



**START**

Security Trainings and Requirements Tool

**ДиалогНаука**

**Знания и навыки по безопасной  
разработке: как наладить контакт  
команды ИБ и разработчиков ПО,  
чтобы создавать и внедрять безопасные приложения.**

Вебинар. Начинаем через 5 минут

7 сентября 2021 года



# START

Security Trainings and Requirements Tool

# ДиалогНаука

# 1. Атаки через уязвимости. Кейсы 2020 и 2021 года

Как недостатки знаний и навыков продуктовых команд приводят к инцидентам безопасности



# On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them

Eduard Marin  
ESAT-COSIC and iMinds  
KU Leuven, Belgium  
eduard.marin@esat.kuleuven.be

Dave Singelee  
ESAT-COSIC and iMinds  
KU Leuven, Belgium  
dave.singelee@esat.kuleuven.be

Flavio D. Garcia  
School of Computer Science  
University of Birmingham, UK  
f.garcia@bham.ac.uk

Tom Chothia  
School of Computer Science  
University of Birmingham, UK  
t.p.chothia@cs.bham.ac.uk

Rik Willems  
Cardiology, University Hospital  
Gasthuisberg  
Leuven, Belgium  
rik.willems@uzleuven.be

Bart Preneel  
ESAT-COSIC and iMinds  
KU Leuven, Belgium  
bart.preneel@esat.kuleuven.be

## ABSTRACT

Implantable Medical Devices (IMDs) typically use proprietary protocols with no or limited security to wirelessly communicate with a device programmer. These protocols enable doctors to carry out critical functions, such as changing the IMD's therapy or collecting telemetry data, without having to perform surgery on the patient. In this paper, we fully reverse-engineer the proprietary communication protocol between a device programmer and the latest generation of a widely used Implantable Cardioverter Defibrillator (ICD) which communicate over a long-range RF channel (from two to five meters). For this we follow a black-box reverse-engineering approach and use inexpensive Commercial Off-The-Shelf (COTS) equipment. We demonstrate that reverse-engineering is feasible by a weak adversary who has limited resources and capabilities without physical access to the devices. Our analysis of the proprietary protocol results in the identification of several protocol and implementation weaknesses. Unlike previous studies, which found no security measures, this article discovers the first known attempt to obfuscate the data that is transmitted over the air. Furthermore, we conduct privacy and Denial-of-Service (DoS) attacks and give evidence of other attacks that can compromise the patient's safety. All these attacks can be performed

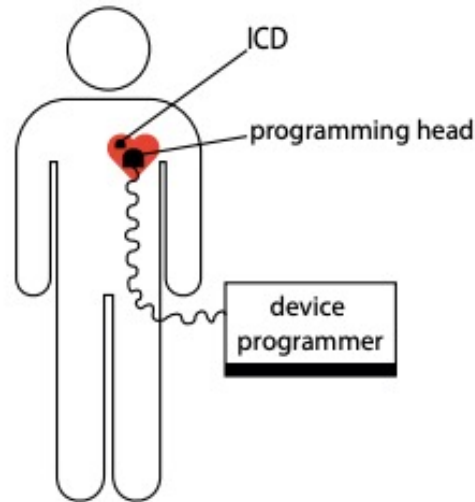
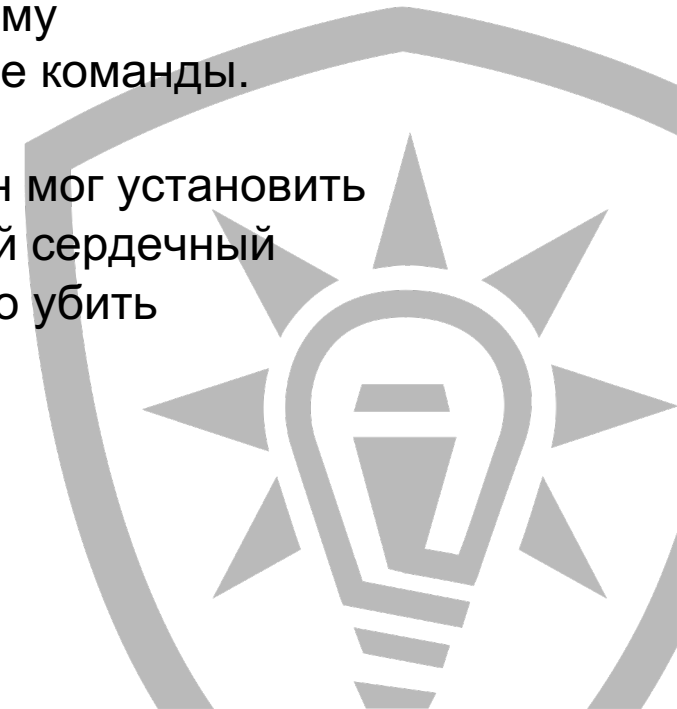


Figure 1: ICD activation procedure

В 2016 году в нескольких моделях кардиостимуляторов обнаружили [смертельно опасные уязвимости](#).

С их помощью злоумышленник мог получить удаленный доступ к имплантированному пациенту кардиоустройству, а затем отправлять ему произвольные команды.

Например, он мог установить некорректный сердечный ритм и просто убить пациента.



# Из электронных трудовых некоторых россиян начал пропадать стаж

Из цифровых трудовых книжек пропала информация о стаже работы на ликвидированных фирмах

  20  181      Добавить в «Мою Л



Фото  
Ново

## Пост Лукацкого

Пост не про ИБ, а про криворуких программистов и архитекторов одного фонда, который не подумал, что при ликвидации компании, запись о ней ликвидируется из электронных трудовых книжек всех, кто в этой компании работал. Но самое печальное во всей этой истории не руки программистов и слабомумие архитекторов, а то, что в случае целенаправленного воздействия на систему, доказать что-то будет нереально. Обратите внимание, что ПФР отказывается принимать в качестве доказательства бумажную трудовую, а как иначе доказать факт работы непонятно. Если кто-то захочет создать напряженность в обществе "мама не горюй", то не надо будет красть деньги со счетов граждан, достаточно будет обнулить все их электронные трудовые. И вот тогда мы действительно вернемся в каменный век 🙄



 2116 00:54

Из электронных трудовых книжек стала исчезать информация о стаже работы на ликвидированных предприятиях. Из-за этого некоторые россияне рискуют остаться без положенной пенсии, **пишет** «Ридус».

<https://lenta.ru/news/2021/08/27/staz/>



# Майнинг еды или «Пятерочка» глазами хакера

Информационная безопасность\*

Из песочницы

## Введение

Написать этот пост меня вдохновила [статья, которая давно висит на Ха](#) перед автором, лучше названия и придумать нельзя. Как вы все знаете рекламирует свои карты лояльности. В статье выше нам рассказывали активируют чужие карточки и списывают баллы. Хакеры пошли дальше карт просто стали взламывать личные кабинеты пользователей. А что? активации карт, давайте разберёмся поподробнее.

## Немного о безопасности личных кабинетов

### Вход в личный кабинет

По номеру телефона    По номеру карты

---

Номер телефона

Пароль


[Забыли пароль?](#)

**ВОЙТИ**

### Получили карту Пятёрочка

Не забудьте активировать, чтоб тратить накопленные баллы

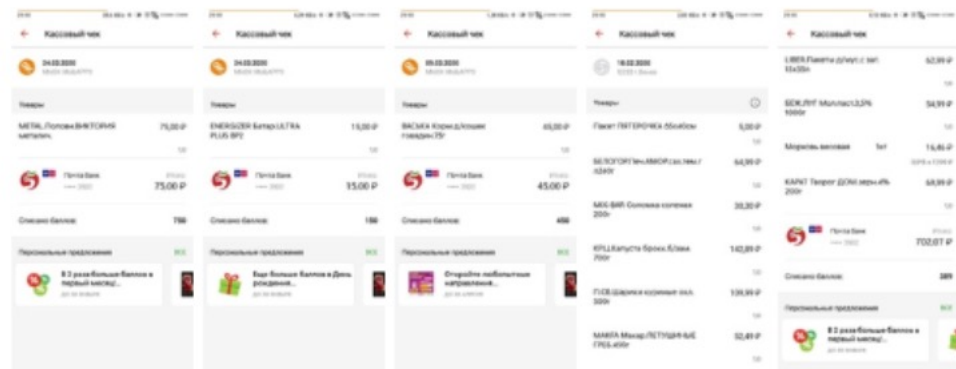
**Активировать карту**





**Александр Рогожин** 25 мар 2020 в 22:14

Надоели списания с выручай карты левые непонятно кем! Объясните 3 первых списан приложил где я сам списывал, при чем здесь значек одноклассников? Обратился 9 ма марта и опять кто-то их списал 24! Опять 2 недели ждать что б на следующий день спи [Посмотреть все изображения](#)



Ответить



**Александр Еговцев** 24 мар 2020 в 11:48

Пятёрочка, может вы подскажете? Гугл особо не помог. Постоянно приходят коды по Картой бонусной давно не пользуюсь

12:47

Pyaterochka

Ваш код подтверждения: 8053

02.02.17

Ваш код подтверждения: 3998

14.03.18.45

<https://habr.com/ru/post/538602/>

# ГОСТ Р 56939—2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования

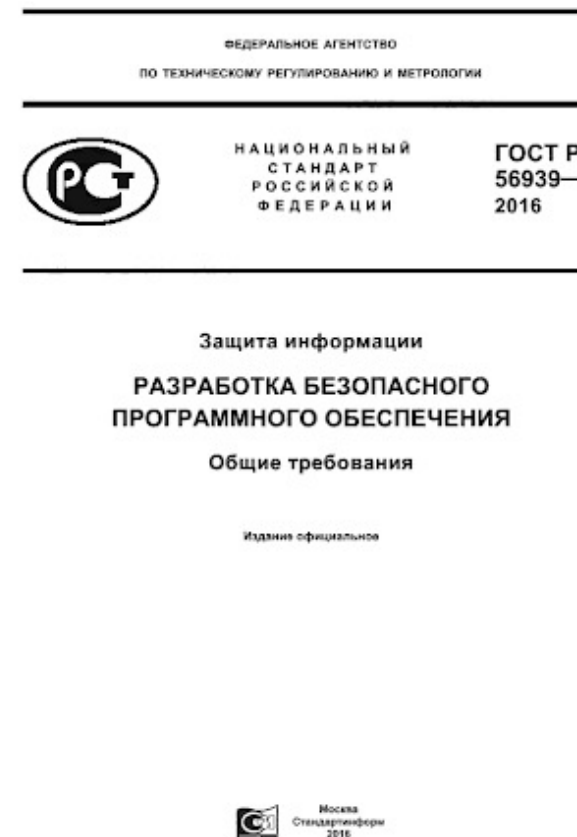
5.1.3.1 Разработчик ПО должен определить требования по безопасности, предъявляемые к разрабатываемому ПО.

5.2.1 Для организации работ, выполняемых в процессах жизненного цикла ПО, и подтверждения соответствия требованиям настоящего стандарта документация разработчика ПО должна содержать перечень определенных требований по безопасности, предъявляемых к разрабатываемому ПО.

Меры по разработке безопасного программного обеспечения, подлежащие реализации

При выполнении проектирования архитектуры программы разработчик ПО должен реализовать следующие меры:

- моделирование угроз безопасности информации;
- уточнение проекта архитектуры программы с учетом результатов моделирования угроз безопасности информации



# Gartner. Secure Design and Threat Modeling. Application security requirements and threat management (ASRTM).

Threat modeling and security requirements gathering are advocated as secure design practices which help application teams anticipate — and eliminate — potential threats and design flaws before code is written.

Despite this, the time required to carry out these activities as manual tasks makes them a poor fit for agile and DevOps practices. This, coupled with a general lack of application security skills and expertise, has resulted in few organizations routinely including formal (versus ad hoc) threat modeling in application development projects. Security requirements are often broadly set across all projects instead of adapted to the specifics of each application technology stack, overburdening low-risk projects and not properly securing high-risk ones. These requirements are often not updated to reflect new technologies or are not detailed enough to cover technology specific implementation details and secure coding practices.

ASRTM can be integrated into a wide variety of SDLC tooling, as well as with GRC tools, helping to bridge the gap with GRC teams.

**Gartner**®



КЛАССИЧЕСКИЙ ТРУД  
ИСПРАВЛЕННОЕ И ДОПОЛНЕННОЕ ИЗДАНИЕ

# Искусство программирования

ТОМ 1

Основные алгоритмы  
Третье издание

ДОНАЛЬД Э. КНУТ

## Разработчики: ожидание

Сдаем продукт / проект в срок  
и с наилучшим качеством

Все требования выполнены

Надо пройти «эту дурацкую  
приемку»





Начните управлять компьютером,  
написав свою первую программу!



# Программирование

## ДЛЯ ЧАЙНИКОВ®

4-е издание

Для  
сомневающихся

На компакт-диске —  
компиляторы и коды  
на нескольких языках  
программирования

Уоллес Вонг

Автор книги  
Microsoft Office 2007  
для чайников



 ДИАЛЕКТИКА  
www.dialektika.com

## Разработчики: реальность

Какие угрозы актуальны?

В чем реальные риски?

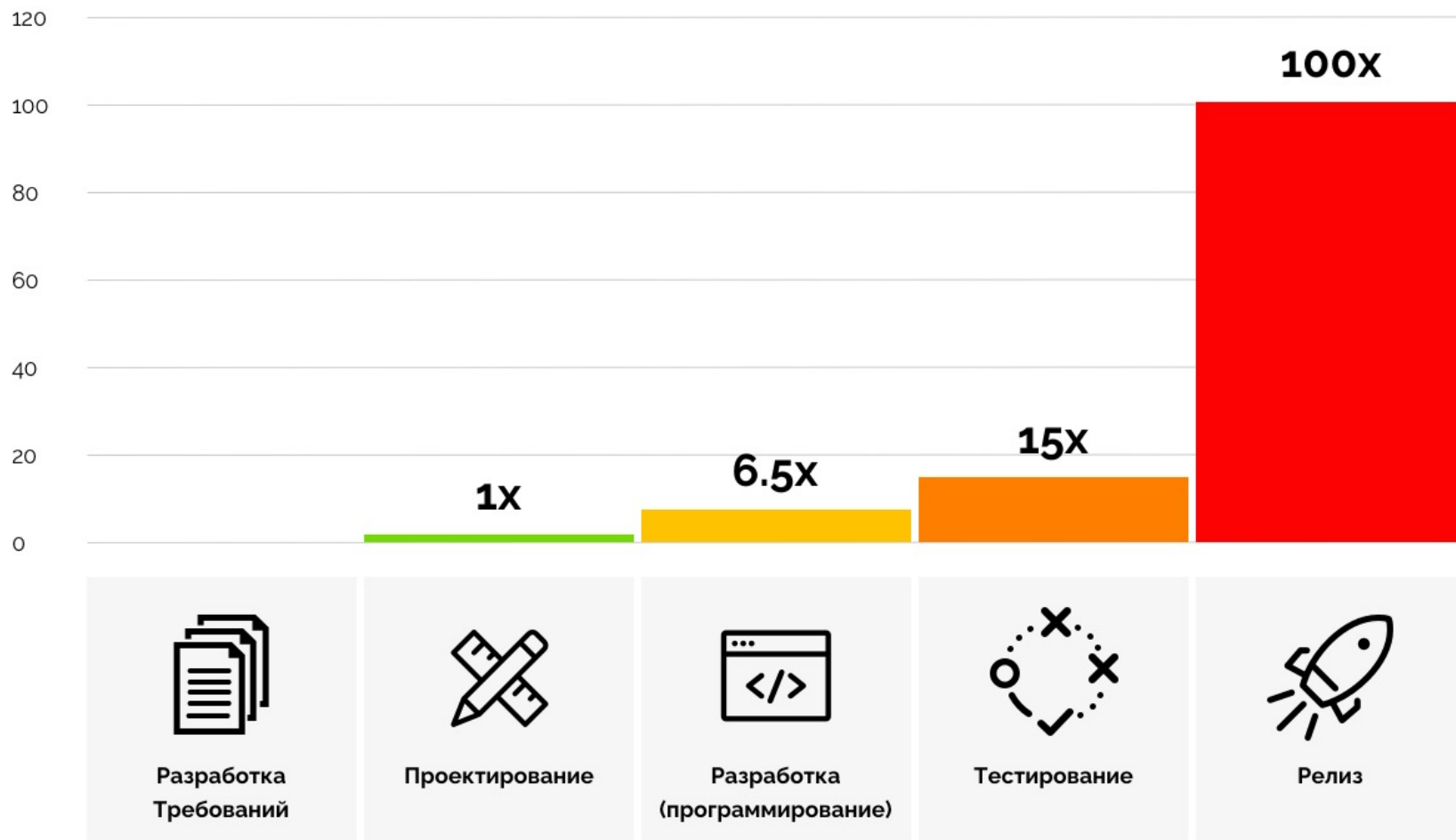
Как писать безопасный код?

+ карго-культ

Какие могут быть проблемы  
с окружением?



## Относительная стоимость устранения дефектов ПО на разных этапах разработки





**START**

Security Trainings and Requirements Tool

**ДиалОгНаука**

## 2. Как сформировать требования по ИБ к ПО

и сделать их понятными для команды



# Создать и наполнять базу требований



ГОСТ Р 56939-2016

«Защита информации. Разработка безопасного программного обеспечения».

Положение Банка России от 4 июня 2020 г. № 719-П  
«О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

Приказ ФСТЭК N 17

Android:

[OWASP Mobile ASVS + Testing guide](#)

[Google Android Security Tips](#)

iOS

[OWASP Mobile ASVS + Testing guide](#)

[iOS Security](#)

Web

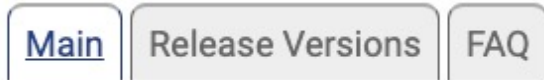
[OWASP Web Testing Guide](#)

[Payment Card Industry Data Security](#)

[Standard](#)



# Учитывая все требования стандартов, руководств и лучших практик



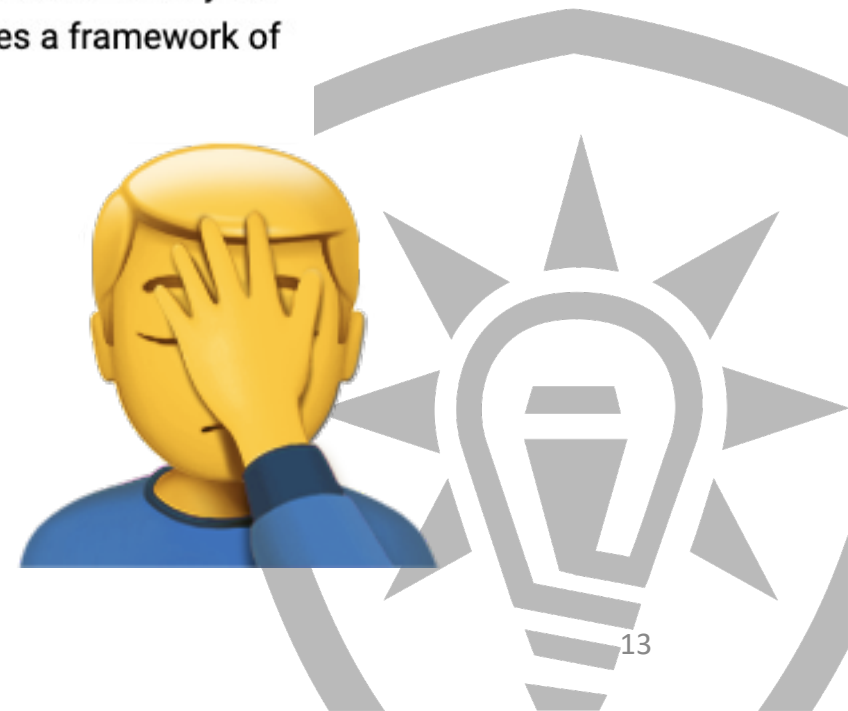
Пример: OWASP Web Security Testing Guide v4.1



The Web Security Testing Guide (WSTG) Project produces the premier cybersecurity testing resource for web application developers and security professionals.

The WSTG is a comprehensive guide to testing the security of web applications and web services. Created by the collaborative efforts of cybersecurity professionals and dedicated volunteers, the WSTG provides a framework of best practices used by penetration testers and organizations all over the world.

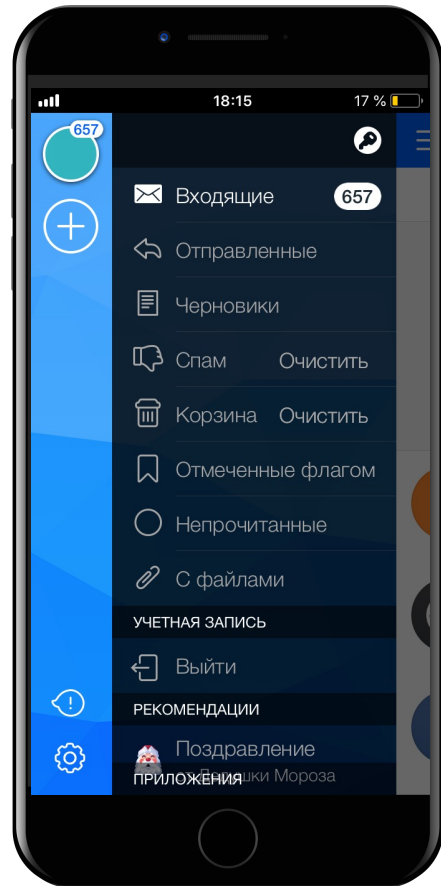
«OWASP спустя 6 лет (только вдумайтесь, где был вебчик 6 лет назад и сейчас!) наконец обновило свое руководство по тестированию безопасности веб-приложений...»



# Уровни требований по информационной безопасности



# Пример: приложение для клиентов



Интеграция с корпоративными системами и авторизация через доменные учетные записи.

Доступ к проектным данным заказчиков и персональным данным клиентов.

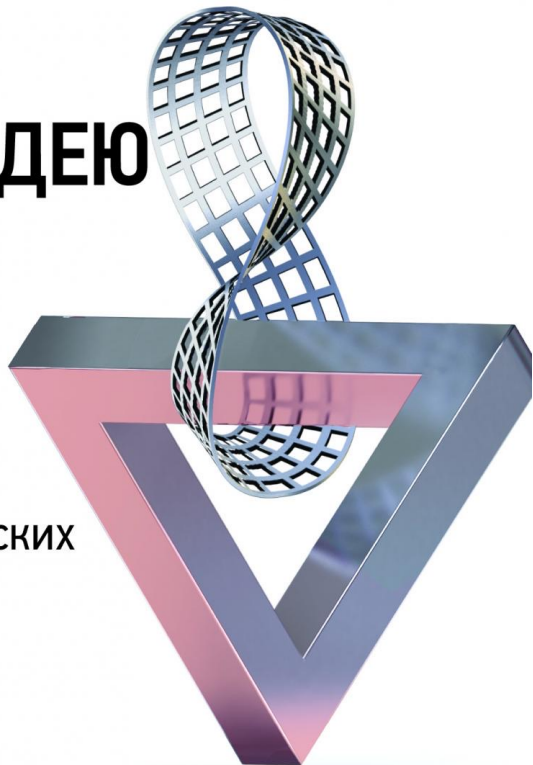
Mobile Application Security Requirements - Android

ID	MSTG-ID	Detailed Verification Requirement	Level 1	Level 2	Status
<b>V1</b>		<b>Architecture, design and threat modelling</b>			
1.1	MSTG-ARCH-1	All app components are identified and known to be needed.	✓	✓	
1.2	MSTG-ARCH-2	Security controls are never enforced only on the client side, but on the respective remote endpoints.	✓	✓	
1.3	MSTG-ARCH-3	A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	✓	✓	
1.4	MSTG-ARCH-4	Data considered sensitive in the context of the mobile app is clearly identified.	✓	✓	
1.5	MSTG-ARCH-5	All app components are defined in terms of the business functions and/or security functions they provide.		✓	N/A
1.6	MSTG-ARCH-6	A threat model for the mobile app and the associated remote services has been produced that identifies potential threats and countermeasures.		✓	N/A
1.7	MSTG-ARCH-7	All security controls have a centralized implementation.		✓	N/A
1.8	MSTG-ARCH-8	There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.		✓	N/A
1.9	MSTG-ARCH-9	A mechanism for enforcing updates of the mobile app exists.		✓	N/A
1.10	MSTG-ARCH-10	Security is addressed within all parts of the software development lifecycle.		✓	N/A
1.11	MSTG-ARCH-11	A responsible disclosure policy is in place and effectively applied.		✓	N/A

Генрих  
Альтшуллер

## НАЙТИ ИДЕЮ

Введение  
в ТРИЗ —  
теорию  
решения  
изобретательских  
задач



“ Генрих Альтшуллер навсегда войдет в мировую историю мысли не только потому, что разработал ТРИЗ и ввел понятия технического и физического противоречий. Он доказал: каждый из нас может существенно улучшить свою способность находить решения самых сложных задач в любой области. Эта книга еще долго будет настольной для всякого желающего жить разумно. ”

Анатолий Вассерман

# Идеальный конечный результат

Как найти самое сильное решение задачи, не решая её?

[Генрих Альтшуллер](#) нашел такой способ.

В 50-е годы он предложил до решения задачи сформулировать самый желанный ответ, пусть даже и невыполнимый, и назвал его [ИКР — Идеальное Конечное Решение](#)



Генрих  
Альтшуллер

## НАЙТИ ИДЕЮ

Введение  
в ТРИЗ —  
теорию  
решения  
изобретательских  
задач



“ Генрих Альтшуллер навсегда войдет в мировую историю мысли не только потому, что разработал ТРИЗ и ввел понятия технического и физического противоречий. Он доказал: каждый из нас может существенно улучшить свою способность находить решения самых сложных задач в любой области. Эта книга еще долго будет настольной для всякого желающего жить разумно. ”

Анатолий Вассерман

# Как сформировать требования по ИБ к ПО и сделать их понятными для команды?

Корректные требования по ИБ  
к ПО формируются командами  
самостоятельно и автоматически



## START

Security Trainings and Requirements Tool





**START**

Security Trainings and Requirements Tool

**ДиалОгНаука**

# 3. Как убедиться, что требования по ИБ актуальны

в условиях постоянных изменений



# Поддерживать знания актуальными

Изменения в стеке технологий

Обновления стандартов

Обнаруженные уязвимости

Публичные инциденты

Обратная связь от процессов тестирования требований: пентест, ПСИ, SAST/DAST и другие методы

Модерация, уведомления об изменениях

SANS

Newsletters

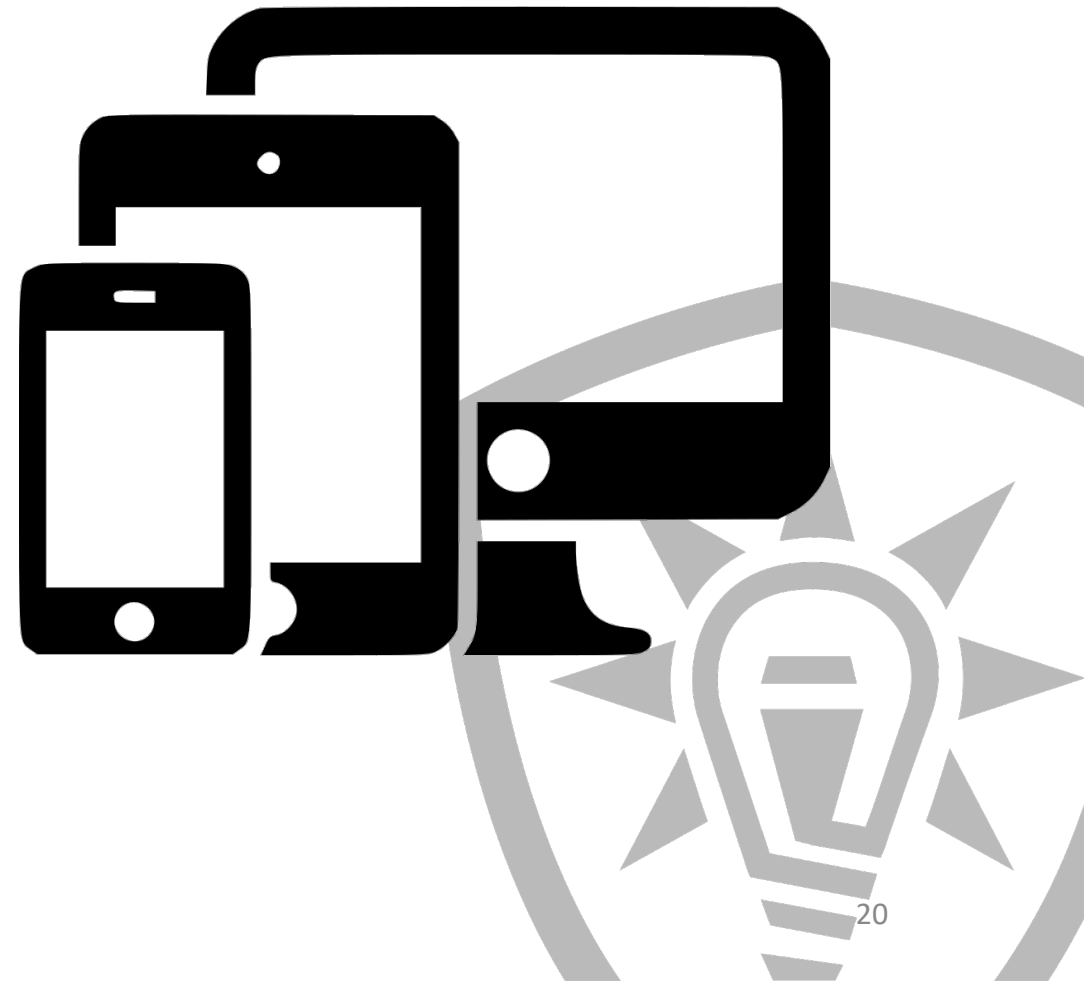
<https://www.sans.org/newsletters/>



# Определить приоритеты и нужный объем знаний для ваших разработчиков

1. Python
2. JavaScript
3. Java
4. C#
5. PHP
6. C++
7. R
8. SQL
9. Swift
10. C

[https://geekbrains.ru/posts/2019\\_lang\\_trends](https://geekbrains.ru/posts/2019_lang_trends)





Генрих  
Альтшуллер

## НАЙТИ ИДЕЮ

Введение  
в ТРИЗ —  
теорию  
решения  
изобретательских  
задач



“ Генрих Альтшуллер навсегда войдет в мировую историю мысли не только потому, что разработал ТРИЗ и ввел понятия технического и физического противоречий. Он доказал: каждый из нас может существенно улучшить свою способность находить решения самых сложных задач в любой области. Эта книга еще долго будет настольной для всякого желающего жить разумно. ”

Анатолий Вассерман

# Как убедиться, что требования по ИБ всегда актуальны?

Требования обновляются автоматически при любом изменении конфигурации ПО, стандартов и нормативных документов.

Изменения сразу видны у инженерных команд

 Jira Software

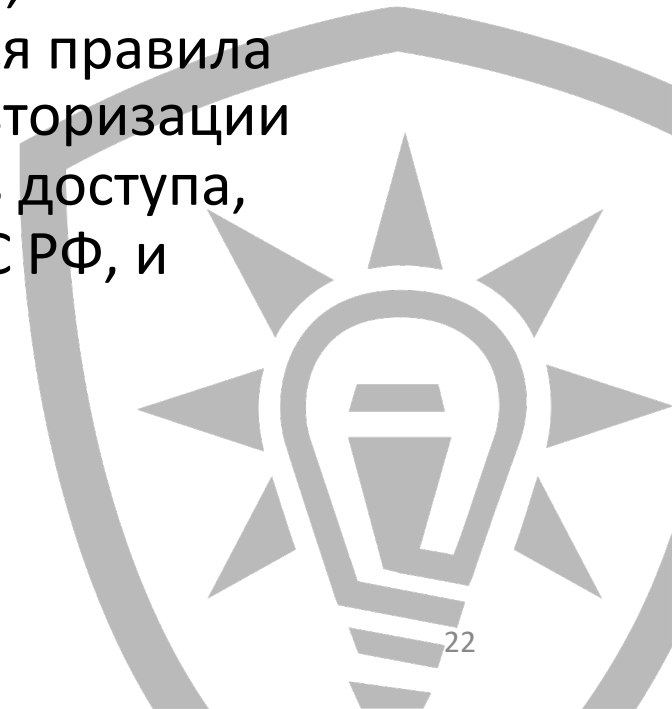
# Сделать маппинг требований



OWASP: ошибки подсистемы аутентификации должны обрабатываться безопасно и не позволяют атакующему войти в АС.



Стандарт Банка России: должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры: идентификации, аутентификации, авторизации субъектов доступа, в том числе внешних субъектов доступа, которые не являются работниками организации БС РФ, и программных процессов (сервисов).



Генрих  
Альтшуллер

## НАЙТИ ИДЕЮ

Введение  
в ТРИЗ —  
теорию  
решения  
изобретательских  
задач



“ Генрих Альтшуллер навсегда войдет в мировую историю мысли не только потому, что разработал ТРИЗ и ввел понятия технического и физического противоречий. Он доказал: каждый из нас может существенно улучшить свою способность находить решения самых сложных задач в любой области. Эта книга еще долго будет настольной для всякого желающего жить разумно. ”

Анатолий Вассерман

# Как убедиться, что требования по ИБ всегда актуальны?

Требования из разных стандартов и от разных регуляторов автоматически сопоставляются в единые, референсные требования без противоречий и дублирования



# START

Security Trainings and Requirements Tool





# START

Security Trainings and Requirements Tool

# ДиалОгНаука

## 4. Как научить разработчиков писать безопасный код

сразу и по умолчанию, а не после очередного пентеста



# OWASP Top Ten

[Main](#)[Translation Efforts](#)[Sponsors](#)[Data 2020](#)

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Globally recognized by developers as the first step towards more secure coding.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

## Top 10 Web Application Security Risks

**A1:2017-Injection:** Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

**A2:2017-Broken Authentication:** Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

Watch




151

Star

548

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

### Project Information

[NEW Website](#) [Flagship Project](#) [Documentation](#) [Builder](#) [Defender](#)[Current Version \(2017\)](#)

### Downloads or Social Links

[Download](#)[Other languages → tab 'Translation Efforts'](#)[Twitter](#)

### Code Repository

[repo](#)





CAPTURE THE FLAG



IV 卡斯基 INDUSTRIAL

CTF

2019



卡斯基 SECURITY ANALYST SUMMIT

OPEN 24/7 HOURS

IV

卡斯基

INDUSTRIAL

CTF

2019





## OWASP WebGoat

[Main](#)[Goals](#)[Lessons](#)[Start](#)[WebWolf](#)

WEBGOAT

release **v8.0.0.M26**

### Learn the hack - Stop the attack

WebGoat is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open source components.

### Description

Web application security is difficult to learn and practice. Not many people have full blown web applications like online book stores or online banks that can be used to scan for vulnerabilities. In addition, security professionals frequently need to test tools against a platform known to be vulnerable to ensure that they perform as advertised. All of this needs to happen in a safe and legal environment.

Even if your intentions are good, we believe you should never attempt to find vulnerabilities without permission. The primary goal of the WebGoat project is simple: create a de-facto interactive teaching environment for web application security. In the future, the project team hopes to extend WebGoat into becoming a security benchmarking platform and a Java-based Web site Honeypot.

**WARNING 1:** *While running this program your machine will be extremely vulnerable to attack. You should disconnect from the Internet while using this program.* WebGoat's default configuration binds to localhost to

Watch

6

★ Star

8

<https://owasp.org/www-project-webgoat/><https://www.hackthissite.org/>

the security of software through its  
ed open source software  
dreds of chapters worldwide,  
tens of thousands of members, and by  
hosting local and global conferences.

### Home

[Home page](#)

### Downloads

[Standalone jar](#)[Docker Image](#)

### Code Repository

[Source code](#)

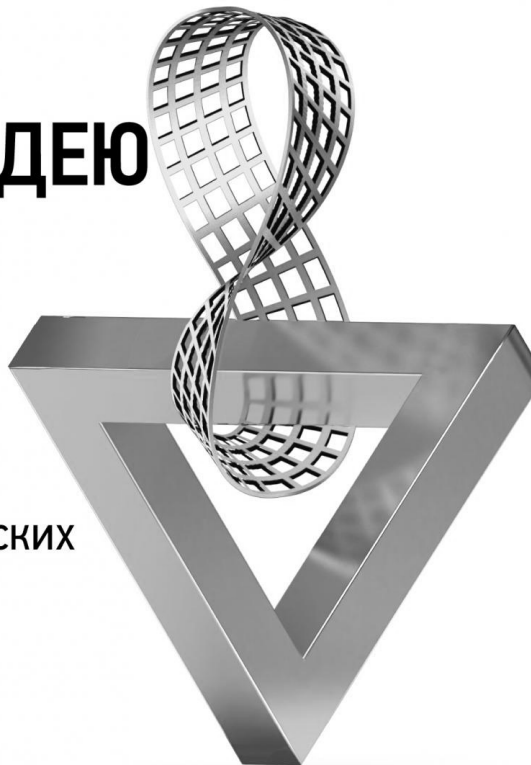
### Helping the Goat!

[Report an issue](#)[Contributing to WebGoat](#)[Forking WebGoat in GitHub](#)[Solutions](#)

Генрих  
Альтшуллер

## НАЙТИ ИДЕЮ

Введение  
в ТРИЗ —  
теорию  
решения  
изобретательских  
задач



“ Генрих Альтшуллер навсегда войдет в мировую историю мысли не только потому, что разработал ТРИЗ и ввел понятия технического и физического противоречий. Он доказал: каждый из нас может существенно улучшить свою способность находить решения самых сложных задач в любой области. Эта книга еще долго будет настольной для всякого желающего жить разумно. ”

Анатолий Вассерман

# Как научить разработчиков писать безопасный код?

Каждый разработчик вместе с требованиями видит конкретные примеры и практики реализации.



# START

Security Trainings and Requirements Tool



Условный злоумышленник может с помощью веб-инспектора изменить значения атрибутов и ввести в форму всё что угодно.

[1. Обработка входных данных и взаимодействие с внешними подсистемами](#)

[2.1 Детальные требования](#)

[2.2 Экранирование при работе с SQL](#)

[2.3 Кодирование и экранирование при работе с браузерами](#)

[3 Защита от подделки запросов \(CSRF\)](#)

[4 Безопасная инициализация XML-парсеров](#)

[5 Загрузка файлов на сервер](#)

[6 Аутентификация, управление сессиями и восстановление паролей](#)

[7 Авторизация и разграничение доступа](#)



# START

Security Trainings and Requirements Tool

октябрь 2021



# START

Security Trainings and Requirements Tool

# ДиалогНаука

## 5. Антифишинг. START

Security Trainings and Requirements Tool: система управления требованиями по информационной безопасности и обучения разработчиков ПО вопросам безопасной разработки





Admin

Проекты

Системы

Настройки

Выйти

Статусы ▾

Теги (2) ▾

Владелец требования

Эксперт по ИБ

Эксперт по инфраструктуре

Владелец продукта

Регуляторы ▾

Технические. Защита клиентской части

Технические. Безопасность подключений

Архитектура и Дизайн

Технические. Идентификация и аутентификация

Admin

Проекты

Системы

Настройки

Выйти

## Мои проекты

[+ Добавить Проект](#)

Проект	Систем	Требований	Последняя активность	Действия
<b>Модернизация ДБО</b> тестовый проект в компании	2	129	10 дней назад →	
<b>СЗ ПДн</b> Новый проект над которым мы работаем	4	200	22 дня назад ↘	

**Тестовый проект**  
Проект по модернизации АС

Коллекции требований

**Банк России**

**PCI Security Standards Council**

Приложение № 1 к Протоколу испытаний АС на соответствие требованиям по ИБ

№ п/п	Код	Формулировка требования	Результат испытания и замечания	Критичность	Срок устранения замечаний
1	AR	<b>Архитектура и Дизайн</b>			
2	AR3	Для взаимодействия с другими приложениями и компонентами должны использоваться учетные записи, обладающие минимально необходимыми полномочиями.	Без замечаний	Средняя	
3	CO	<b>Технические. Общие требования и документирование</b>			
4	CO1	В документации на приложения должны быть перечислены все используемые криптографические библиотеки, цели и способы их	Без замечаний	Высокая	

Антифишинг  
admin

Проекты

Системы

Настройки

Выйти



## Мои проекты

+ Добавить Проект

Проект	Систем	Требований	Последняя активность	Действия
<b>Банк №1</b> Новый проект над которым мы работаем	7	607	Сейчас	
<b>Магазин</b>	1	120	44 дня назад	

### Коллекции требований



Банк России



ФИНТЕХ  
АССОЦИАЦИЯ







# START

Security Trainings and Requirements Tool

# ДиалогНаука

## 6. Бесплатные материалы для клиентов ДиалогНауки

Примеры требований по ИБ на этапах DevSecOps

Применение START в рамках DevSecOps

Базовый набор требований по ИБ



# Примеры требований по информационной безопасности из Антифишинг. START на этапах DevSecOps

**T** - Тип требования    **K** - Критичность    **I** - Инструмент

Передача информации между компонентами приложения и другими приложениями должна осуществляться только по защищенным протоколам

- T** Документационное / Техническое
- K** Высокая
- I** Анализ документации / Ручное тестирование по ИБ

- На проект должен быть назначен эксперт по защите информации
- T** Организационное
- K** Высокая

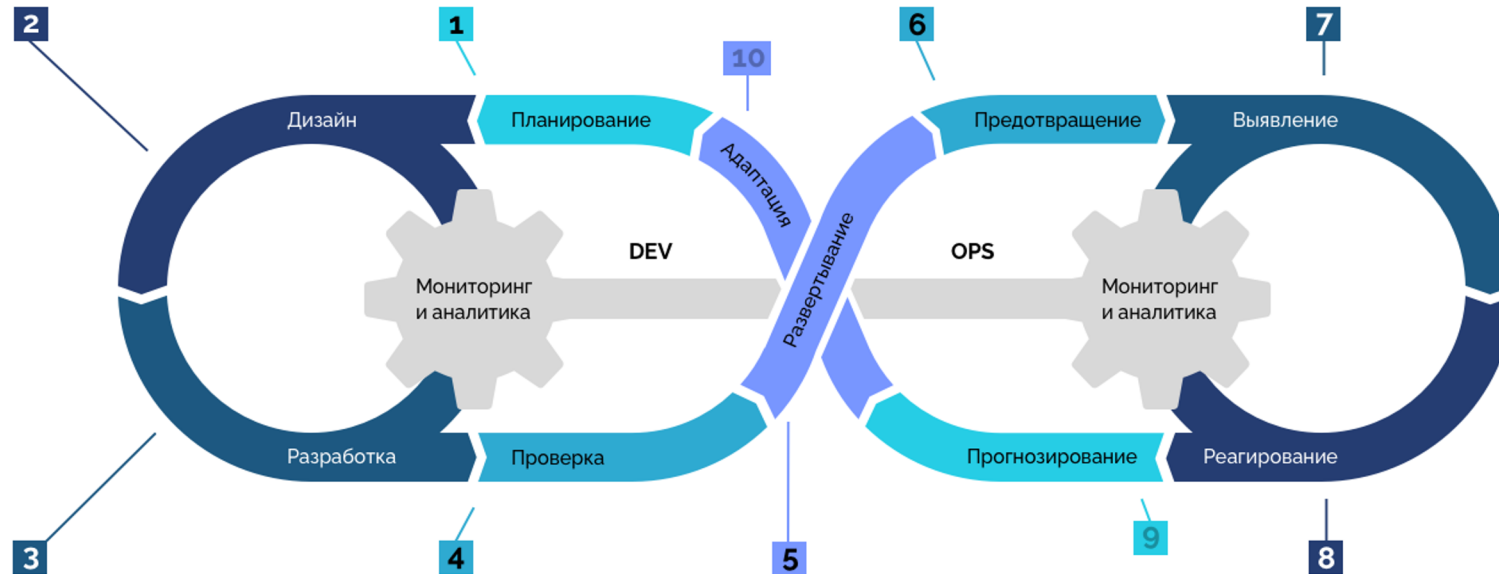
Выполненные на этапах производства ПО требования позволяют в полной мере применять механизмы безопасности на этапах его эксплуатации.

Приложение обнаруживает и реагирует на наличие root или jailbreak. В случае выявления либо уведомляя пользователя, либо прекращает работу

- T** Техническое
- K** Средняя
- I** Ручное функциональное тестирование

Должно осуществляться уведомление пользователя в случае выявления попыток входа в приложения(как успешных, так и не успешных) из необычного окружения

- T** Техническое
- K** Низкая
- I** Ручное функциональное тестирование



В приложении реализован SSL pinning и соединение с серверами, которые предлагают другой сертификат или ключ, даже если они подписаны доверенным центром сертификации (CA) не устанавливается.

- T** Техническое
- K** Высокая

Для подключения приложения в контур CI/CD необходимо провести предварительную интеграцию с системой статического анализа приложений

- T** Техническое

Операционная система на базе которой функционирует приложение должна быть настроена в соответствии с рекомендациями вендора по обеспечению информационной безопасности

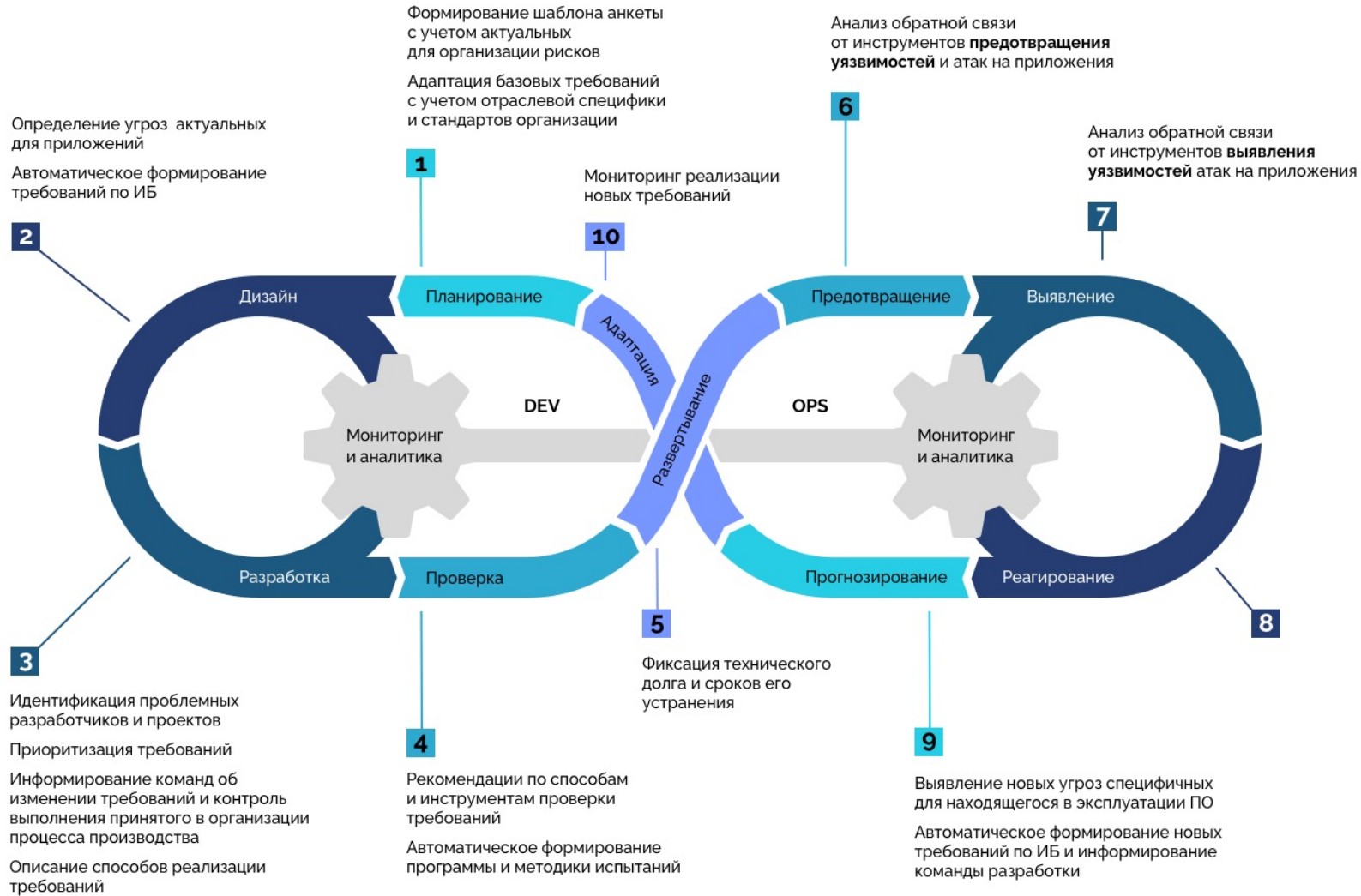
- T** Техническое
- K** Средняя

Приложение информирует пользователей о всех важных действиях с их учетной записью. Пользователи могут просматривать список устройств, просматривать дополнительную информацию (IP-адрес, местоположение и т.д.), и блокировать конкретные устройства.

- T** Техническое
- K** Низкая



# Применение Антифишинг. START в процессах DevSecOps





# Специализированный набор требований

по информационной безопасности  
для мобильных приложений  
на языке продуктовых команд



**START**  
Security Trainings and Requirements Tool

Грамотные сотрудники, разработчики ПО  
и инженерные команды – ваша лучшая защита.

Обучайте и тренируйте своих людей.

**START**

Security Trainings and Requirements Tool

[ask@antiphish.ru](mailto:ask@antiphish.ru)

[www.antiphish.ru/products/start](http://www.antiphish.ru/products/start)

**ДиалОГНаука**

[marketing@dialognauka.ru](mailto:marketing@dialognauka.ru)

[www.dialognauka.ru](http://www.dialognauka.ru)