ООО «Си Ти Ай» | г. Москва, ул. Кржижановского, д. 29, корп. 1 | тел.: +7.495.784.73.13

# Указ Президента РФ №250

## решения, технологии, практические аспекты реализации

itsec® ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ РОССИИ

cti.ru

CTI

20 ЛЕТ
В IT С ВАМИ!

системная
интеграция

разработка ПО

облака
и управляемые
сервисы

cti.ru

CTI Communications Technology Innovations

О КОМПАНИИ

# CTI

## 20 ЛЕТ В IT С ВАМИ!

**ТОП-25** крупнейших ИТ-компаний по показателю эффективности ведения бизнеса

»»»

**ТОП-25** лучших системных интеграторов России

**>30 тыс** реализованных проектов

**>350** сотрудников

**>800** профессиональных сертификатов

**>100** партнеров со всего мира

собственный Департамент R&D

# >30 тыс

реализованных проектов

МТС

IKEA

Alfa-Bank

S7 Airlines

VimpelCom

МАГНИТ

РОСБАНК
SOCIETE GENERALE GROUP

Домодедово
Международный аэропорт

Ростелеком

X5 RETAIL GROUP

Русский Стандарт
Банк

HOME CREDIT BANK

ЭР-ТЕЛЕКОМ

globus

УРАЛСИБ
Финансовая корпорация

РОСНАНО

TELE2

Газпром нефть

РУСФИНАНС БАНК
Группа Сосьете Женераль

Международный аэропорт Шереметьево

ЮниКредит Банк

Аэропорт Иркутск

AIRPORT TOLMACHEVO
NOVOSIBIRSK

Международный аэропорт Краснодар
INTERNATIONAL AIRPORT KRASNODAR

# >100

партнеров
со всего мира

NAUMEN · Webinar · IVA · kaspersky

Труконф · BSS · ПРОТЕЙ · RUSIEM · ЦРТ ГРУППА КОМПАНИЙ

positive technologies · КОД безопасности · s-terra · infotecs · ГАРДА ТЕХНОЛОГИИ

Check Point SOFTWARE TECHNOLOGIES LTD · INFOWATCH · VIDEOMOST.COM video conferencing server · 3iTech · aurus

cisco Partner · DELL Technologies · Hewlett Packard Enterprise · f5 · H3C

VERINT · APC by Schneider Electric · Lenovo · NetApp

vmware Partner Connect · paloalto NETWORKS · FORTINET · JUNIPER NETWORKS

aruba a Hewlett Packard Enterprise company · Omilia Conversational Intelligence · AVAYA · ZOOM INTERNATIONAL · VERITAS

СТИ 20 ЛЕТ В IT С ВАМИ!

# УКАЗ №250 ПРЕЗИДЕНТА РФ:

# РЕШЕНИЯ, ТЕХНОЛОГИИ, ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ

# указ Президента РФ №250 от 01 мая 2022 г. «О дополнительных мерах по обеспечению информационной безопасности РФ»



## на кого распространяется Указ

**ФОИВы**

**Государственные фонды**

**Госкорпорации**

**Стратегические и системообразующие предприятия**

**Субъекты КИИ**

(классы ОКВЭД: 05, 06, 07, 08, 09, 19, 20, 24, 26 (26.51), 30, 35, 49, 50, 51,52, 53, 61, 64, 65, 66, 72, 84 (84.12), 86.)

# указ Президента РФ №250: решения, технологии, практические аспекты реализации



## что необходимо сделать?

**Создать отдельное структурное подразделение по обеспечению информационной безопасности**, либо возложить эти обязанности на уже существующее структурное подразделение

**Создать должность заместителя генерального директора по информационной безопасности**

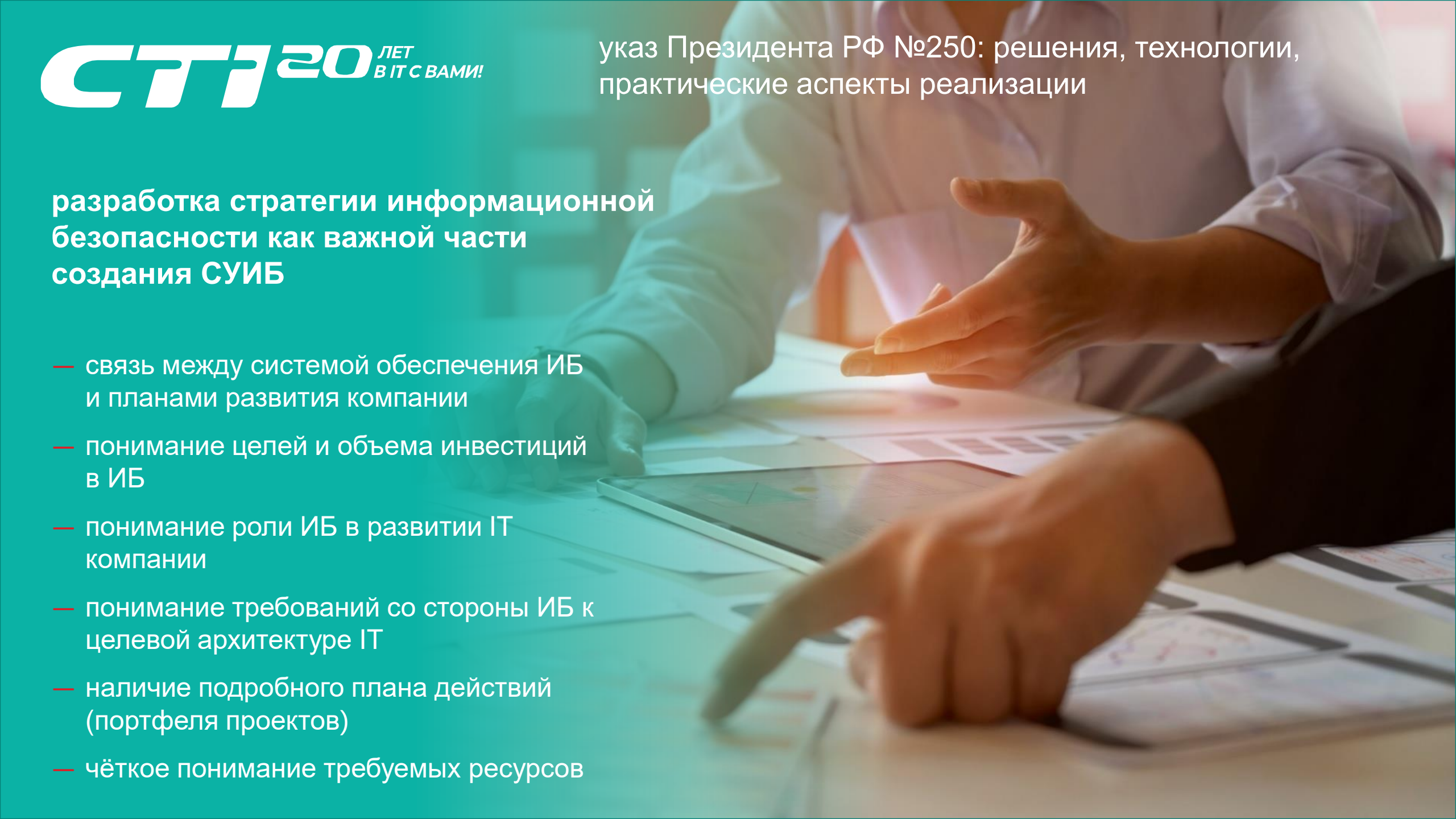
**Провести анализ защищённости информационных систем** (относится к компаниям из перечня, утвержденного Распоряжением Правительства от 22 июня 2022 г. N 1661-р)

**Организовать обмен данными с НКЦКИ**

**Обеспечить незамедлительную реализацию организационных и технических мер**, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их компетенции и направляются на регулярной основе в органы (организации) с учетом меняющихся угроз в информационной сфере

СТИ 20 ЛЕТ В IT С ВАМИ!

указ Президента РФ №250: решения, технологии, практические аспекты реализации



## разработка стратегии информационной безопасности как важной части создания СУИБ

- связь между системой обеспечения ИБ и планами развития компании
- понимание целей и объема инвестиций в ИБ
- понимание роли ИБ в развитии IT компании
- понимание требований со стороны ИБ к целевой архитектуре IT
- наличие подробного плана действий (портфеля проектов)
- чёткое понимание требуемых ресурсов

## что входит в разработку стратегии?

- анализ перечня конфиденциальной информации, обрабатываемой в организации
- определение ключевых бизнес-процессов и ИТ-активов организации
- анализ рисков ИБ
- анализ информационной инфраструктуры организации и определение её ключевых элементов
- анализ защищённости информационных систем
- построение модели угроз и модель нарушителя

## что предлагает CTI для выполнения требований Указа №250?

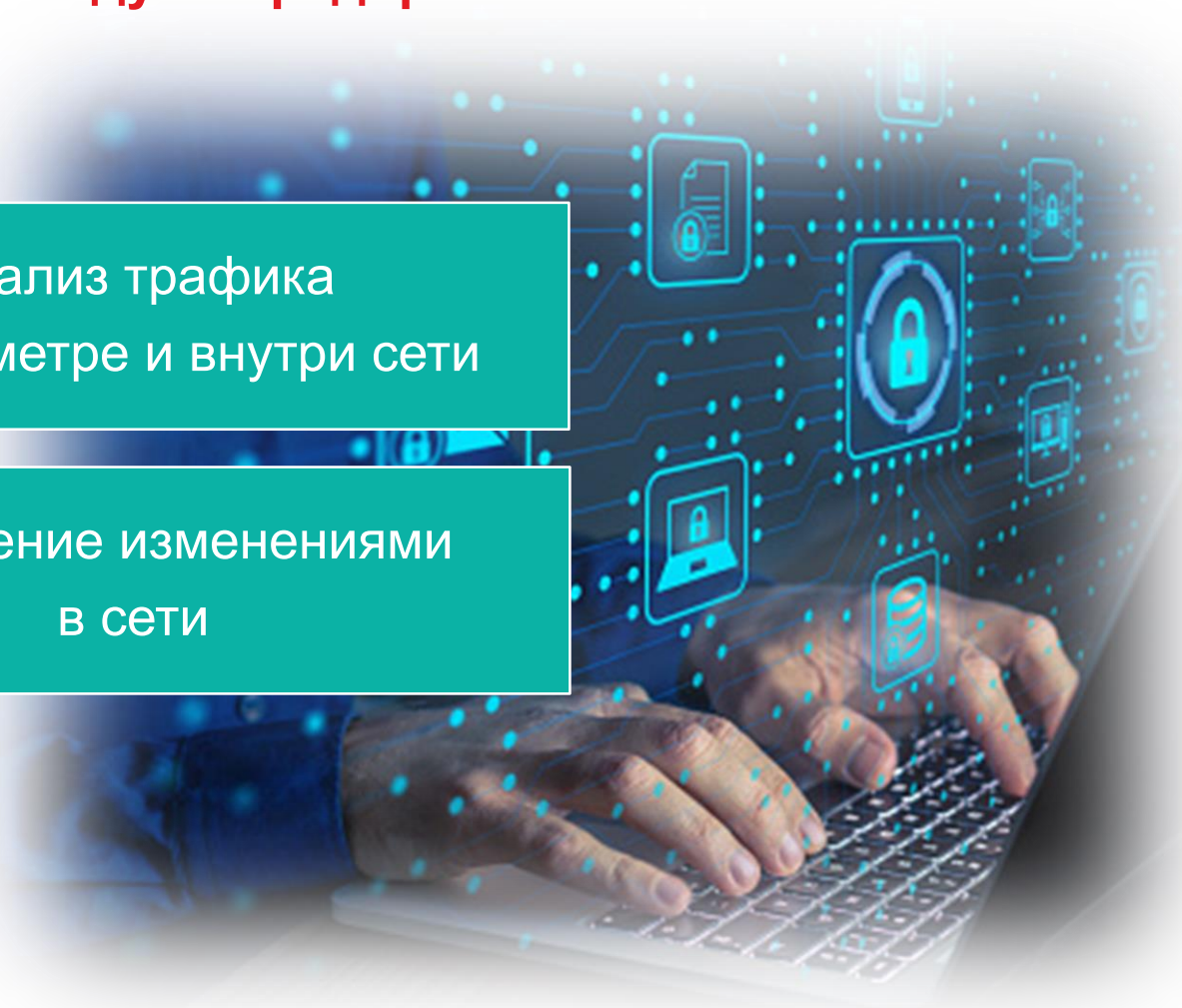
- оценка рисков ИБ
- разработка политики ИБ и других организационно-распорядительных документов
- определение критичных ИТ-активов и ключевых бизнес-процессов
- разработка модели угроз безопасности информации и модели нарушителя
- внедрение решений по оценке и повышению осведомлённости сотрудников в вопросах ИБ
- приведение оценки соответствия компании требованиям законодательства
- проведение киберучений по противодействию компьютерным атакам
- проведение анализа защищённости и тестирование на проникновение
- внедрение решений для передачи информации об инцидентах в НКЦКИ
- внедрение решений ИБ, включая решения по сетевой безопасности, мониторингу инцидентов и защите прикладных систем

# указ Президента РФ №250: решения, технологии, практические аспекты реализации



**некоторые из важных мер, которые мы рекомендуем предпринять**

- решения по сетевой безопасности
- анализ трафика на периметре и внутри сети
- внедрение UEBA решений
- управление изменениями в сети



## выбор и внедрение решений по сетевой безопасности

- Система обнаружения/предотвращения вторжений (IDS/IPS)
- Контроль приложений (Application Control) Если пользователь попытается запустить неизвестную программу, NGFW заблокирует запуск и уведомит администратора;
- Антивирусная защита (Anti-Virus)
- Защита почтового трафика (безопасность почты, антиспам)
- Веб-фильтрация
- Обнаружение утечек информации (DLP)
- Инспектирование SSL-трафика
- Мониторинг туннелей, в частности, загрузка VPN-туннелей
- Создание VPN-туннелей.
- Проверка почтового трафика.
- Поддержка кластеризации.
- Балансировка нагрузки
- Инспектирование SSL-трафика

**критерии выбора и перечень характеристик NGFW:**

1. тип платформы (аппаратное, программное или облачное решение)
2. набор функций (глубокая проверка пакетов, контроль приложений, DLP, IDS/IPS сигнатуры, умение работать с SSL и т.д.)
3. производительность
4. управляемость

## анализ трафика как способ обнаружить атаку на компанию

предпосылки внедрения

- сетевые решения ИБ важны, но тем не менее не являются панацеей от всех бед
- существенная часть всех атак – целевые атаки (41% в 2021 году по данным Лаборатории Касперского) – обход NGFW и других СЗИ
- при выполнении работ по анализу защищенности экспертам Positive Technologies удалось проникнуть в сеть 93% организаций

# анализ трафика как способ обнаружить атаку на компанию

**Системы анализа сетевого трафика (NTA)** предназначены для перехвата потоков данных и обнаружения признаков сложных, чаще всего целевых атак (APT).

С их помощью можно проводить ретроспективное изучение сетевых событий, обнаруживать и расследовать операции злоумышленников в информационной инфраструктуре предприятия, а также эффективно реагировать на соответствующие происшествия.

Такие системы отлично дополняют продукты класса Endpoint Detection and Response (EDR), могут служить богатым источником сведений для SIEM-систем или центров мониторинга и оперативного реагирования на инциденты информационной безопасности (SOC).

**основные функции NTA-решений:**

- анализ трафика как на периметре сети, так и внутри инфраструктуры
- выявление атак с помощью комбинации технологий обнаружения
- помощь в расследовании инцидентов

**архитектура NTA-решений включает:**

- сетевой сенсор, который собирает трафик,
- серверы централизованного управления
- консоль мониторинга (дашборд)

## анализ инцидентов ИБ с применением технологии UEBA (User and Entity Behaviour Analytics)

### предпосылки использования

- большое количество данных, с которыми приходится ежедневно работать сотрудникам служб ИБ
- усиление компетенций злоумышленников, атаки становятся всё более скрытыми, доля целевых атак в 2021 году, по данным Лаборатории Касперского, составила 41%
- 0-day уязвимости и эксплойты
- проблемы с обновлением сигнатур западных решений

**сигнатурные методы обнаружения атак**

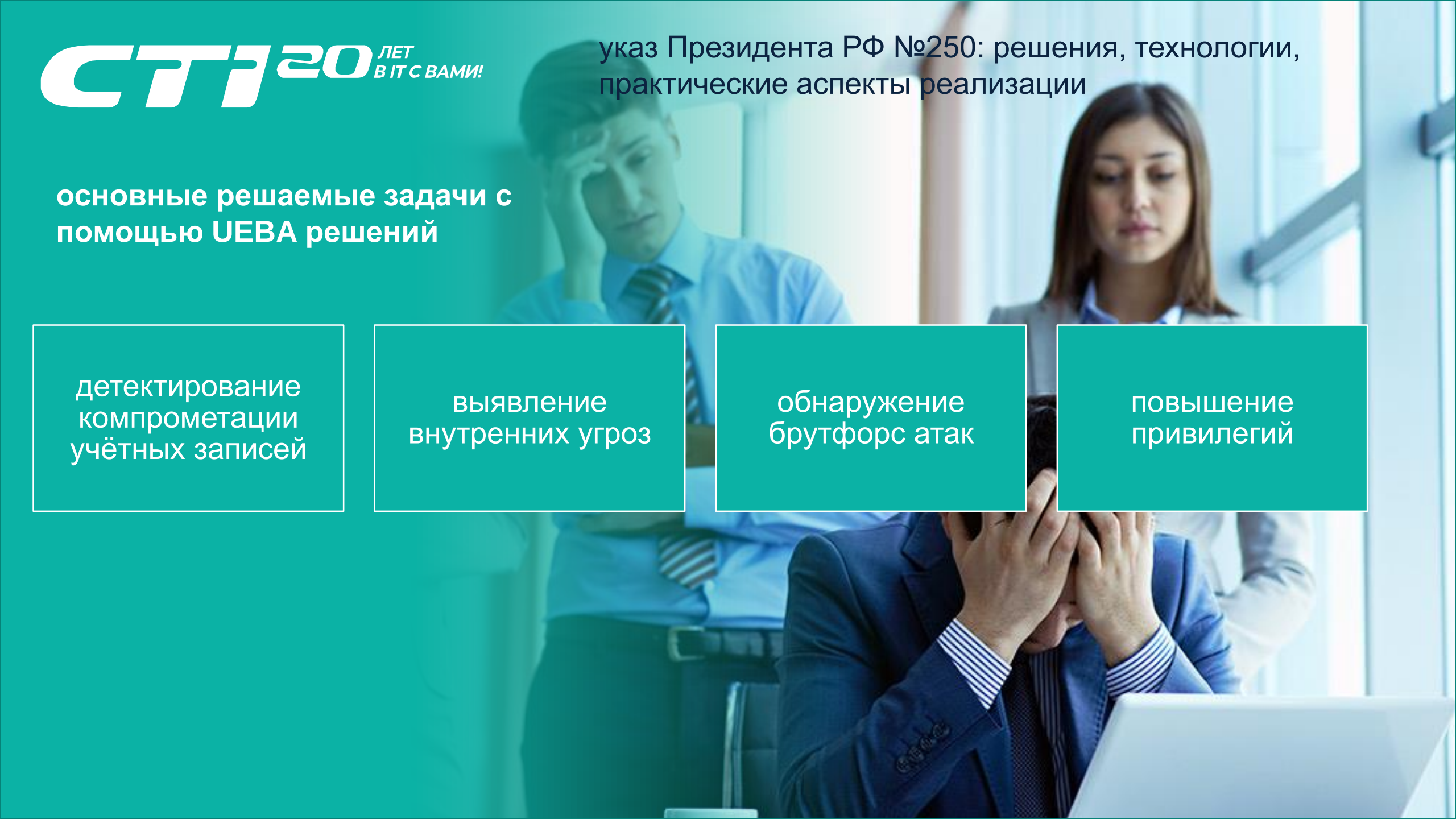
- точность метода
- минимальное число ложных срабатываний

**UEBA**

- независимость от сигнатур
- определение атаки даже если хакер уже в сети

СТ 20 ЛЕТ В IT С ВАМИ!

# указ Президента РФ №250: решения, технологии, практические аспекты реализации



## основные решаемые задачи с помощью UEBA решений

- детектирование компрометации учётных записей
- выявление внутренних угроз
- обнаружение брутфорс атак
- повышение привилегий

СТП 20 ЛЕТ В IT С ВАМИ!

# указ Президента РФ №250: решения, технологии, практические аспекты реализации

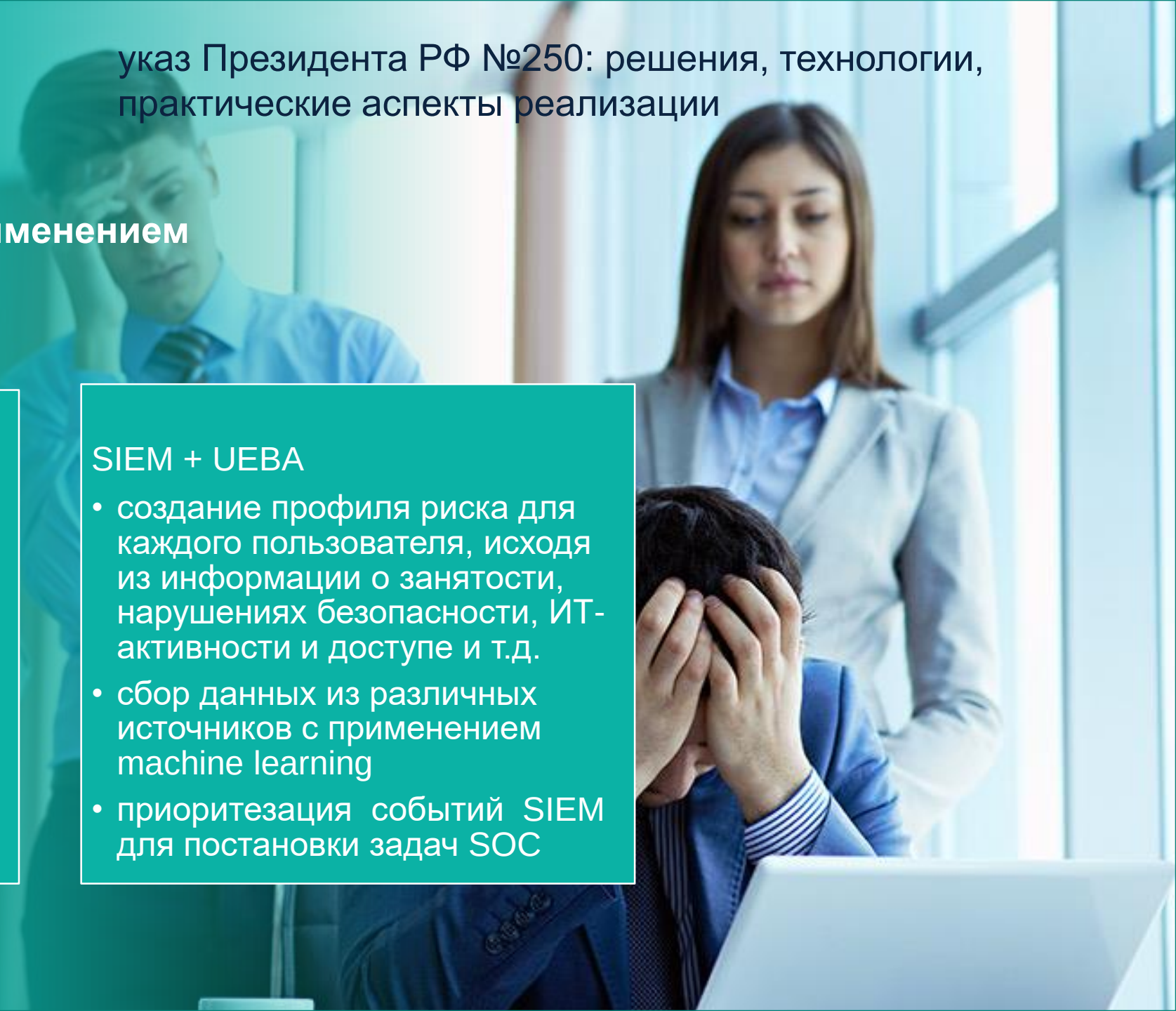
## анализ инцидентов ИБ с применением технологии UEBA
## SIEM + UEBA

SIEM

- работа на основе правил корреляции (требуется разработка множества правил корреляции)
- ложноположительные срабатывания
- слабость против методов социальной инженерии

SIEM + UEBA

- создание профиля риска для каждого пользователя, исходя из информации о занятости, нарушениях безопасности, ИТ-активности и доступе и т.д.
- сбор данных из различных источников с применением machine learning
- приоритезация событий SIEM для постановки задач SOC



# указ Президента РФ №250: решения, технологии, практические аспекты реализации



**защита неструктурированных данных и управление изменениями в сети**

предпосылки для внедрения

80% данных являются неструктурированными

(по оценке Gartner)

65% атак нацелены на получение конфиденциальной информации из неструктурированных данных

на 30% ежегодно увеличивается объём

20% информации не несут никакой пользы

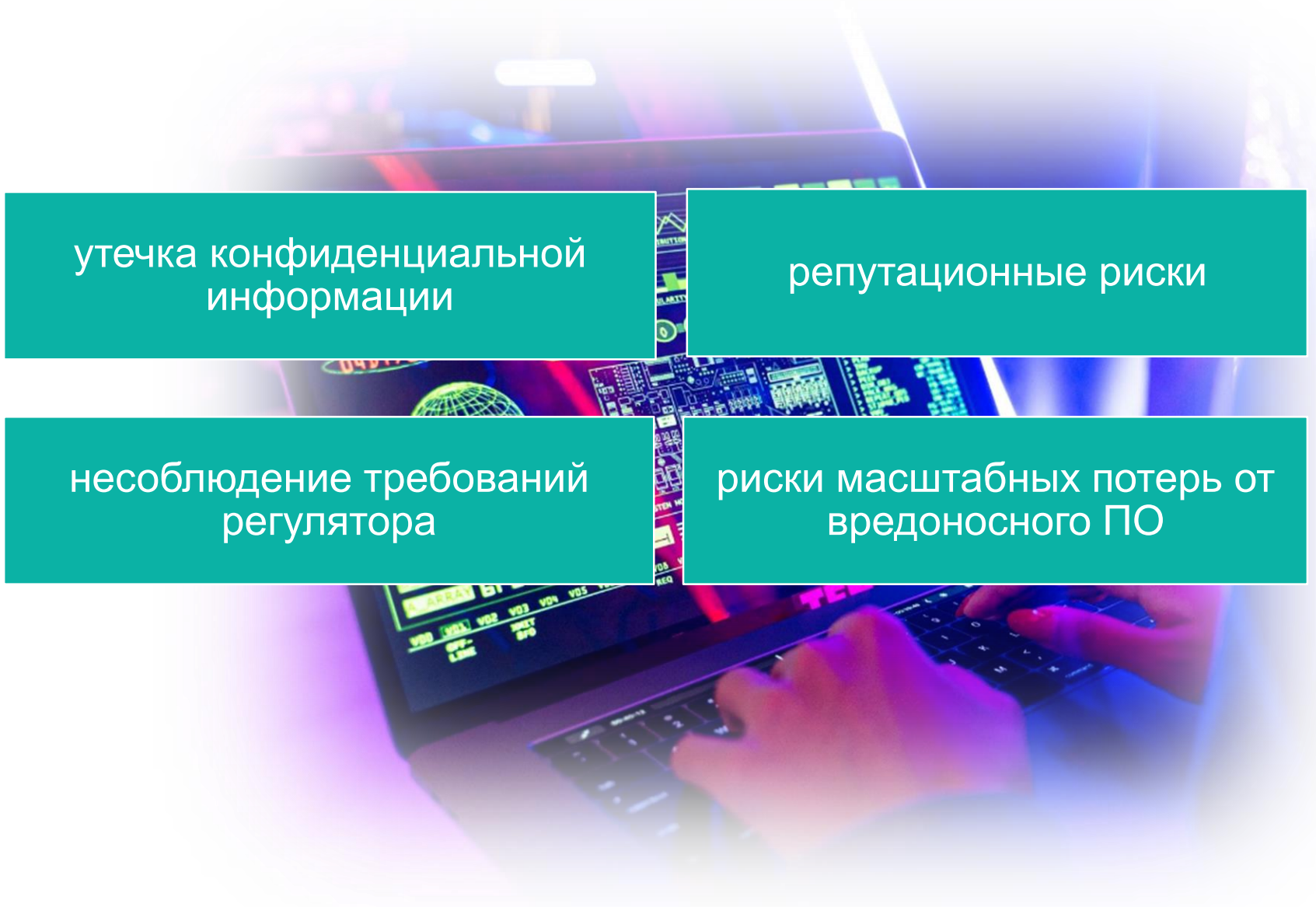
(копии документов, файлы без изменений и т.д.)

*по данным Cyberpeak

# указ Президента РФ №250: решения, технологии, практические аспекты реализации

**защита неструктурированных данных и управление изменениями в сети**

риски, связанные с неструктурированными данными



- утечка конфиденциальной информации
- репутационные риски
- несоблюдение требований регулятора
- риски масштабных потерь от вредоносного ПО

# указ Президента РФ №250: решения, технологии, практические аспекты реализации



**защита неструктурированных данных и управление изменениями в сети**

задачи, решаемые продуктами класса DCAP

## классификация данных

- анализ файловых хранилищ, текущий уровень доступа к файлам и папкам
- категорирование файлов на соответствие стандартам 152 ФЗ, PCI DSS и т.д.
- выявление дубликатов конфиденциальной информации

## контроль доступа

- текущие права пользователей и групп
- контроль изменений прав доступа в AD
- контроль действий с файлами

## поведенческий анализ

- построение профилей пользователей, компьютеров, файлов
- фиксация аномальной активности

## оптимизация ИТ-ресурсов

- поиск дубликатов, неиспользуемых файлов
- отчет по приросту хранилища

# соответствие требованиям

## ISO 27001

bsi.

By Royal Charter

Сертификат Регистрации

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - ISO/IEC 27001:2013

Настоящим удостоверяется, что: ООО «Си Ти Ай»
ул. Кржижановского, д. 29, к. 1
Москва
117218
Российская Федерация

Выдан Сертификат №: IS 602823

о соответствии действующей Системы Менеджмента Информационной Безопасности требованиям стандарта - ISO/IEC 27001:2013 в отношении следующих видов деятельности:

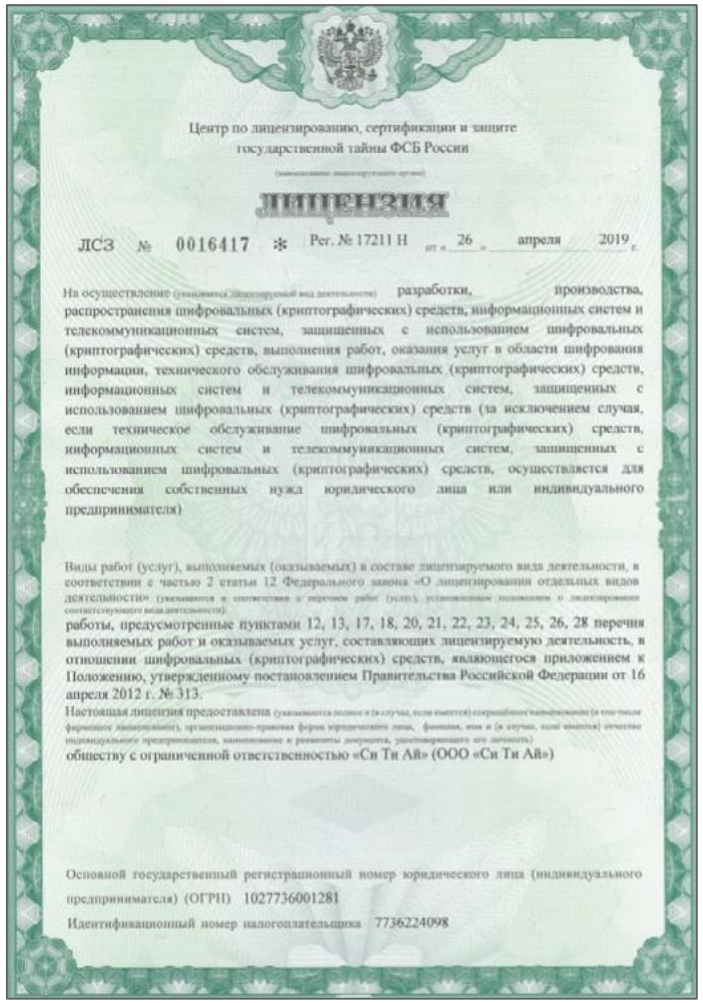
Оказание услуг по аутсорсингу функций эксплуатации и технической поддержке аппаратных средств, программного обеспечения и управляемых сервисов, предоставляемых внешним заказчикам в соответствии с "Положением о применимости контролей" в.11 от 13/09/2019.

От имени и по поручению BSI: Andrew Launn, EMEA Systems Certification Director

Дата первоначальной регистрации: 2013-11-06
Дата последней выдачи: 2019-10-11
Действителен с: 2019-11-07
Действителен до: 2022-11-06
Стр.: 1 из 1

...making excellence a habit.

## лицензия ФСБ



Центр по лицензированию, сертификации и защите государственной тайны ФСБ России

ЛИЦЕНЗИЯ

ЛСЗ № 0016417 Рег. № 17211 Н от «26» апреля 2019 г.

На осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)

Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности, в соответствии с частью 2 статьи 12 Федерального закона «О лицензировании отдельных видов деятельности» (указываются в соответствии с перечнем работ (услуг), установленным положением о лицензировании соответствующего вида деятельности)

работы, предусмотренные пунктами 12, 13, 17, 18, 20, 21, 22, 23, 24, 25, 26, 28 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.

Настоящая лицензия предоставлена (указываются полное и (в случае, если имеется) сокращенное наименования (в том числе фирменное наименование), организационно-правовая форма юридического лица, фамилия, имя и (в случае, если имеется) отчество индивидуального предпринимателя, наименование и реквизиты документа, удостоверяющего его личность)

обществу с ограниченной ответственностью «Си Ти Ай» (ООО «Си Ти Ай»)

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН) 1027736001281

Идентификационный номер налогоплательщика 7736224098

## лицензия ФСТЭК

СЕРИЯ КИ 0296 НОМЕР 014892

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 3491 от 9 июня 2018 г.

*Лицензия предоставлена* Обществу с ограниченной ответственностью «Си Ти Ай» (ООО «Си Ти Ай») ОГРН 1027736001281, ИНН 7736224098

*Адрес места нахождения:* 117218, г. Москва, ул. Кржижановского, д. 29, корпус 1, этаж 5, пом. 1, комн. 23-28

*Адрес места осуществления лицензируемого вида деятельности:* 117218, г. Москва, ул. Кржижановского, д. 29, корпус 2

*Перечень работ и услуг, на которые распространяется настоящая лицензия:*

**проектирование в защищенном исполнении:** средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений

*Перечень услуг, на которые распространяется настоящая лицензия:*

**контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;**

**установка, монтаж, наладка, испытания, ремонт средств защиты информации** (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

*Лицензия предоставлена на основании приказа ФСТЭК России от 9 июня 2018 г. № 212-л*

*Лицензия действует бессрочно*

Заместитель директора А.Куц

CTI

20 ЛЕТ В IT С ВАМИ!

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

# ключевые партнеры

«высшая лига» в области информационной безопасности

эксперты CTI готовы помочь восстановить контур защиты, обеспечить безопасность ценной информации и инфраструктуры

positive technologies
kaspersky
ГАРДА ТЕХНОЛОГИИ
КОД безопасности
s•terra
RUSIEM
Checkmarx
INFOWATCH
CHECK POINT
INDEED ID
iDM
Ростелеком Солар
UserGate
SECURITY VISION

# помощь организациям в новых условиях

- ПОДДЕРЖКА 24X7
  поддержка клиента по вопросам функционирования внедренных ранее ИТ-систем в случае отказа зарубежных производителей работать на территории РФ и блокировки их решений
- ИМПОРТОЗАМЕЩЕНИЕ
  частичное и полномасштабное
- ОПЫТ И ЭКСПЕРТИЗА
  опыт реализации и поддержки комплексных проектов различного масштаба и уровня сложности. Мы имеем достаточную экспертизу по внедрению решений российских вендоров, у нас заключены все нужные партнерские соглашения и сертифицированы специалисты
- АУДИТ, ПИЛОТИРОВАНИЕ, МИГРАЦИЯ
  эксперты CTI готовы провести аудит, пилотирование и миграцию на альтернативные программные и аппаратные решения
- СЕРВИСНЫЙ ЦЕНТР КОМПАНИИ CTI
  услуги технической поддержки и технического сопровождения оборудования и программного обеспечения в прежнем режиме

**95%**

инцидентов решается CTI без привлечения вендора

CTI обладает достаточным количеством ресурсов и компетенций, позволяющих нам самостоятельно решать большинство сервисных запросов


СТ
20 ЛЕТ
В IT С ВАМИ!
СТРЕМЛЕНИЕ
ВПЕРЕД С ИННОВАЦИОННЫМИ
РЕШЕНИЯМИ
для достижения
поставленных целей
заказчика

+7 (495) 784-73-13

cti.ru I cti-service.ru

info@cti.ru

# спасибо за внимание!

www.cti.ru