beeline cloud

Вебинар

Начало в 11:00

Заблуждения в ИБ, от которых страдает безопасность компаний

Спикеры

Дмитрий Коршунов

Руководитель отдела сервисов кибербезопасности beeline cloud

Артем Костоусов

Руководитель направления развития продуктов информационной безопасности beeline cloud

beeline cloud в цифрах

100+
Облачных сервисов и решений

3000+
Клиентов из разных отраслей бизнеса

99,95%
Облачный SLA

6
ЦОДов в РФ уровня Tier III

5
Независимых интернет-провайдеров

Secure by design

УЗ-1 152-ФЗ
Публичное облако

ГИС К1, ИСПДн УЗ-1
Изолированный сегмент

PCI DSS 4.0
Соответствие стандарту

ГОСТ Р 57580.1-2017
Первый уровень защиты информации

ФСБ, ФСТЭК
Лицензии

Партнеры

kaspersky · MULTIFACTOR · positive technologies · radware · UserGate · COMMUNIGATE SYSTEMS · ARENADATA · ФЛАНТ

Заблуждение 1

Купили облако, зачем нам сервисы ИБ

01

Купили облако, зачем нам сервисы ИБ

Что такое безопасное облако:

- Отказоустойчивость и высокая доступность платформы.
- Изоляция и исключение влияния клиентов друг от друга.
- Многоуровневая безопасность: платформа виртуализации, сеть, СХД, приложения.
- Портфель сервисов кибербезопасности.
- Резервирование компонентов облачной инфраструктуры.
- Резервирование систем питания, охлаждения и критически важных элементов.
- Обеспечение физической безопасности.

Пример заблуждения
У меня все защищено: в облаке можно не заботится о дополнительной безопасности сети, сервисов и виртуальных машин.

Заблуждение 2

Аттестованное облако = моя аттестованная система

02

Аттестованное облако ≠ моя аттестованная система

Система не будет автоматически аттестована, если просто разместить её в аттестованном сегменте облака

- У каждой компании уникальная информационная система со своими требованиями по ИБ.
- Именно Оператор ПДн проводит оценку соответствия или аттестацию для каждой из своих ИСПДн.

Пример заблуждения
Требования под ключ: подпишу договор на размещение в аттестованном сегменте или аренду ресурсов, и этим в полной мере выполню требование регулятора.

Условное обозначение и номер меры	Меры защиты информации	Ответственность провайдера за реализацию мер	Ответственность клиента за реализацию мер
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	На уровне: физического оборудования; средств управления средой виртуализации; сервисных/служебных серверов ИС «Сегмент ГИС Облака beeline cloud»; сервисов ИС «Сегмент ГИС Облака beeline cloud».	На уровне: технических средств (АРМ, серверов и т.п.), размещенных в собственной инфраструктуре клиента; виртуальных серверов, предоставляемых клиенту.
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	На уровне физического оборудования ИС «Сегмент ГИС Облака beeline cloud»	
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	На уровне: физического оборудования; средств управления средой виртуализации; сервисных/служебных серверов ИС «Сегмент ГИС Облака beeline cloud»; сервисов ИС «Сегмент ГИС Облака beeline cloud».	
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	На уровне: физического оборудования; средств управления средой виртуализации; сервисных/служебных серверов ИС «Сегмент ГИС Облака beeline cloud»; сервисов ИС «Сегмент ГИС Облака beeline cloud».	

Заблуждение 3

ИБ «по дефолту» — и так сойдет

03

ИБ «по дефолту» — и так сойдет

Начинайте проект с обсуждения деталей: необходимо понимать, что и как следует защищать

- Изучите описание сервиса провайдера услуг.
- Уточняйте, что входит в состав услуги и как можно повысить ее уровень ИБ.
- Для качественной настройки средств защиты погружайте провайдера в детали: подробное техническое задание или совместная работа с командой провайдера.

Небезопасный пример:

- Сайт за WAF с настройками «по дефолту».
- Публикация на NGFW сервисов RDP или SSH с заменой стандартного порта на нестандартный.
- В облаке провайдера безопасно, значит могу открыть все порты.

Заблуждение 4

Бэкап — не моя забота

04

Бэкап — не моя забота

Зачастую компании не заказывают услугу резервного копирования, думая, что сервис включен по умолчанию

48%

Компаний, использующих IaaS, пользуются РК

70%+

Российских компаний потеряли данные из-за недостаточного РК*

25%

Российских компаний не используют резервное копирование*

Осознанный выбор

Некоторые компании используют собственные средства для бэкапа или считают, что достаточно резервировать данные средствами приложения. Важно, чтобы такие решения принимались обдуманно.

*По статистике RAEC

Бэкап — не моя забота

Резервное копирование должно выполняться на отдельном оборудовании, а не на том же, где хранятся основные данные

Бэкапы должны храниться на отдельной площадке для возможности восстановления системы с нуля

Небезопасный пример

- Сделаю бэкап на соседнюю виртуальную машину. В случае чего, восстановлюсь с нее.
- Считаю, что провайдер делает бэкап моей виртуалки «по умолчанию».

Рекомендации

- Бэкапа «по дефолту» может быть не достаточно.
- Имейте несколько резервных копий (full, incremental).
- **Checkup backup:** 1 раз в полгода проводите проверку возможности восстановления из бэкапов.
- Храните бэкапы в изолированных сегментах.
- 2 недели – рекомендуемый минимальный период хранения резервных копий.

Заблуждение 5

Анализ уязвимостей — не наша задача

05

Анализ уязвимостей — не наша задача

Сканирование уязвимостей позволяет понять, какие проблемы в системе безопасности могут использовать злоумышленники для атаки на инфраструктуру

- Несанкционированное сканирование может расцениваться как попытка неправомерного доступа к ИС с привлечением к гражданско-правовой, административной и вплоть до уголовной ответственности (гл.28 ст.272-274 УК РФ).
- Сканирование информационных систем клиентов должно происходить только после подписания необходимых договоров и соглашений.

Заблуждение
Передам свою информационную систему на аутсорсинг или размещу в облаке, а сканированием уязвимостей и обеспечением безопасности займется кто-то другой.

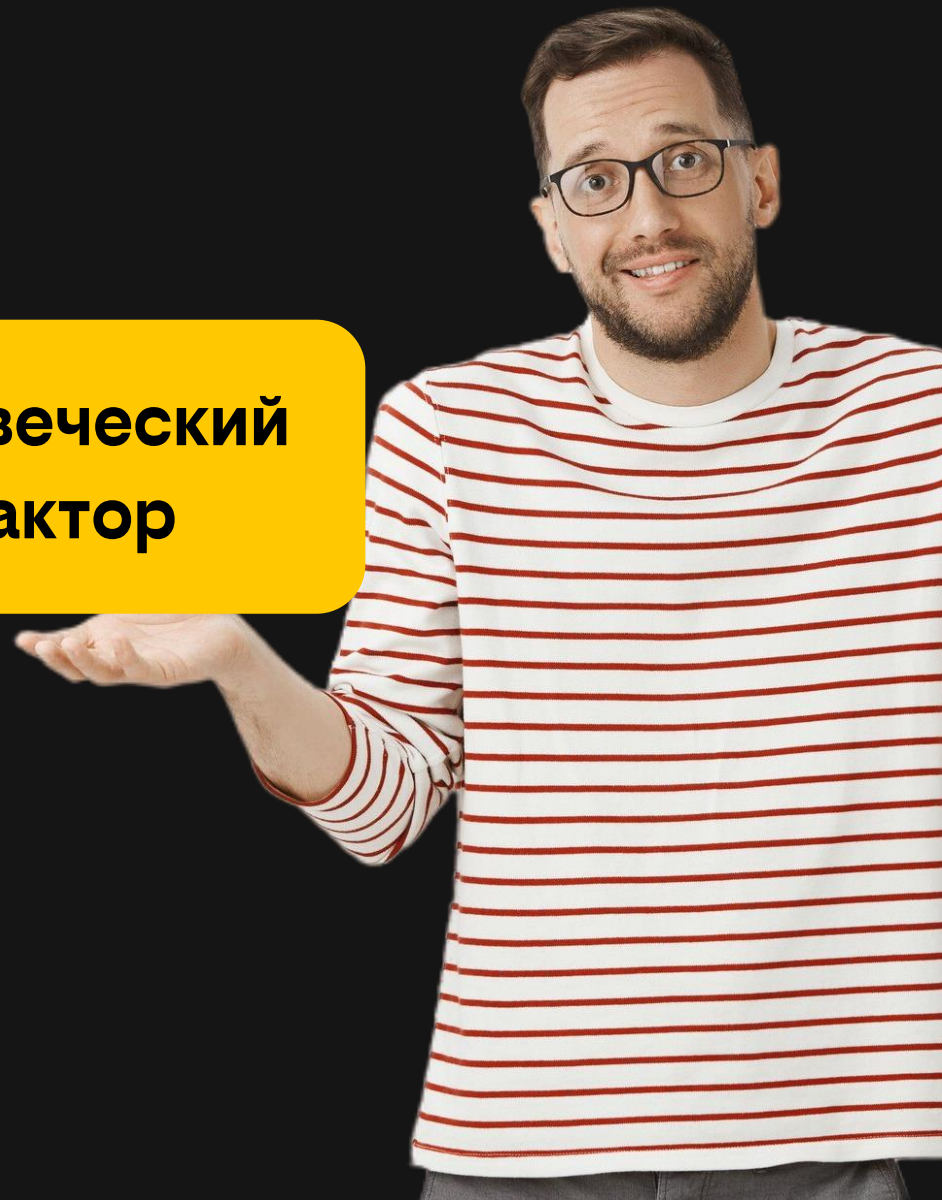
Заблуждение 6

СЗИ защитят от всего

06

СЗИ защитят от всего

- Многомиллионные затраты на СЗИ не защитят от «я что-то нажала, и тут все замигало...»
- ~80% кибер-инцидентов компании происходят по вине сотрудников.
- Сотрудников нужно непрерывно обучать, чтобы повышать уровень осведомленности.
- Легче предотвратить инцидент, чем исправлять последствия после его возникновения.

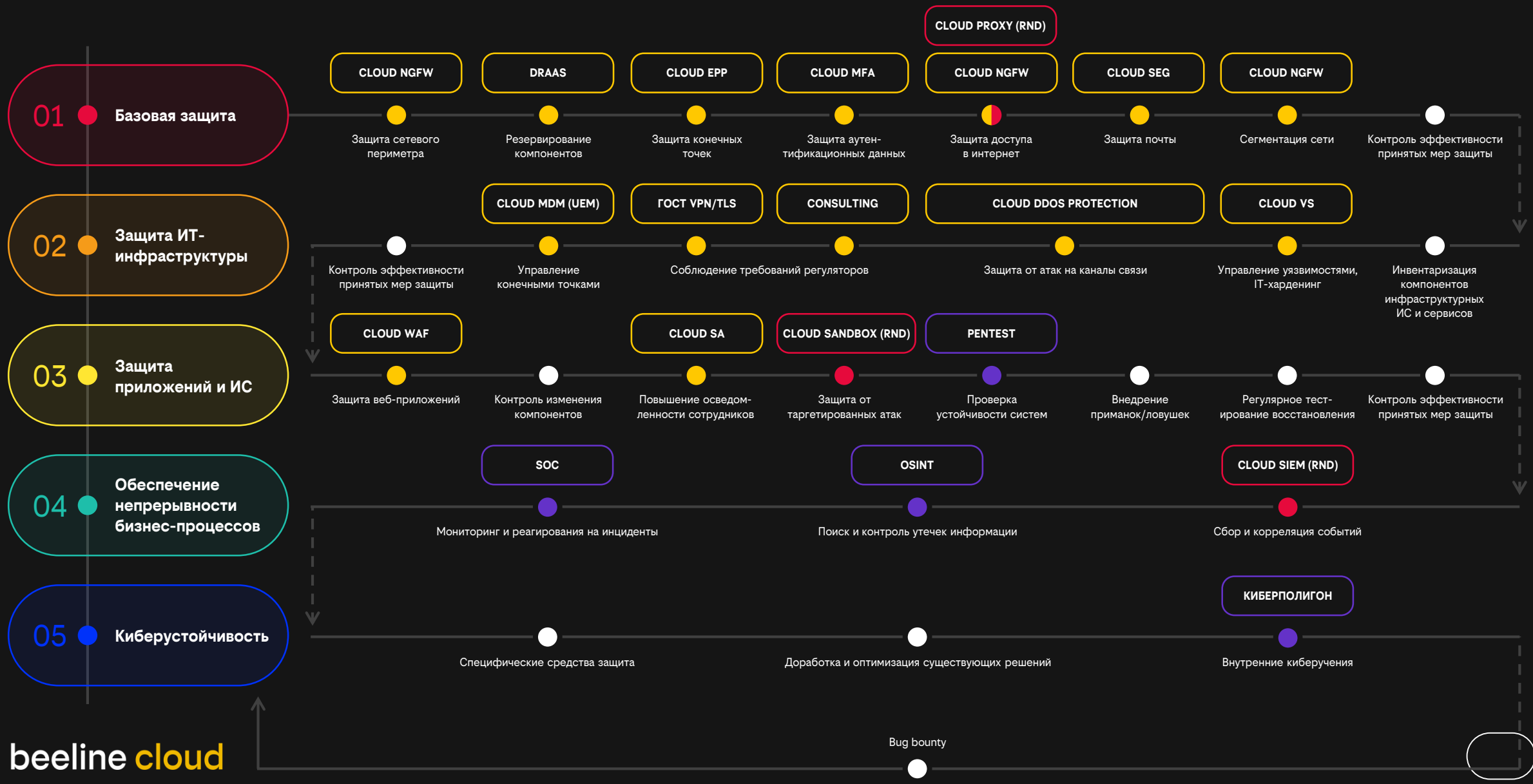


Полезные ссылки

Методический документ ФСТЭК

Матрица ATT&CC

Путь к киберустойчивости



beeline cloud

beeline cloud

Спасибо за внимание!