

# Мифические Security Champion'ы или как не сойти с ума в мире безопасной разработки

Газизова Светлана  
Swordfish Security

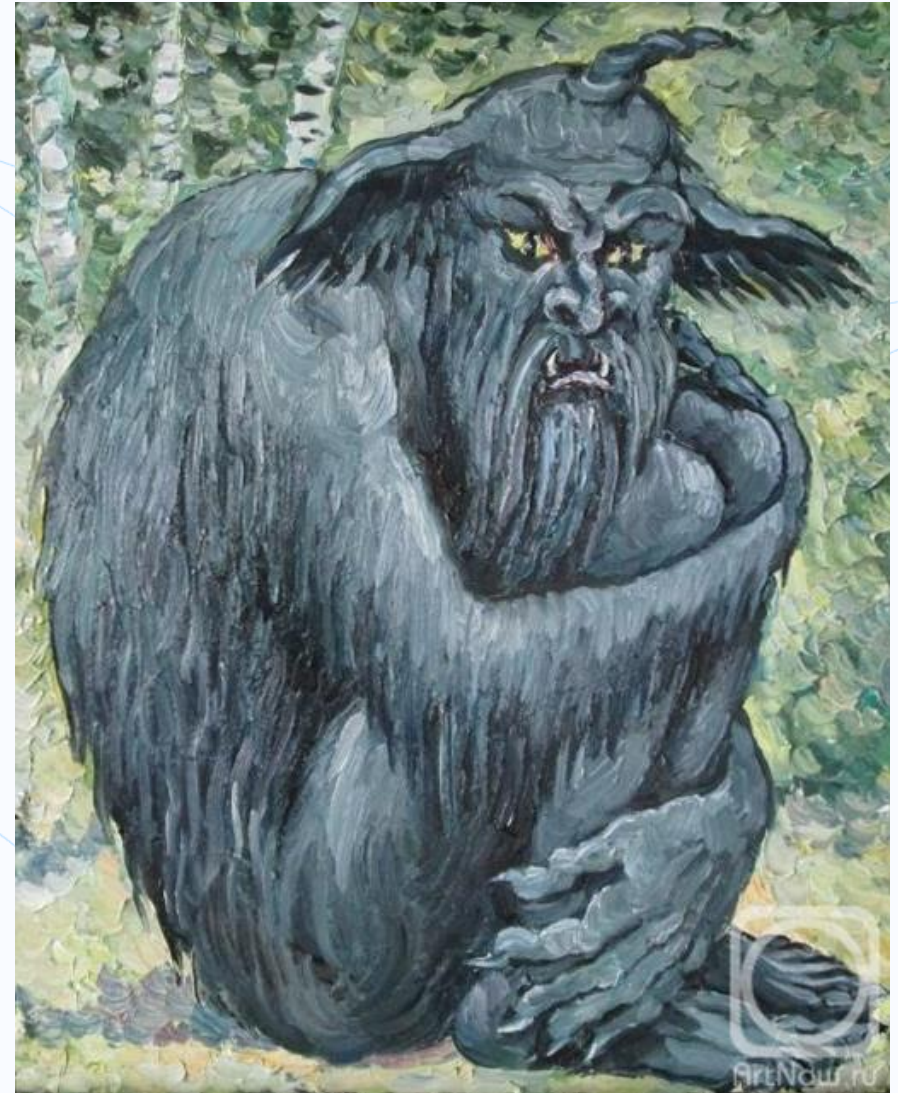
# Шурале

Шурале обитает преимущественно в лесу - в одном лесу могут обитать сразу несколько особей.

Занимается тем, что сбивает одиноко идущих по лесу людей с пути, заманивает в глухие чащи; способен защекотать до смерти своими длинными пальцами.

Шурале боится воды, что можно использовать как один из способов спастись от него — перепрыгнуть ручей. Также боится огня. Шурале можно поймать в ловушку, например, уговорив его засунуть палец в расщеплённое дерево, после чего вышибить клин.

(с) Википедия



Картина Ягужинской Анны  
artnow.ru

# Security Champion

...

Сирена

Дед Мороз

Русалка

Единорог

Валькирия

Вампир

Феникс

Зубная фея

Шурале

**Security Champion**

Йети

Оборотень

Дракон

# DISCLAIMER

**Все совпадения с реальностью  
являются чистойшей случайностью!**

# Почему есть смысл меня слушать?

## **#ктоя**

руководитель направления аудита  
безопасной разработки: выстраиваю  
процессы, занимаюсь стратегией AppSec и  
всея, что около 😊  
автор и тренер курсов DevSecOps

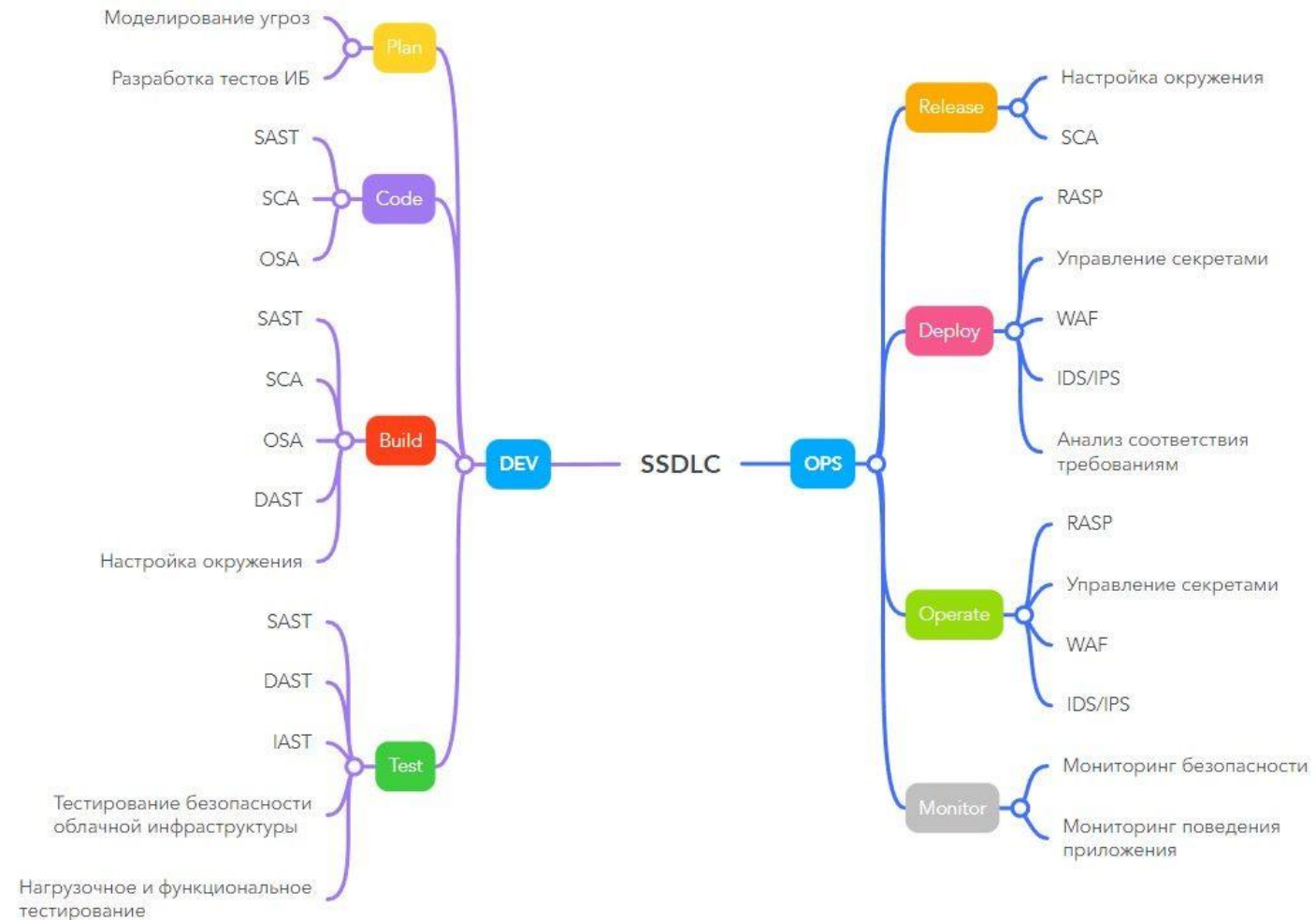
## **#ктомы**

архитекторы, консультанты, инженеры процессов  
безопасной разработки  
внедряли DevSecOps/Appsec в финтех, банки, ИТ-  
компании, здравоохранение, гос.сектор

# Агенда

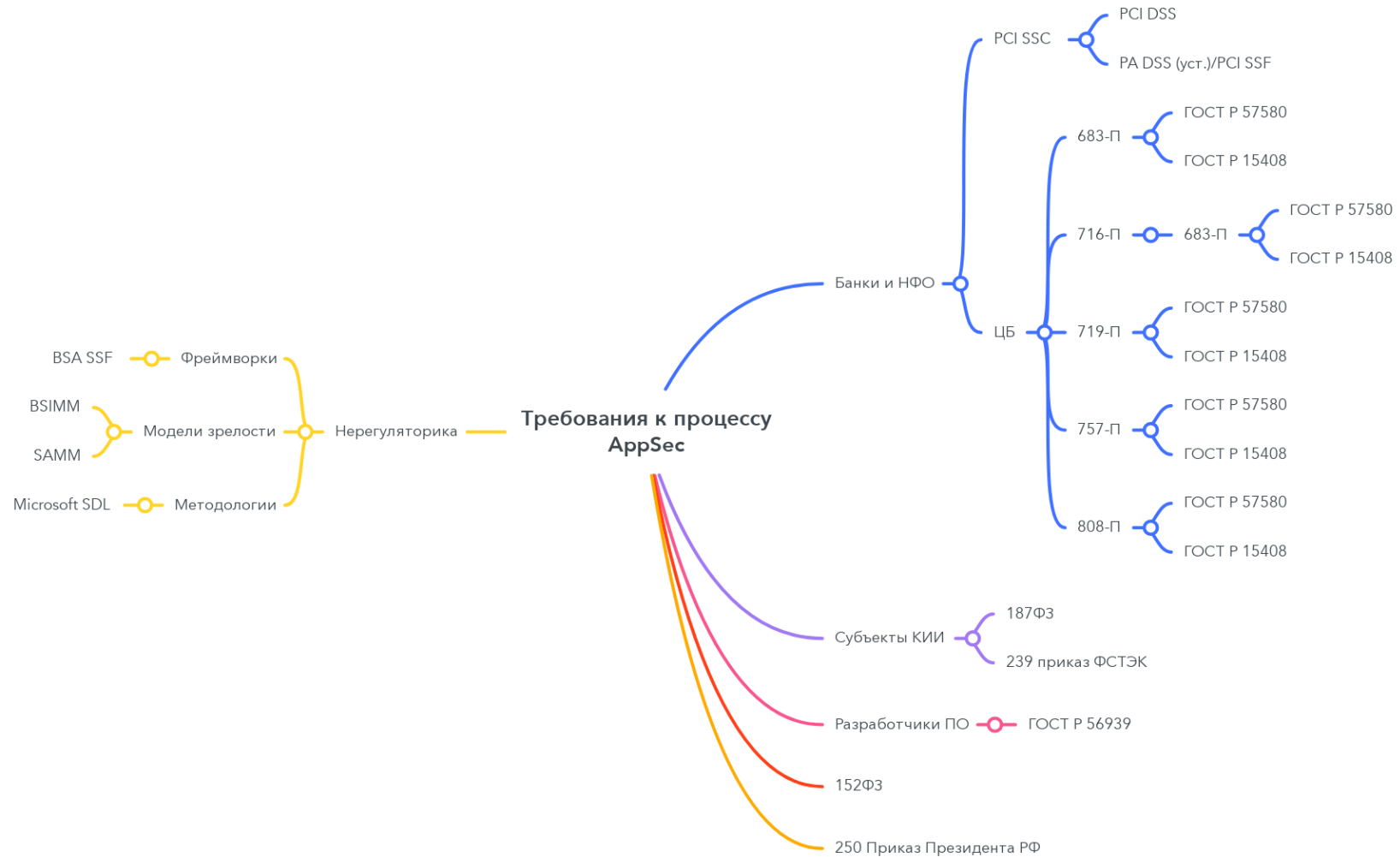
- 1. Кто такие Security Champion'ы?**
- 2. Почему они нужны и почему их нет?**
- 3. Как сделать сказку явью?**

# Лирическое отступление

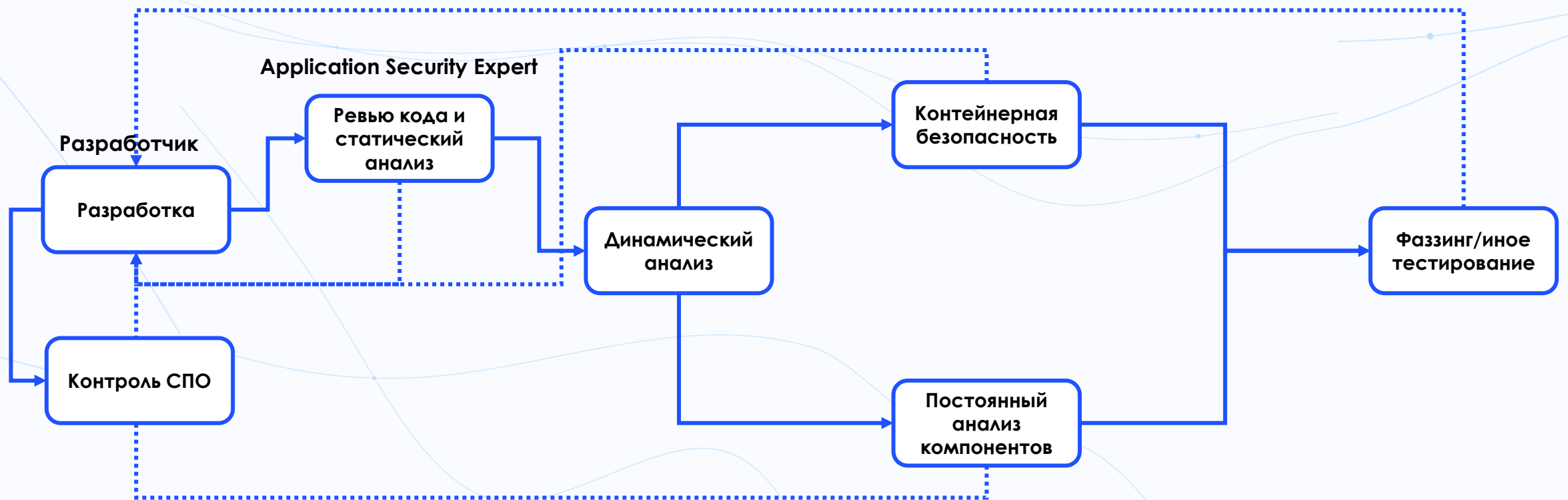




# Лирическое отступление



# Хороший DevSecOps



# Security Champion. Понять

Ну не внедряются у нас секурити чемпионы 13:02

Никому не интересно 13:02

Дело не в мотивации, а в том что непонятно им чего делать 13:03

Их нет, это миф) послушаю запись потом 10:42

AppSec Journey Chat

Их нет, это миф) послушаю запись потом

Вот и хочу попробовать его развеять 10:58

Не работает\не живёт это Либо я не видел edited 15:34

Не работает\не живёт э... Кто? Секчемпы? 16:32

Svetlana Gazizova Кто? Секчемпы? Да 16:33

Просто это оборотень, котоый должен перейти в иб, если у него есть интерес и быть закреплег за своей бывшей командой

Да камон!

10 апр в 10:39

Секьюрити Чемпионов, то их нет 17:12

Секчемпы)

Их нет, это миф) послушаю запись потом

Вот и хочу попробовать его развеять

СекChamp – как по мне, возможность «разгрузить» appsec'ов.

Они, безусловно, есть. Зачастую ими выступают team lead разработки, т.к. выставляются требования со стороны, но есть истории, когда интерес возникает со стороны dev/devops.

Чемпионы не работают. Как написали выше - все только и рассказывают про эту "пилюлю" со сцены и в своих статьях, но никто так и не показал результатов, метрик или чего-то подтверждающего, что это работает. Либо поработали год на энтузиазме, а потом практика загнулась.

Весь мир уже шагает в сторону AppSec Business Partners, отдельные компании в РФ уже внедрили/внедряют эту практику, а тут до сих пор теоретические статьи про Шампиньенов. Давайте еще про атаки типа Ping of Death или Mac Flooding писать, тоже может быть актуально

# Security Champion. Что говорит интернет?

Обычно так называют сотрудников команды разработки, выступающих в интересах группы ИБ. Они участвуют в повседневной разработке, понимают цели, процессы и особенности команды. Чемпионами могут быть QA, проект-менеджеры, разработчики — кто угодно, лишь бы сотрудник «радел» за безопасность. Чемпионы выступают в качестве «точки входа», «мостика» к безопасности приложений для своей команды.

(с) статья на Хабр  
<https://habr.com/ru/companies/vk/articles/725088/>

# Security Champion. Что говорит регулятор?

**Security Champion** – активный член команды, как правило, не являющийся сотрудником подразделения информационной безопасности, который вводит и поддерживает в рамках командных практик лучшие практики по обеспечению информационной безопасности, идентификации рисков ИБ и т.д. Такой член команды может сочетать роль Security Champion с ролью разработчика, тестировщика и др.

(с) Профиль Защиты

[https://www.cbr.ru/content/document/file/132666/inf\\_note\\_feb\\_0422.pdf](https://www.cbr.ru/content/document/file/132666/inf_note_feb_0422.pdf)

# Security Champion. Что думаю я?

**Security Champion** – *(не)вымышленный персонаж*, который находится в ИТ-команде и помогает Application Security подразделению в разборе дефектов и адаптации практик ИБ внутри своей команды.

Вопросы, которые может решать SC:

- исправление уязвимостей
- принятие риска
- security awareness/продвижение культуры
- доработка правил на инструменте

....

**и много-много чего еще!**

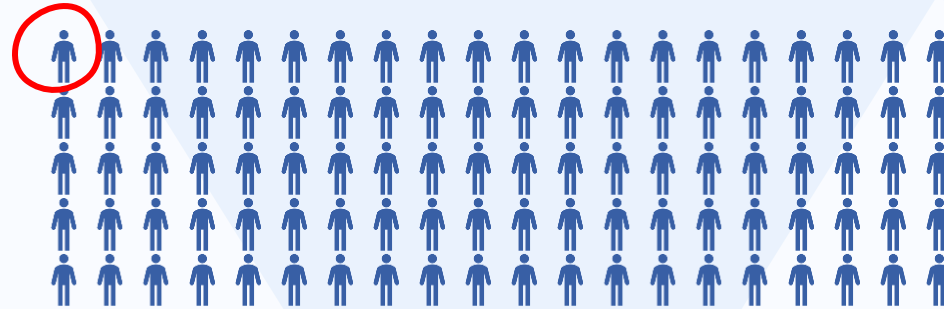


**Почему они вообще появились?**

# Мы не вывозим!

Соотношение

100:10:1



Разработчики ПО  
(Development)



Инженеры сопровождения  
(Operations)



Эксперт ИБ  
(Security)



# Автономия команд

Учитывая нехватку ИБ-кадров, нужно иметь своих «агентов» внутри команд разработки.

Помимо очевидной пользы, это позволит не контролировать работу инструментов и технический долг в каждой отдельно взятой команде разработки. Цель сделать команды разработчиков более самостоятельными и автономными может быть достигнута только при наличии знаний и понимания.

# Автономия команд



# Нелинейное развитие ИБ

Важно, чтобы безопасные методы разработки были признаны и поняты всеми командами разработчиков. Если инженеры обучают инженеров, это гораздо более успешный подход к развитию этих знаний и образования. Единственный способ масштабировать безопасную разработку — через инженерную организацию, предоставив команде безопасности полномочия и поддержку разработчиков.

# Нелинейное развитие ИБ



# Нам нужны союзники





**Почему их нет?**

# (Не)очевидные причины





# Свой среди чужих и чужой среди своих

Задачи, вроде бы, как у разработчика.  
KPI, вроде бы, как у разработчика.



# Свой среди чужих и чужой среди своих

Задачи, вроде бы, как у разработчика.  
KPI, вроде бы, как у разработчика.

**ВРОДЕ БЫ?!**

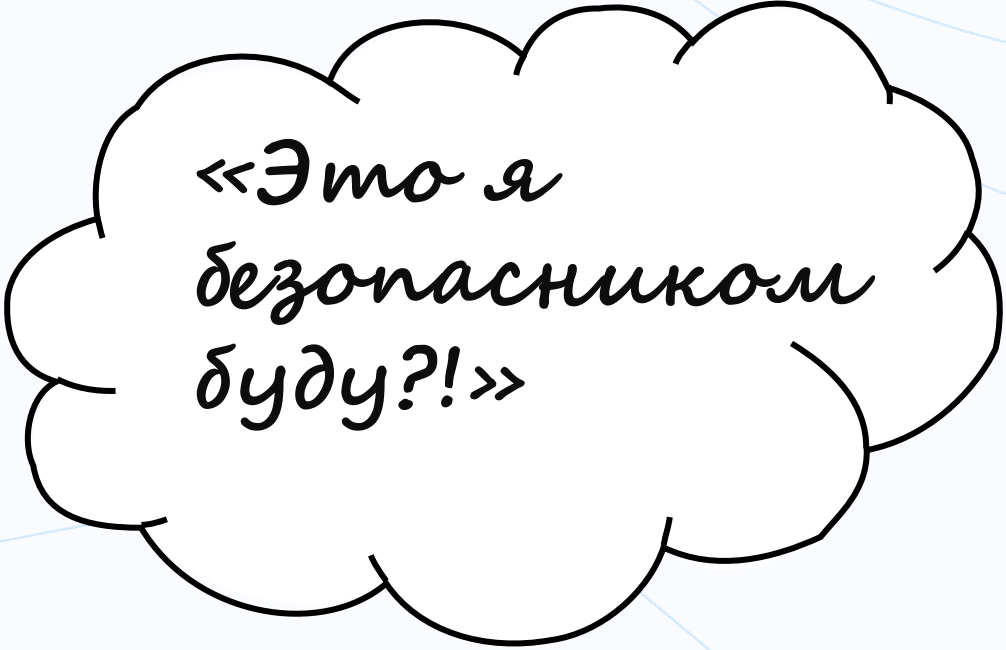
# А мне это зачем?!

«Ага, ответственность  
переложить просто  
хотят!»»

«Напиши мне письмо  
как надо и отстань»»

«Может мы все вместе  
будем это делать»»

**А мне это зачем?!**



*«Это я  
безопасником  
буду?!»»*

# Где взять *Security Champion*'ов?



**Категорическое «нет»**

**Нанять с рынка!**

**Категорическое «нет»**

~~**Нанять с рынка!**~~

**Категорическое «нет»**

**Перевести кого-то из ИБ!**

**Категорическое «нет»**

**~~Перевести кого-то из ИБ!~~**



**Категорическое «нет»**

**Прописать в должностной  
инструкции!**

**Категорическое «нет»**

**~~Прописать в должностной инструкции!~~**



**Категорическое «да»**

**Привлечь HR!**

# Привлечь HR!

Любые около-кадровые перестройки должны быть под надзором тех, кто понимает немного психологии сотрудников.

Если человек будет демотивирован, выполняя второстепенную для него работу – в чем смысл?





**Категорическое «да»**

**Поговорить с командой!**

# Поговорить с командой!

Все программы по обучению специалистов, создаются, как правило с привлечением экспертов отрасли, ресурсов извне и авторским надзором.

А учиться-то не им... **Поговорите с командой, что они хотят?**





**Категорическое «да»**

**Выделить бонусов!**

# Выделить бонусов!

## «За деньги да»

Пожалуйста, прекратите предлагать хвалить специалистов, дарить нам кружки, футболки, ручки и внутри говорить: «А вот Вася после работы еще два часа триажит!»

**ДАЙТЕ ВАСЕ ДЕНЕГ И СВОБОДУ ДЕЙСТВИЙ!**



**Прокурлыкал за AppSec!**



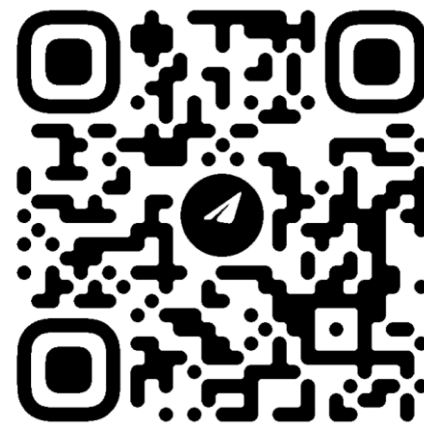
**Что можно сделать конкретно мне?**

**Спасибо, что вы здесь!**

**Визитка**



**Кое-что невошедшее**



**@APPSECJOURNEY**