



START

Security Trainings and Requirements Tool



Как снизить риски и быстрее внедрять инновации в банке

Налаживаем контакт с безопасностью

antiphish.ru/products/start

28 сентября 2021 года



START

Security Trainings and Requirements Tool

1. Что может пойти не так?

Как недостатки требований, знаний и навыков продуктовых команд приводят к инцидентам безопасности



Из электронных трудовых некоторых россиян начал пропадать стаж

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



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/>

Пример: «деньги из воздуха»

 Приёмная Кит Великан 3 июн в 21:59

 Слушать

Мошенники пользуются уязвимостью валютных фондов «Тинькофф»

Предисловие. Мошенническая схема, которую я опишу ниже, не является секретной или малоизвестной. В пульсе, соцсети «Тинькофф», по несколько раз в неделю появляются возмущенные посты людей, о том, что у них пропадают деньги.

 125  

22 027 просмотров

В техподдержку также постоянно пишут жалобы, т.е. «Тинькофф» тоже обо всем знает, но не предпринимает никаких действий.

Так что моя совесть чиста, на случай, если после этой публикации начнётся массовый приток новых халявщиков.

<https://vc.ru/claim/254127-moshenniki-polzuyutsya-uyazvimostyu-valyutnyh-fondov-tinkoff>





Стакан TEUR



Bid, €	0,0004 (0,387%)		Ask, €
0,1033	2202700	101094	0,1037
0,1032	88257	164225	0,1038
0,1031	15348	2250530	0,1039
0,1030	67003	105492	0,1040
0,1029	23235	2031	0,1041
0,1028	50740	6210	0,1042
0,1027	55980	6299	0,1043
0,1026	8913	5757	0,1044



Список изменений



Обратная связь



Справка



Чат поддержки



ENG

12:22

21.05.2021



Пример: раскрытие данных клиентов

Приёмная Александр Лопатин 12 июл в 21:09

🔊 Слушать

«СберБанк»: мои персональные данные попали к злоумышленникам — их может предоставлять голосовой робот

<https://vc.ru/claim/269097-sberbank-moi-personalnye-dannye-popali-k-zloumyshlennikam-ih-mozhet-predostavlyat-golosovoy-robot>

Сегодня 12.07.2021 года в 18:14 поступил звонок от мошенников «СберБанк безопасности СберБанка» с номера +74959665374.

🗨 522 📌 📤

Мне периодически поступают подобные звонки от "СберБ. свободное время, и я начал диалог с " младшим специалистом, обычная, попытка перевода на 3000 рублей (остаток по карте 3000 рублей, это я знал точно), злоумышленники уже привязали к моему номеру один номер, который мне не известен, и так далее. Спрашиваю какой номер, который я помню. Говорю что 350 000 там лежит на карте, выходных покупать авто. Через несколько вопросов, говорю попытка перевода на 120 000 рублей, и что дело серьезно

Друзья, мы выяснили как такое возможно. Во время общения с младшим сотрудником, старший звонит на номер 900 подставляя на исходящий мой номер. Там робот предлагает продиктовать мне остаток по картам, просит назвать номер, если назвать номер наугад, то робот дружелюбно сообщает что такой карты нет, и называет номера всех действующих карт (Сбер, это реально круто, спасибо). Далее называешь номер любой из карт, и он сообщает тебе остаток. Это просто офигенно. **Вопрос про слив данных сотрудником снимается, виноват робот.** Новые вопросы к Сберу: почему сотрудники не знают что так можно? Почему вообще так можно? Добавлю в пост.

Безопасность: ожидание

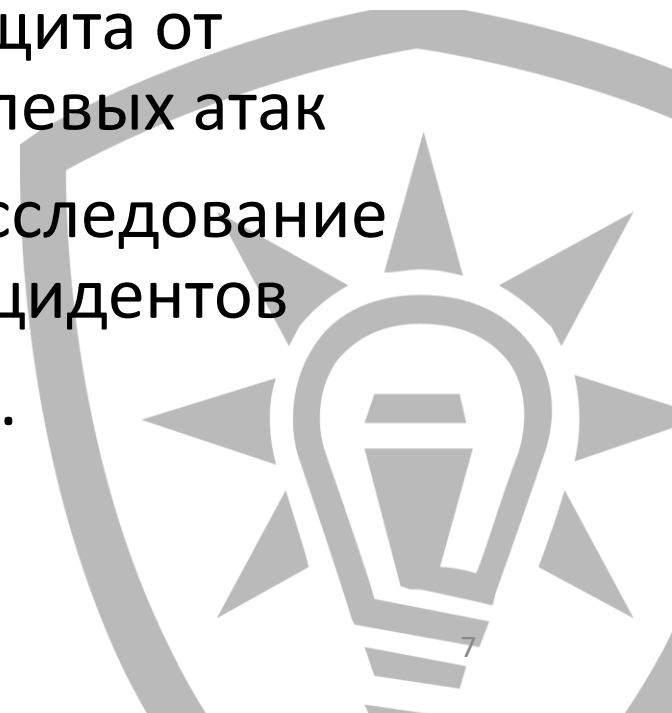


Анализ рисков
Моделирование
угроз

Защита от
целевых атак

Расследование
инцидентов

etc.



Безопасность: реальность

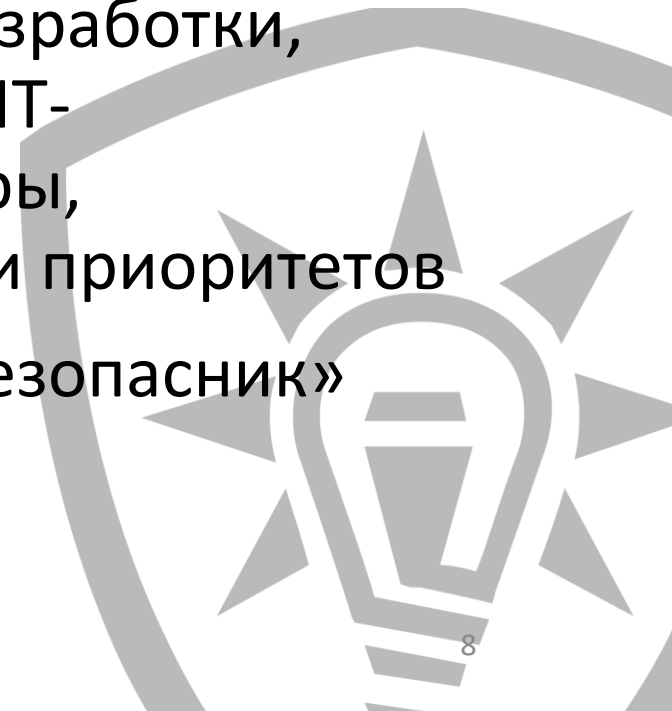


Низкая квалификация

Узкое мышление

Незнание реалий:
технологий разработки,
собственной ИТ-
инфраструктуры,
бизнес-задач и приоритетов

«Бумажный безопасник»



Искусство программирования

ТОМ 1

Основные алгоритмы
Третье издание

ДОНАЛЬД Э. КНУТ

Продуктовые команды: ожидание

Сдаем продукт / проект в срок
и с наилучшим качеством

Все требования выполнены

Agile-команды и непрерывная
доставка ценности

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

Продуктовые команды: реальность

Какие угрозы актуальны?

В чем реальные риски?

Как писать безопасный код?

+ карго-культ

Какие могут быть проблемы
с окружением?



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

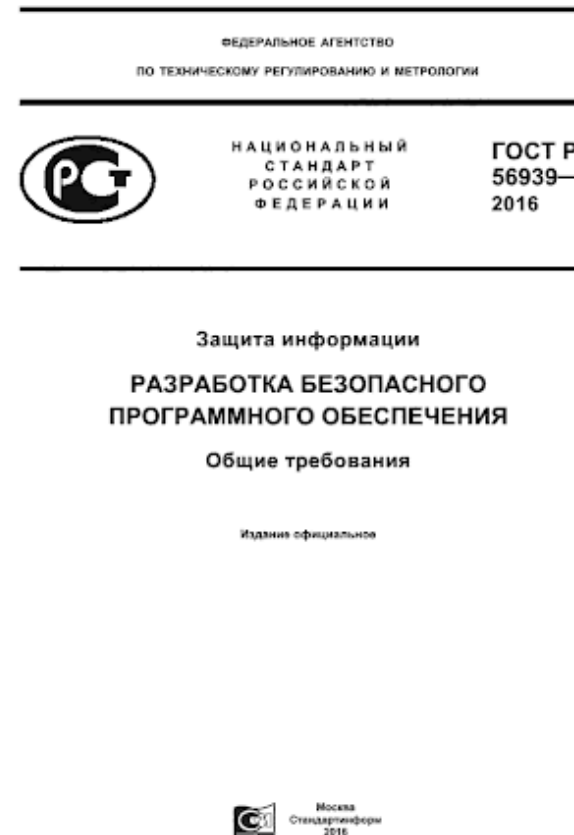
5.1.3.1 Разработчик ПО должен определить требования по безопасности, предъявляемые к разрабатываемому ПО.

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.

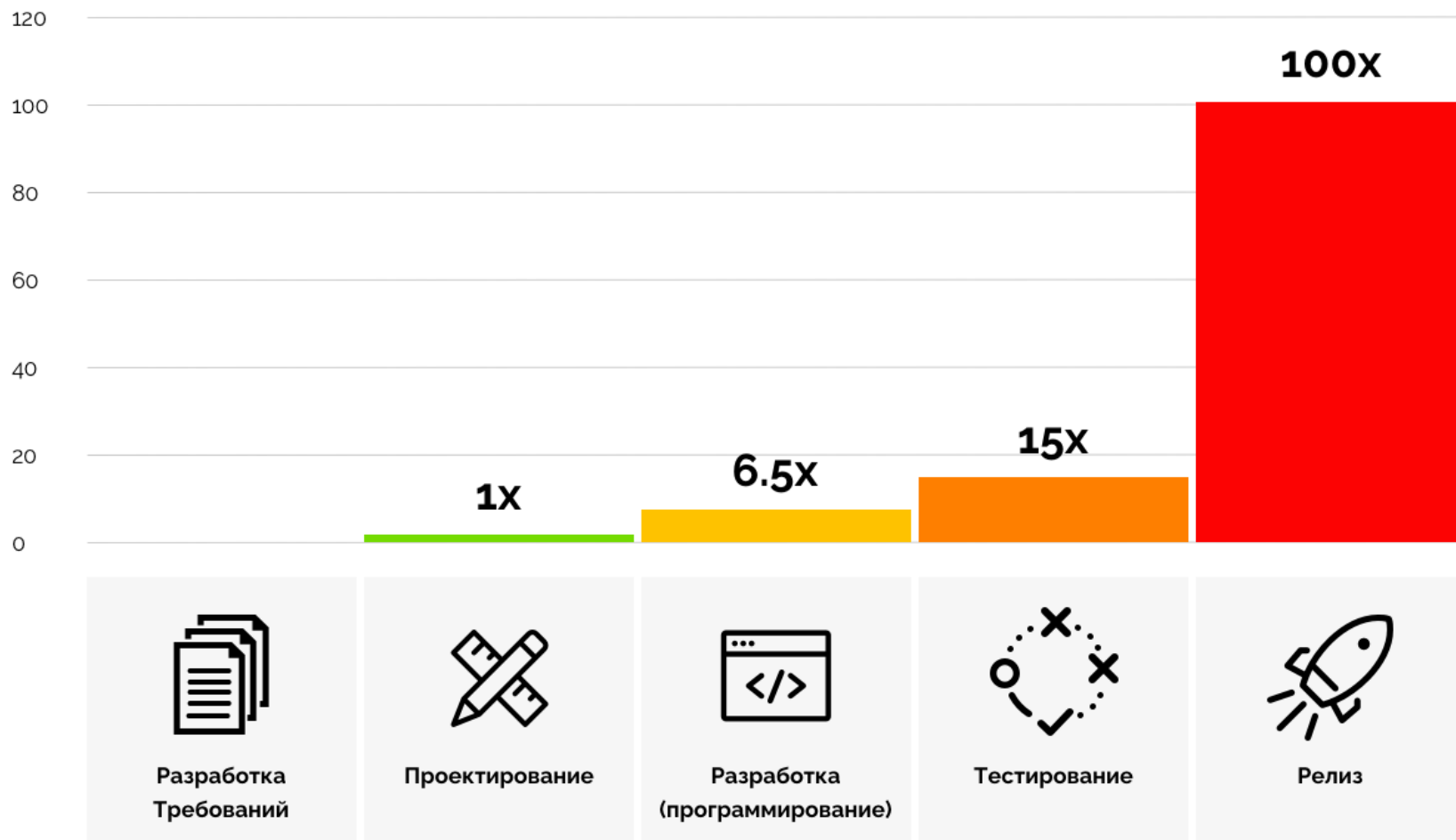
Despite this, the time required to carry out these activities as manual tasks makes them a poor fit for agile and DevOps practices. This, coupled with a general lack of application security skills and expertise, has resulted in few organizations routinely including formal (versus ad hoc) threat modeling 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®



Относительная стоимость устранения дефектов ПО на разных этапах разработки





START

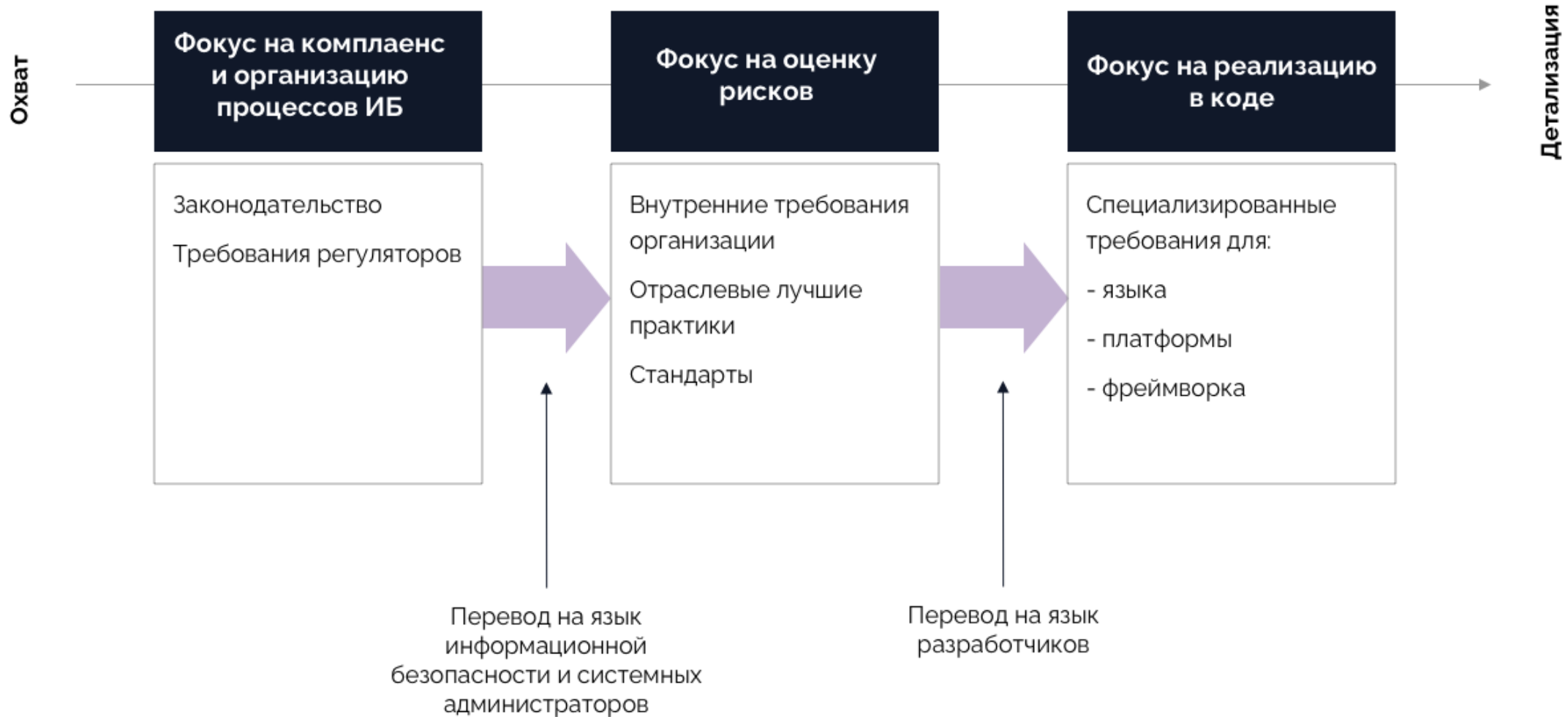
Security Trainings and Requirements Tool

2. Как сформировать требования по ИБ к ПО

и сделать их понятными для команды



Уровни требований по безопасности



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



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



Генрих
Альтшуллер

НАЙТИ ИДЕЮ

Введение
в ТРИЗ —
теорию
решения
изобретательских
задач



Как научить разработчиков писать безопасный код?

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

“ 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



START

Security Trainings and Requirements Tool

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

Продукты Решения Услуги Ресурсы Компания

Международные новости утечек информации, аналитические отчеты и статистика за последние годы.

29 октября 2020

Промышленность, ТЭК и транспортный сектор

Экспертно-аналитический центр группы компаний InfoWatch [далее - ЗАЦ] подготовил исследование

Запросить аналитический отчет

Имя

input#report-download-email-modal form-email.required 422 x 45

Корпоративный email

ЗАПРОСИТЬ

Elements Console Sources Network Performance Memory Application Security Lighthouse AdBlock Plus

```
<input autocomplete="off" data-drupal-selector="report-download-email-modal" type="email" id="report-download-email-modal" name="email" value size="60" maxlength="254" class="form-email required" required="required" aria-required="true" > => id
```

Styles Computed Layers Event List

Filter

element.style {

.form__field_modern input, .form__field_modern label {

width: 100%;

.ui-widget, .ui-widget input {

font-family: "DIN Pro", Arial, Helvetica;

font-size: 1em;

.form__field_modern input, .form__field_modern label {

[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

3. 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

Admin

Проекты

Системы

Настройки

Выйти

Мои проекты

[+ Добавить Проект](#)

Проект	Систем	Требований	Последняя активность	Действия
Модернизация ДБО тестовый проект в компании	2	129	10 дней назад →	
СЗ ПДн 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	Архитектура и Дизайн			
2	AR3	Для взаимодействия с другими приложениями и компонентами должны использоваться учетные записи, обладающие минимально необходимыми полномочиями.	Без замечаний	Средняя	
3	CO	Технические. Общие требования и документирование			
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
Банк №1 Новый проект над которым мы работаем	7	607	Сейчас	
Магазин	1	120	44 дня назад	



Коллекции требований



Банк России



ФИНТЕХ
АССОЦИАЦИЯ



OWASP



Security
Standards Council



START

Security Trainings and Requirements Tool

Бесплатные материалы

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

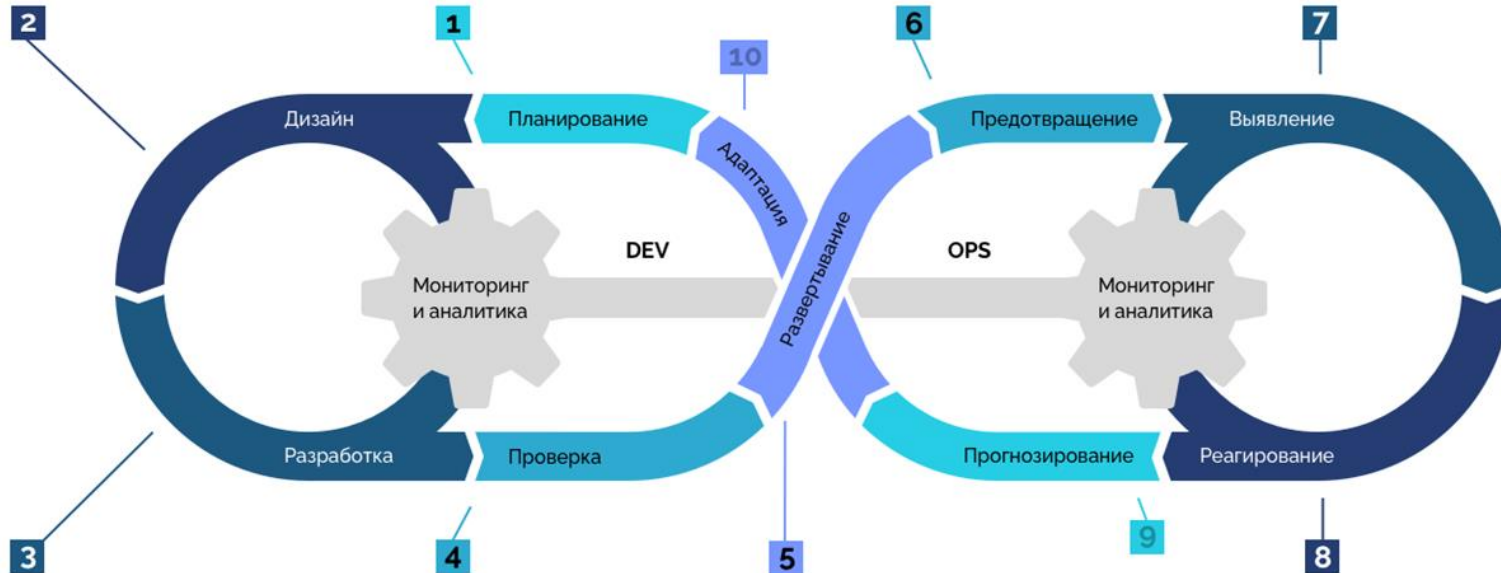
Выполненные на этапах производства ПО требования позволяют в полной мере применять механизмы безопасности на этапах его эксплуатации.

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

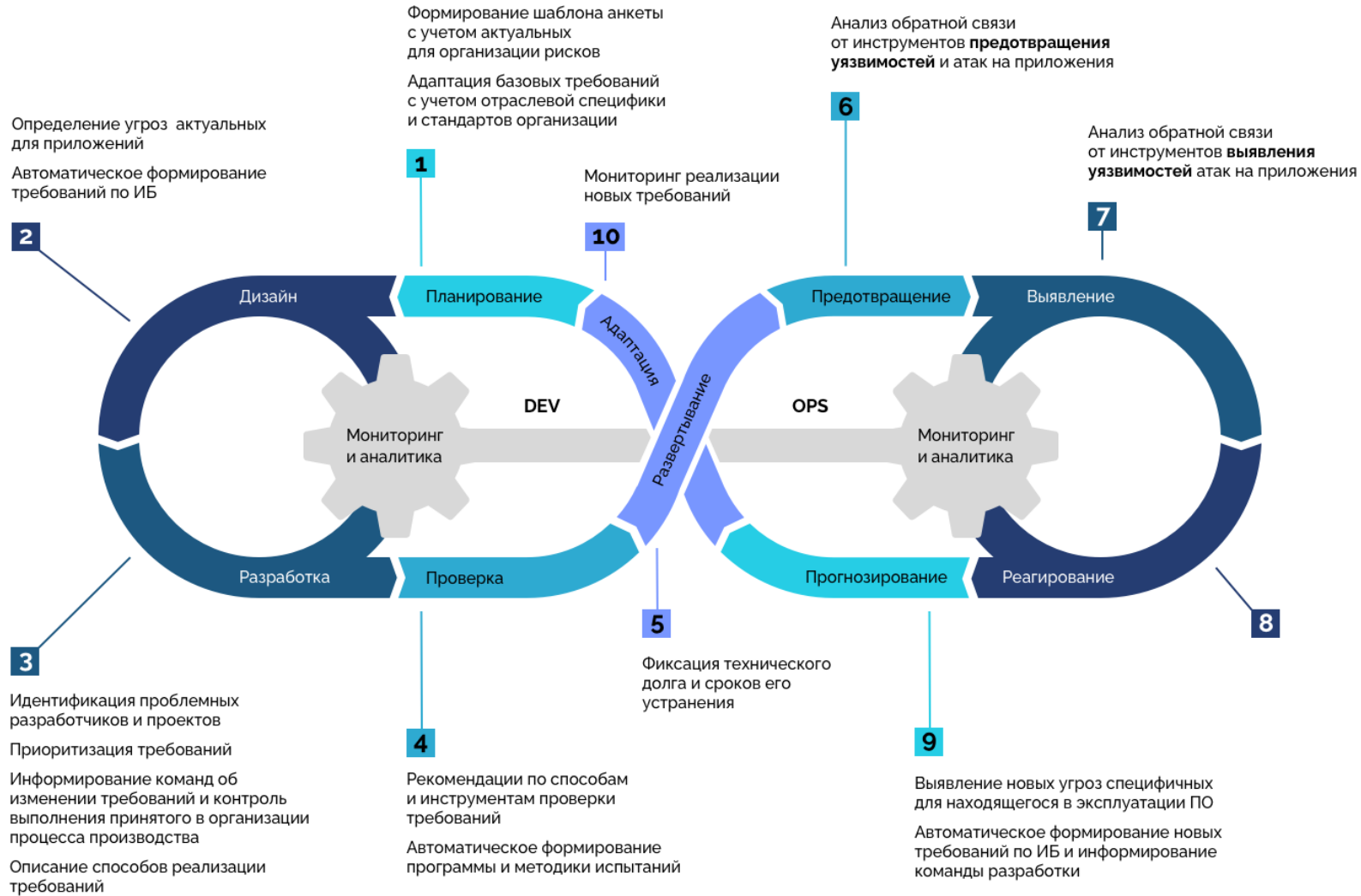
- T** Техническое
- K** Средняя

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



Хакми Банк

Крутым ребятам
крутой процент!



START

Security Trainings and Requirements Tool


практический CTF-тренажер
в рамках Антифишинг. START


Balance:


- 0 RUB
- 0 USD
- 0 EUR


Exchange rates:


Currency	Buy	Sell
USD	72.72	72.52
EUR	86.26	86.06


 90107430600220100571
0 RUB


 Deposit


 Transfer


 History


 90107430600220200572
0 USD


 Deposit

 Transfer



 90107430600220300573
0 EUR

 Deposit

 Transfer



START

Security Trainings and Requirements Tool

практический CTF-тренажер
в рамках Антифишинг. START

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

Обучайте и тренируйте своих людей.

START

Security Trainings and Requirements Tool

ask@antiphish.ru

antiphish.ru/products/start

