

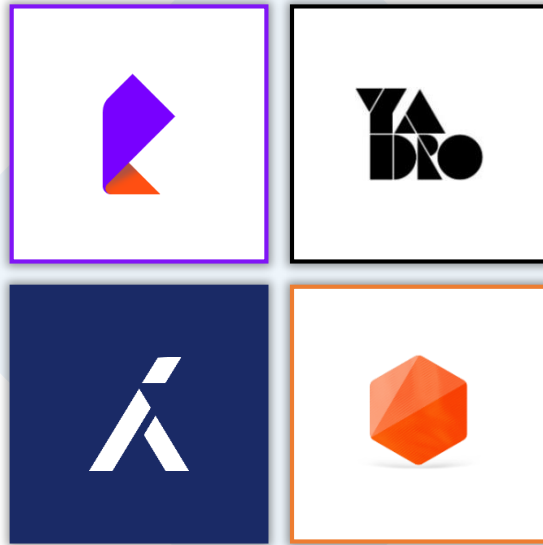
Базис.Virtual Security

BASIS



БАЗИС–сейчас

 «БАЗИС» – ведущий российский разработчик программных продуктов для оказания облачных услуг, платформы динамической инфраструктуры и виртуализации



- Компания образована в результате создания СП «Облачная платформа» лидирующими компаниями ИТ-рынка – Ростелеком, YADRO и Rubytech
- Результатом объединения стала уникальная интеграция экспертиз известных разработчиков и появление единого продуктового портфеля от ТИОНИКС, Digital Energy и Скала Софтвер

О нас




Решения уровня Enterprise и Cloud Provider с самой большой подтвержденной референсной базой




✓ Более **50 000** 


✓ CPU

✓ Более **5 000 ТВ** 

✓ RAM

✓ Более **100 РВ** 

✓ Дискового пространства

✓ Более **100 000** 

✓ Виртуальных машин

- Эксперты с 10-летним стажем на рынке импортозамещения в области виртуализации
- Наличие сертификатов ФСТЭК и ФСБ - соответствия требованиям регуляторов до 1 класса защищенности
- Партнёрство с ведущими отечественными производителями оборудования (Kaspersky, Yadro, Скала и др.)
- Участник разработки стандартов виртуализации в рамках работы с Ростех и ГЕОП

Объединенная продуктовая линейка BASIS



Программный вендор решений – экосистема IaaS и PaaS решений на рынке России



Динамическая инфраструктура и IaaS

Базис.DynamiX

- Высокопроизводительная платформа на базе динамической инфраструктуры для управления виртуальными машинами, bare metal серверами, и контейнерами.



Виртуализация рабочего места

Базис.WorkPlace

- Платформа для виртуализации рабочих мест сотрудников посредством VDI или публикации отдельных терминальных приложений.



Конвейер DevOps

Базис.Digital Energy

- DevOps конвейер на базе динамической инфраструктуры для полного цикла разработки и тестирования



Гипервизор

Базис.vCore

- Аппаратный гипервизор, который устанавливается непосредственно на физический сервер



Безопасность виртуальной инфраструктуры

Базис.Virtual Security

- Средство защиты информации систем виртуализации и облачных платформ
- Есть сертификация ФСТЭК



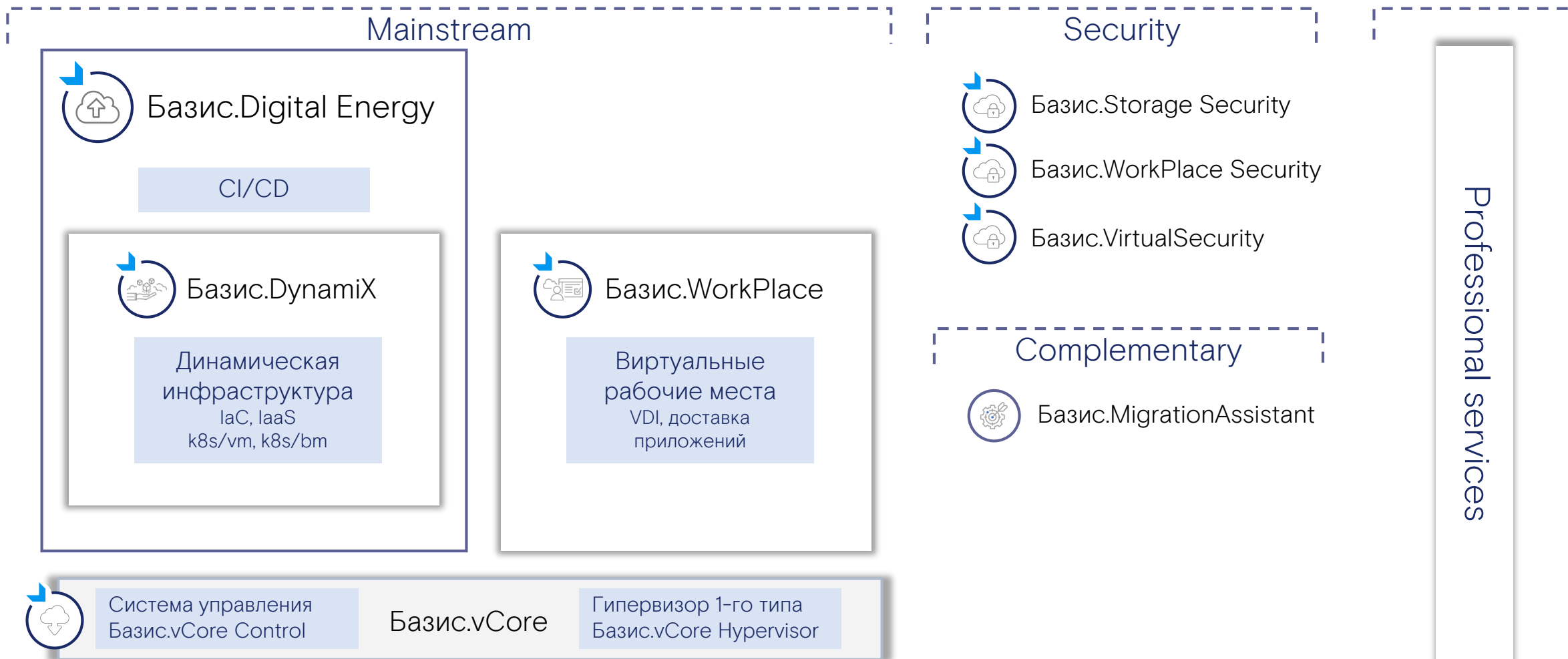
Безопасность виртуального рабочего места

Базис.WorkPlace Security

- Организация защищенного доступа до VDI машин
- Флеш-носитель для безопасного подключения к физическому рабочему месту из любой точки
- Есть сертификация ФСТЭК



Общая экосистема



Замещаемые иностранные решения



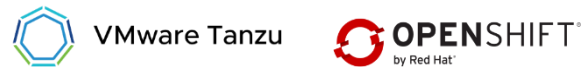
Базис.vCore



Базис.Dynamix



Базис.DigitalEnergy



Базис.WorkPlace



Базис.WorkPlace Security



Базис.VirtualSecurity

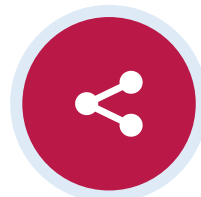
Основы для создания Базис.Virtual Security

Рост количества информационных систем, требующих аутентификации пользователя



Снижение времени доступа к приложениям

Необходимость защиты средств виртуализации на рынке СЗИ для KVM



Необходимость обеспечения безопасности на каждом уровне системы

Большие издержки на администрирование ИС



Несанкционированный доступ к информационным системам

Исполнение требований законодательства:



№ 149-ФЗ от 27.07.2006 г. (ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации»

№ 152-ФЗ от 27.07.2006 г. (ред. от 29.07.2017) «О персональных данных»

Базис.Virtual Security



Средство защиты конфиденциальной информации для решения следующих задач



Реализация технологии единой точки
Доступа (Single Sign On) к ИС



Управление доступом
к информационным системам



Защита средств виртуализации



Идентификация и
аутентификация



Многофакторная
аутентификация



Регистрация событий
безопасности

Сертификация средства защиты информации во ФСТЭК РФ



Базис.Virtual Security - первое в России программное средство защиты конфиденциальной информации, которое получила сертификат соответствия ФСТЭК РФ



Сертификат получен в декабре 2020 г.

Соответствует требованиям ФСТЭК РФ



«Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»



4 уровень доверия



Требованиям технических условий RU.НРФЛ.00002-01.90.01

Достижения и экономические выгоды



Первый

Проект по комплексной системе обеспечения информации на базе KVM



9 из 10 мер защиты средств виртуализации

закрываются одним продуктом (кроме антивируса)



IT-выгоды

Горизонтальная масштабируемость системы за счет кластеризации и обеспечение высокой доступности системы



Взаимодействия с внешними каталогами посредством протоколов

LDAP

- Active Directory
- Red Hat Directory Server
- Tivoli
- Novell eDirectory
- Другой

Kerberos

Архитектура

Сервис-агент

Устанавливается непосредственно на контролируемые вычислительные сущности и обеспечивает следующий функционал

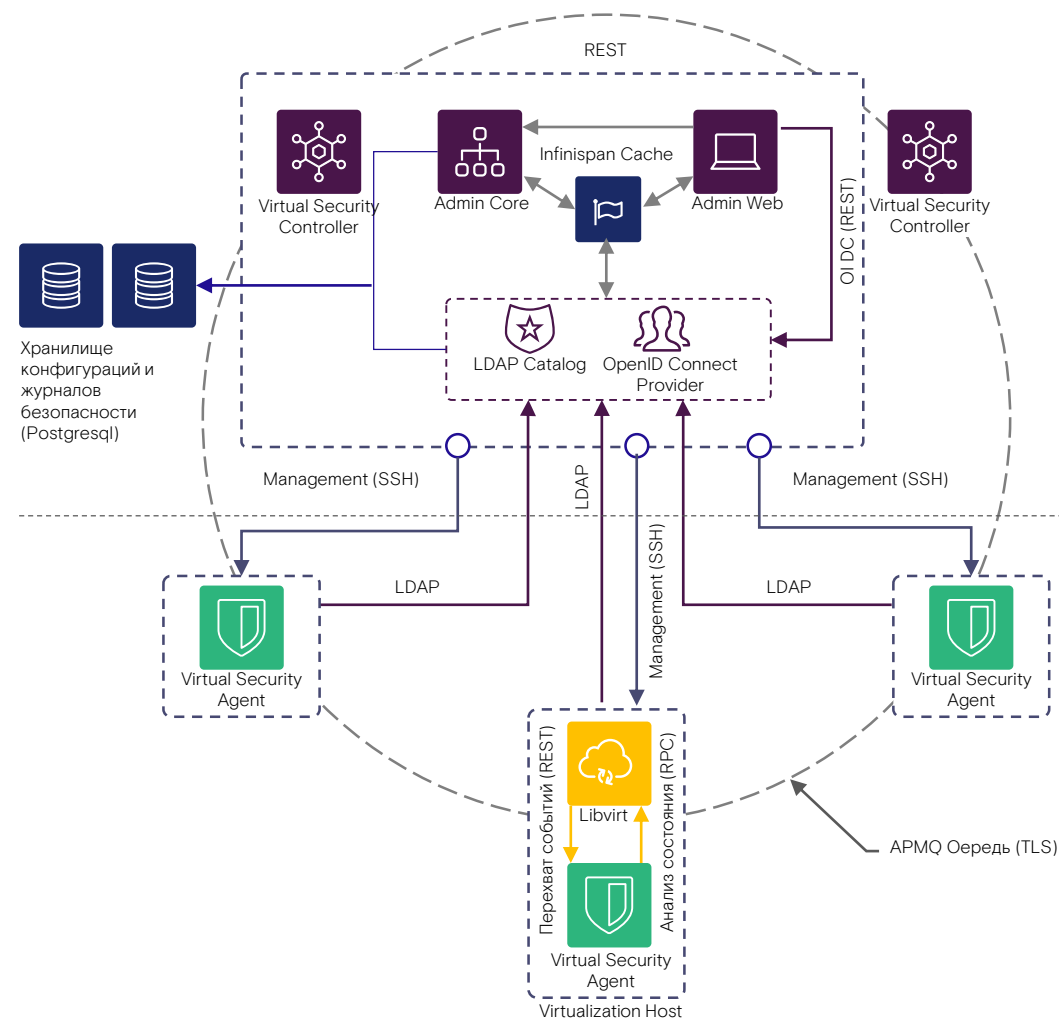
- Контроль запуска, миграции и изменения конфигурации, мониторинг событий изменения состояния виртуальных машин, виртуальных сетей и их портов
- Мониторинг состояния виртуальных машин, управление ими в пределах вычислительной сущности

Сервис авторизации и аутентификации

- Компонента обеспечения аутентификации и авторизации по протоколу OpenID Connect
- Компонента обеспечения аутентификации и авторизации LDAP

Контроллер управления

- Компонента консоли управления платформой
- Ядро управления платформой



Многофакторная аутентификация



В Базис.Virtual Security реализована возможность многофакторной (двухфакторной) аутентификации, с использованием TOTP алгоритма создания одноразовых паролей

Функции безопасности



В Базис.Virtual Security объединяются результаты мониторинга записей регистрации из разных источников

Состав и содержание информации о событиях безопасности обеспечивают возможность идентификации:



Идентификационной информации источника



Субъекта доступа связанного с событием



Типа события безопасности



Событие безопасности



Результат события безопасности



Дата и время

Интеграционные возможности Базис.Virtual Security



Безопасность

Обеспечение подлинности сетевых соединений, в том числе для защиты от подмены сетевых устройств и сервисов

Сокращение числа параллельных сеансов доступа для каждой учетной записи



Блокирование сеанса доступа в ПО после установленного времени неактивности пользователя или по его запросу

Ограничение неуспешных попыток доступа к ПО для защиты системы от брутфорс атак

Технология единого входа



SSO - Single Sign-On - механизм единого входа в систему или в приложение

Базис.Virtual Security
поддерживает два стандарта
реализации единого входа



1. Lightweight Directory Access Protocol (LDAP)
2. OpenID Connect 1.0

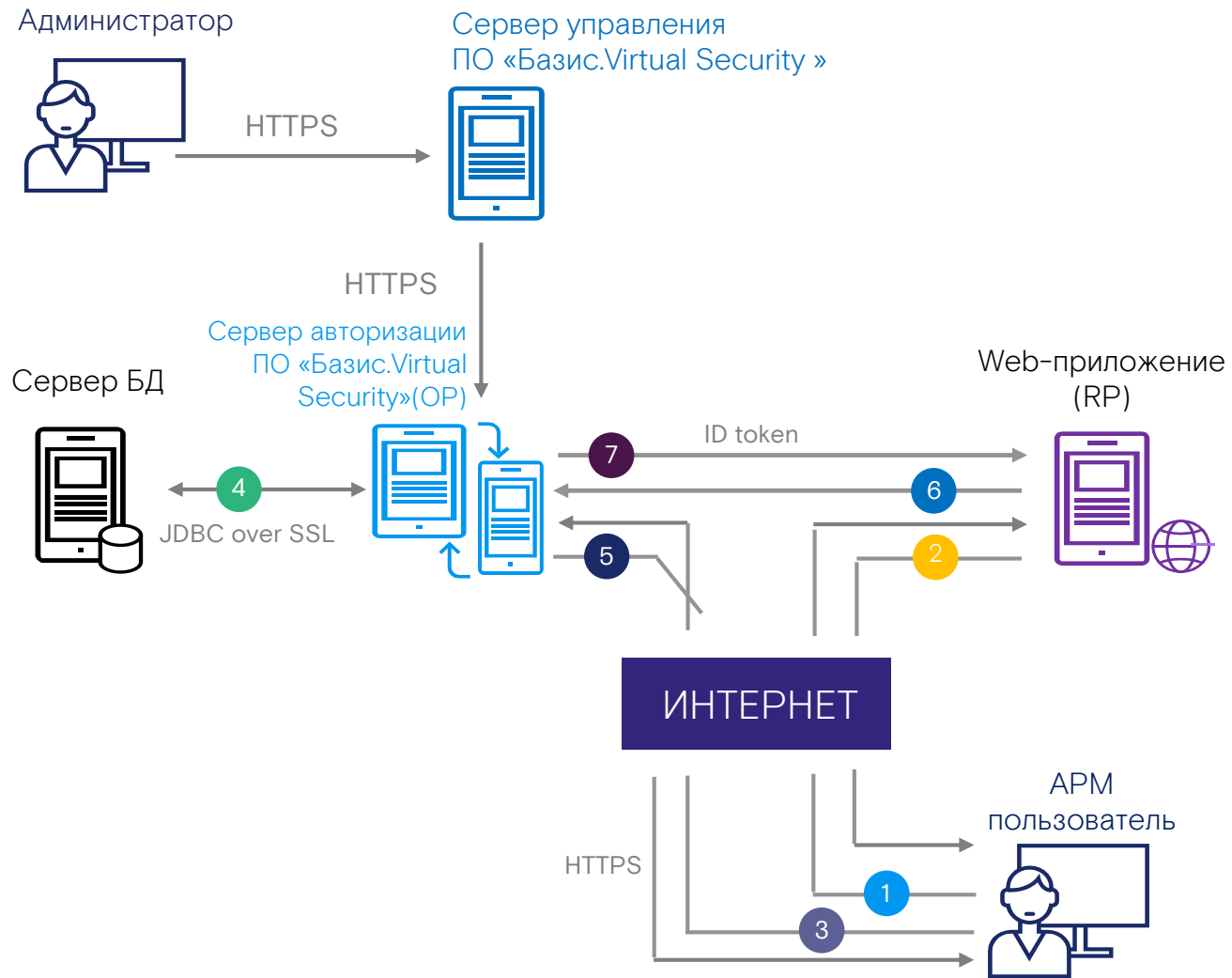
Основные задачи, которые
решает SSO система



- Уменьшение хаоса между различными комбинациями имени пользователя и пароля
- Уменьшение кол-ва запросов по восстановлению забытых паролей
- Централизованное управление паролями
- Сокращение времени доступа к приложениям
- Снижение рисков несанкционированного доступа



Реализация единого входа - OpenID Connect



- 1 | Пользователь пытается осуществить Web-доступ к приложению (SP)
- 2 | Приложение формирует Authorization Code Request (протокол OAuth2.0) и перенаправляет браузер пользователя на сервер авторизации TVS (OP)
- 3 | Пользователь вводит свои учетные данные на OP
- 4 | OP аутентифицирует пользователя одним из установленных способов
- 5 | В случае успеха, OP запрашивает у пользователя разрешение на передачу RP информации о нем. В случае положительного решения, возвращает сообщение Authorization Response, которое содержит код авторизации
- 6 | RP проверяет ответ OP, после чего отправляет запрос на токен (Token Request).
- 7 | В случае успешной проверки запроса на токен, OP отправляет RP токены идентификации и авторизации (ID Token, Access Token)

Политика паролей и поддержка входа при помощи ЕСИА



При управлении аутентификационной информацией реализованы следующие возможности и ограничения

Генерация и выдача начальной аутентификационной информации



Установление характеристик средств аутентификации



Задание максимального времени действия пароля



Защита аутентификационной информации от неправомерного доступа и модифицирования



Также реализован вход с использованием ЕСИА

Соответствие требованиям



Для государственных и персональных информационных систем до 1 класса защищенности включительно

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Приказ ФСТЭК России от 18.02.2013 г. № 21

«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК России от 14.03.2014 г. № 31

«Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Приказ ФСТЭК России от 25.12.2017 г. № 239

«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Методический документ от 11.02.2014 г.

«Меры защиты информации в государственных информационных системах»

Спасибо за внимание!

Наши контакты



+7 495 645 6889

Presale@basistech.ru

BASIS