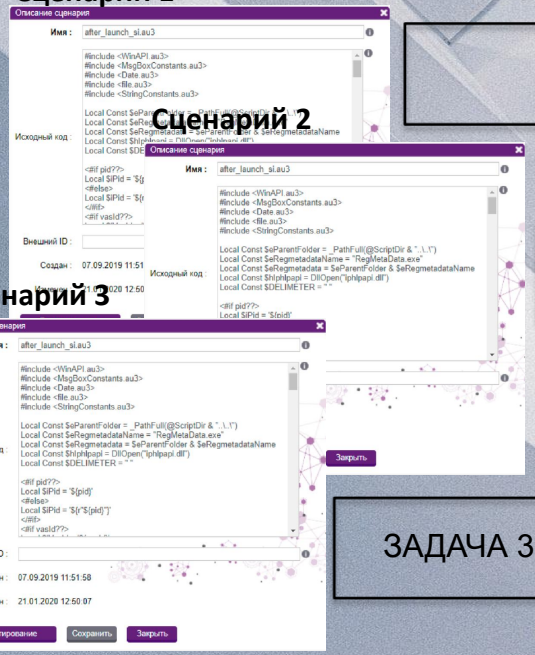
Задача

Объект администрирования + Сценарий запуска + Инструмент

Сценарий 1

Сценарий 2

Сценарий 3

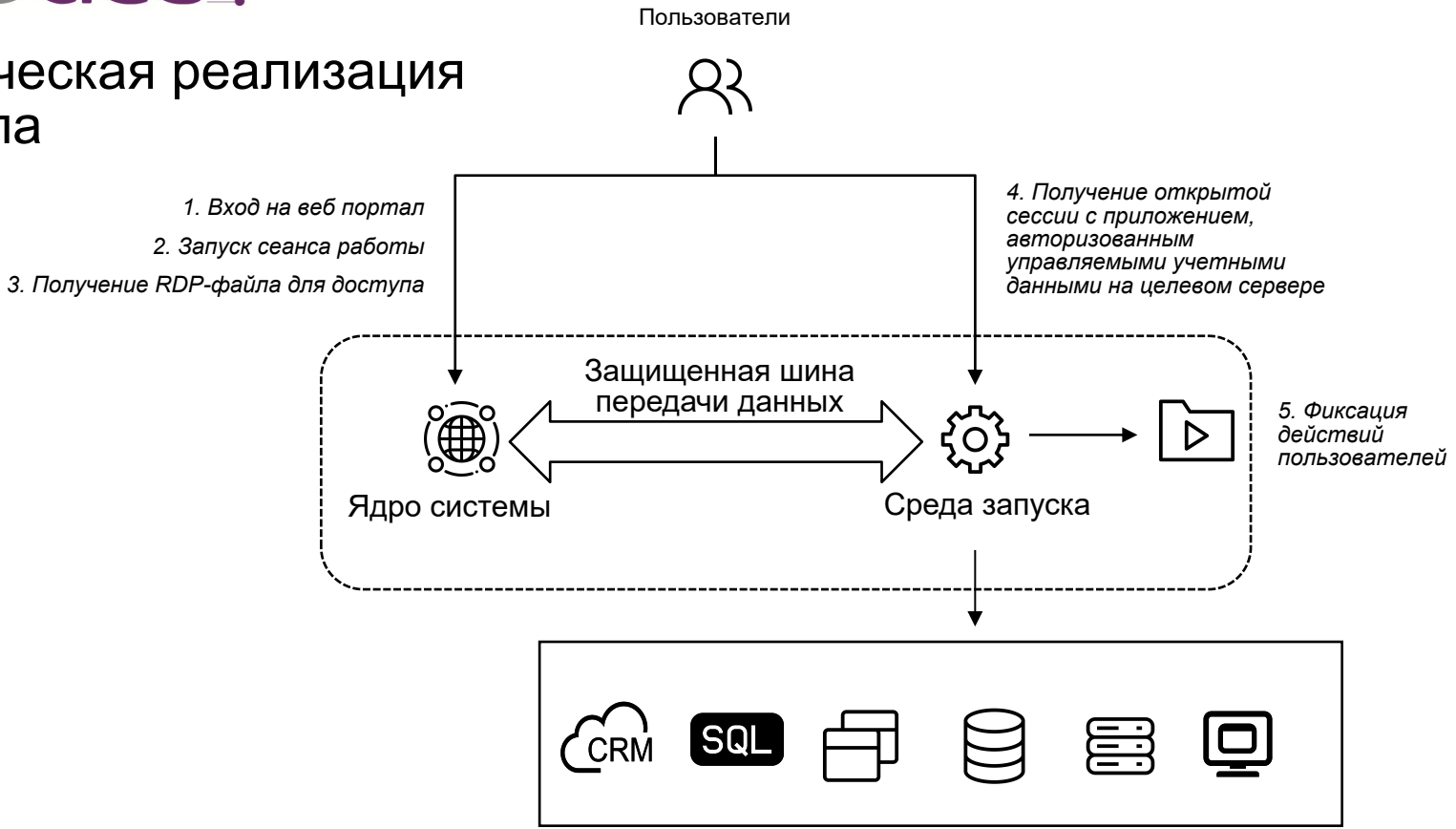


ЗАДАЧА 1 – Настройка БД

ЗАДАЧА 2 – Анализ данных

ЗАДАЧА 3 – Настройка сервера

Техническая реализация доступа



ЯДРО - главный управляющий элемент системы

- Единый веб портал для пользователей, аудиторов и администраторов
- Встроенная защищенная база данных
- Защищенная шина передачи данных
- Служба хранения данных аудита
- Поддержка инсталляции на Ubuntu/Debian/CentOS/Astra Linux

Поддерживается распределенная установка ядра

Защищенная СРЕДА ЗАПУСКА инструментов

- Доверенная среда исполнения инструментов администрирования
- Безопасный проброс учетных данных целевых систем
- Широкие возможности масштабирования
- Запись сеансов и keylog
- Поддержка всех актуальных версий Windows Terminal Server

Преимущества sPACE

- Быстрая интеграция на основе запуска открытых для редактирования сценариев в рамках бизнес-задач
- Простой механизм наделения привилегиями с использованием нарядов-допусков
- Удобство и простота эксплуатации
- Развитый API для интеграции с другими инструментами ИБ
- Распределенная архитектура (масштабирование, автоматическая балансировка нагрузки и устойчивость к отказам)
- Нетребовательность к ИТ-ресурсам - низкая стоимость эксплуатации и масштабирования

Игорь Базелюк

bazelyuk@web-control.ru
+7 (495) 925-77-94

www.web-control.ru
e-mail: info@web-control.ru

www.s-pace.ru
e-mail: info@s-pace.ru