Как статический анализ дополняет TDD

Андрей Карпов

PVS-Studio, DevRel

Байки для разминки

- Полёты за багом
- DllMain

Андрей Карпов

DevRel. Один из основателей проекта PVS-Studio.

TDD

TDD

- Test-driven development
- Разработка через тестирование

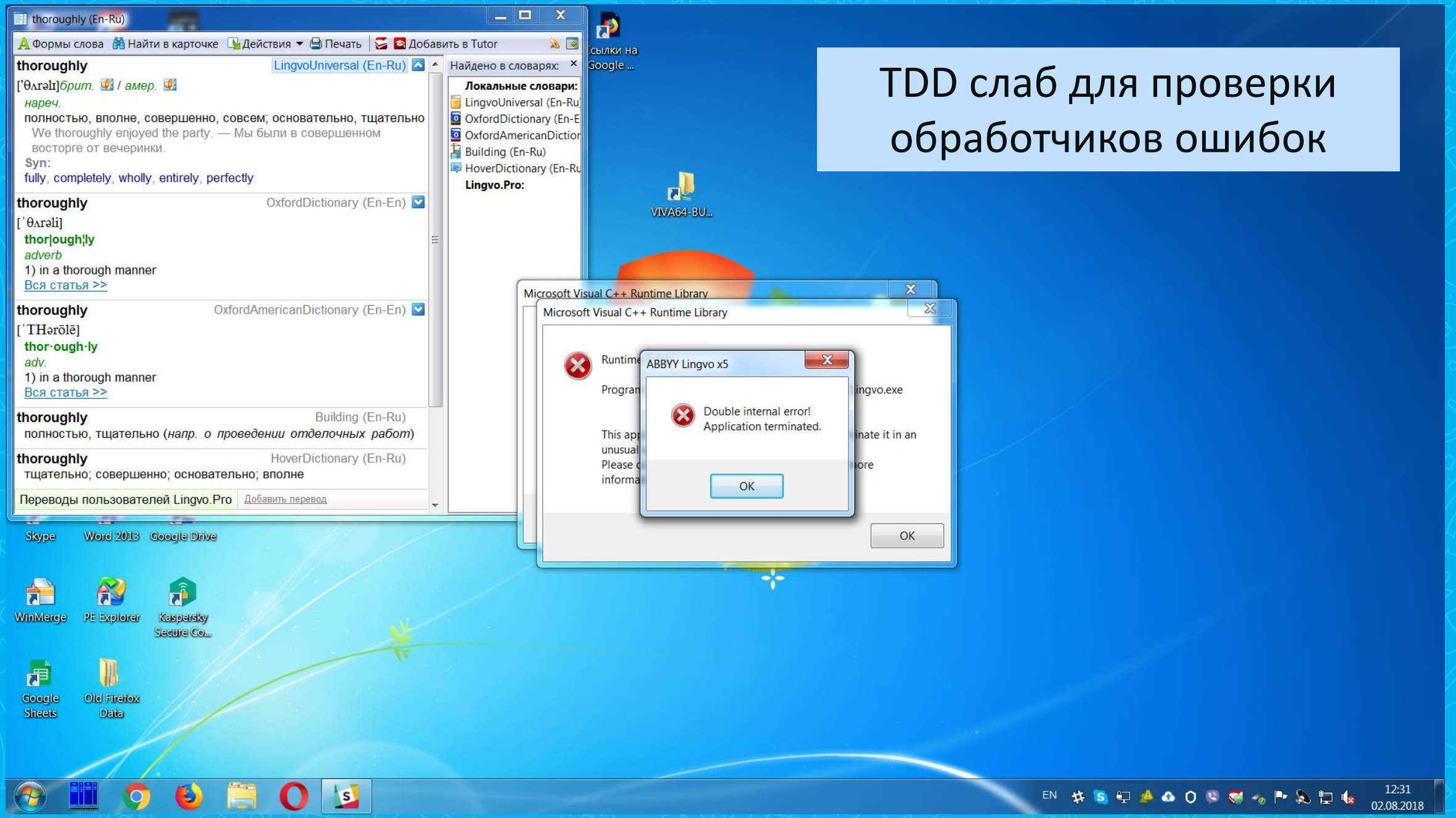
- Это Unit-тестирование
- Только тесты пишутся до кода

TDD это хорошо, но

- Некоторые ошибки невозможно выявить с помощью тестов
- Или это крайне сложно и нерационально по трудозатратам
- Чуть позже будут PROOF-ы

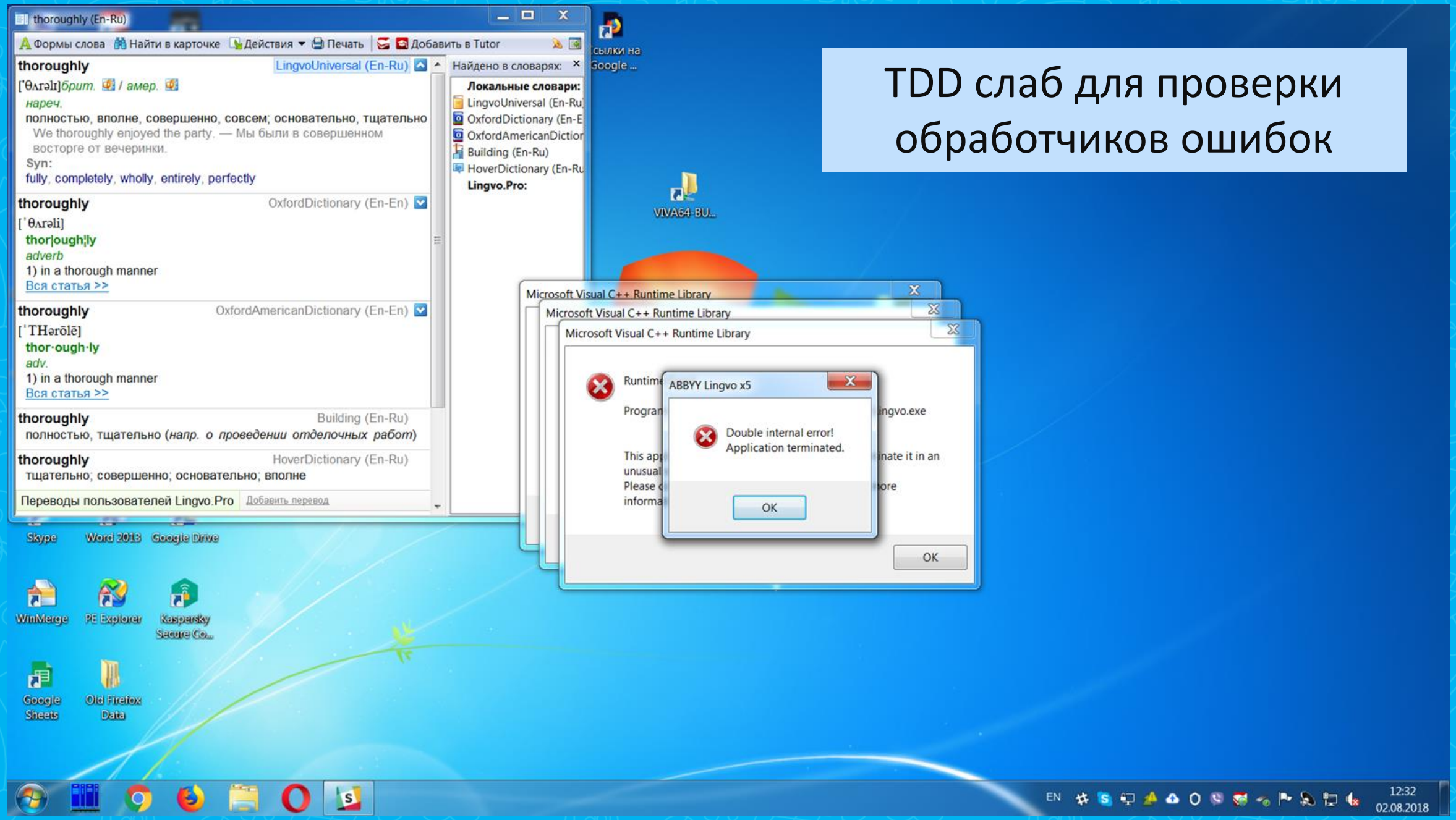
TDD слаб

- Когда ошибка не ломает поведение, а замедляет код
- Ошибки могут содержать сами тесты
  - Никто не пишет тесты на тесты
- Ошибка проявляет себя только на больших объёмах данных
- Скучно/нерационально/сложно тестировать некоторые участки кода

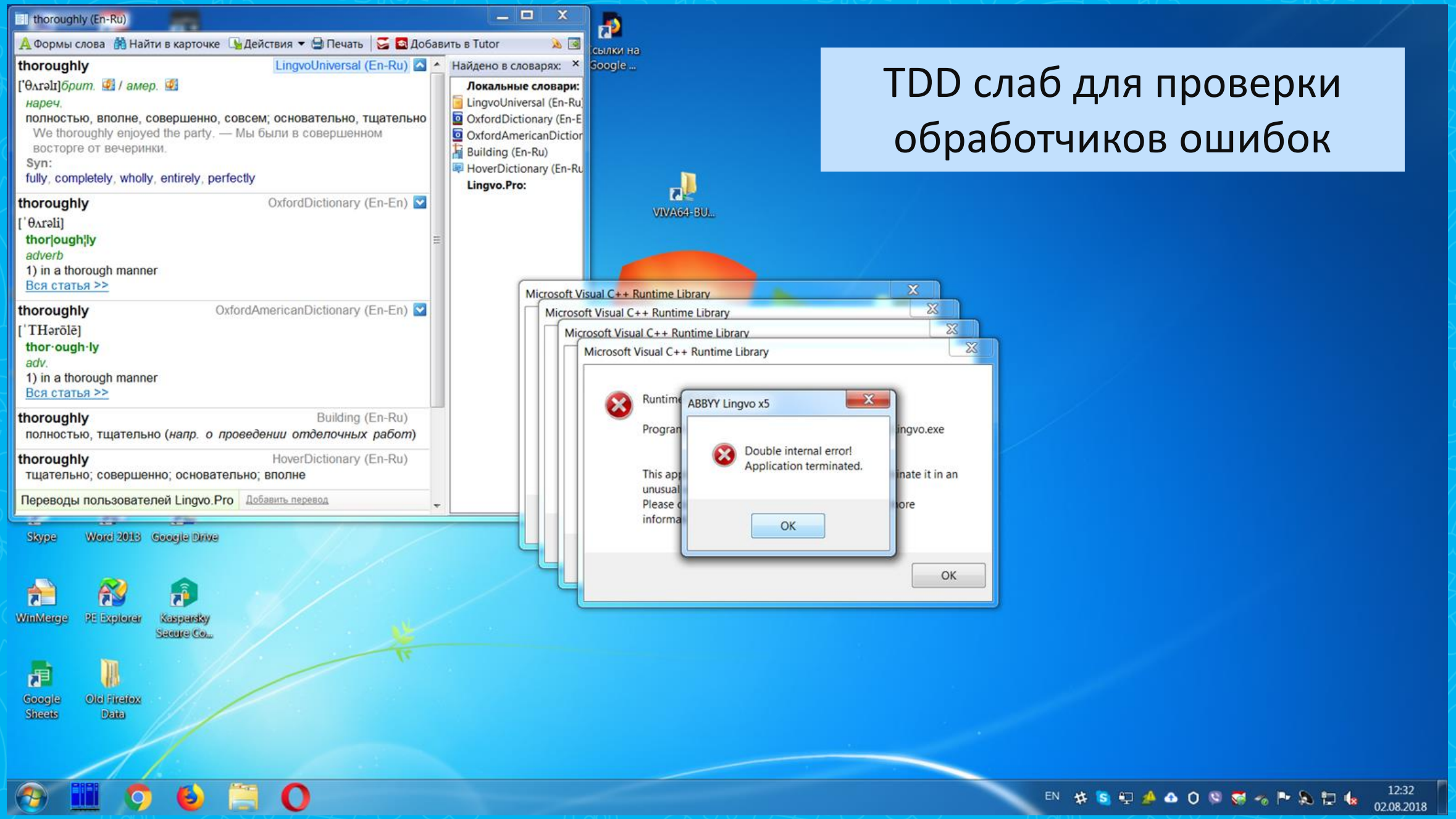


TDD слаб для проверки обработчиков ошибок

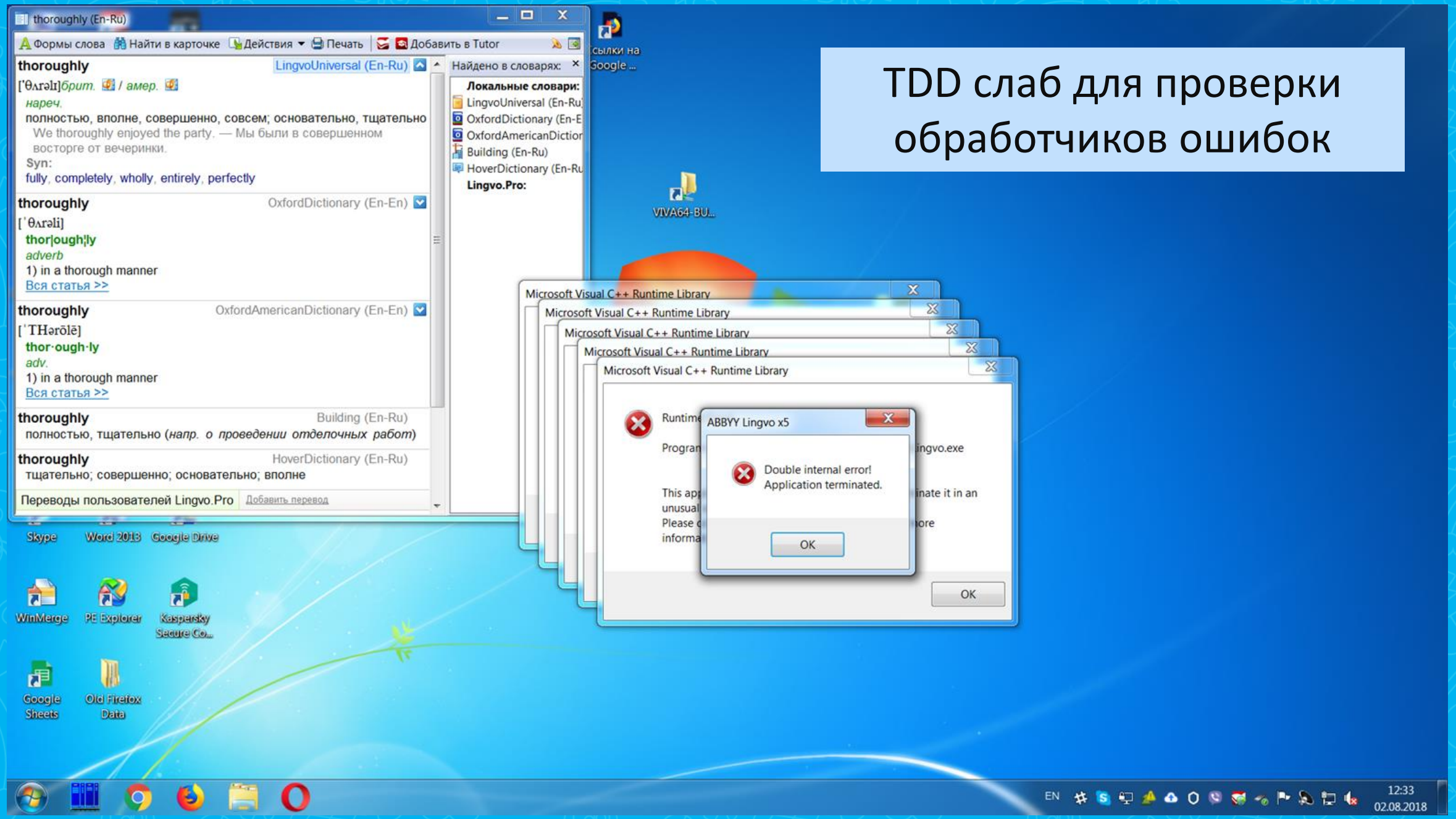
TDD слаб для проверки обработчиков ошибок

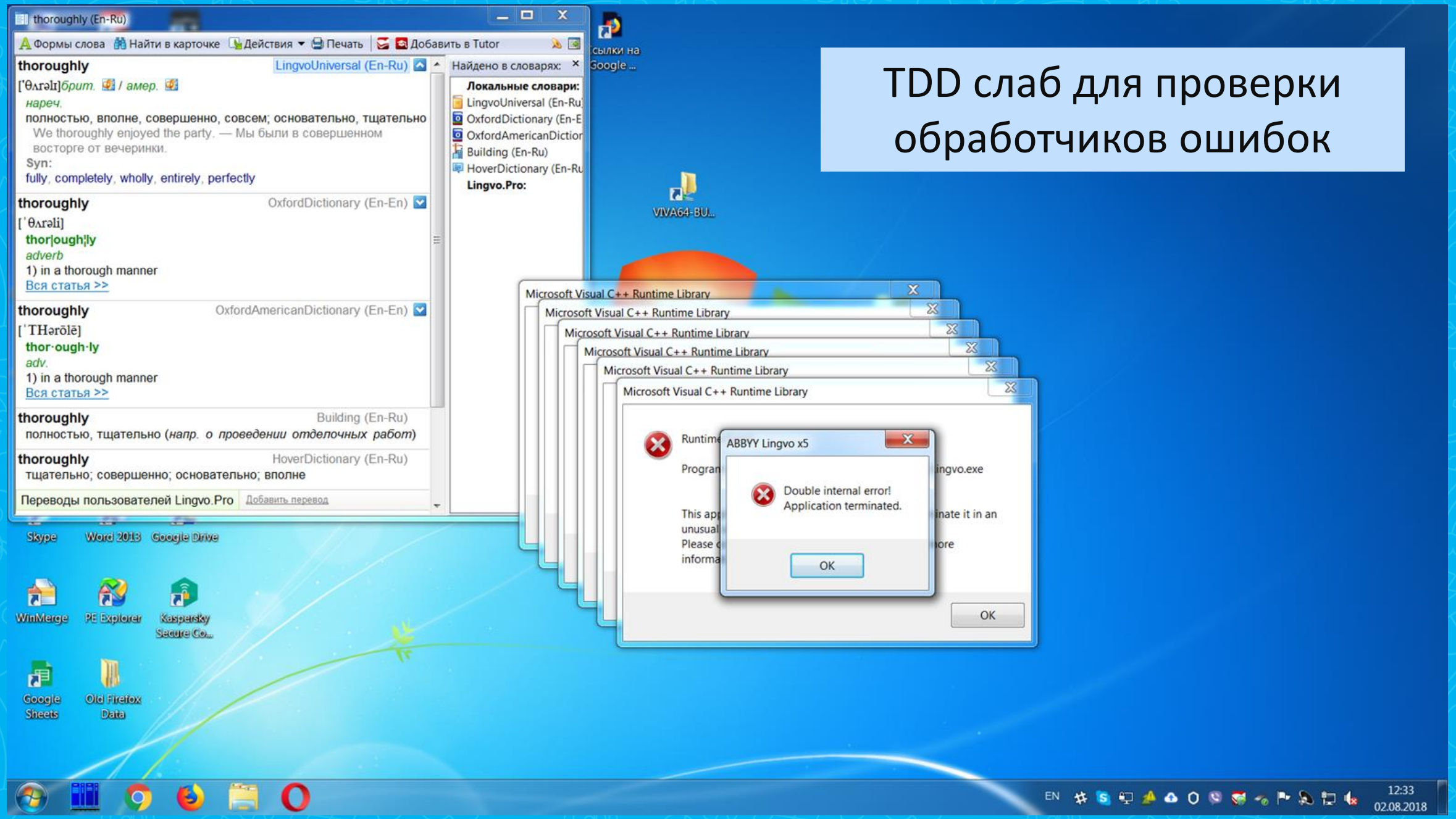


TDD слаб для проверки обработчиков ошибок

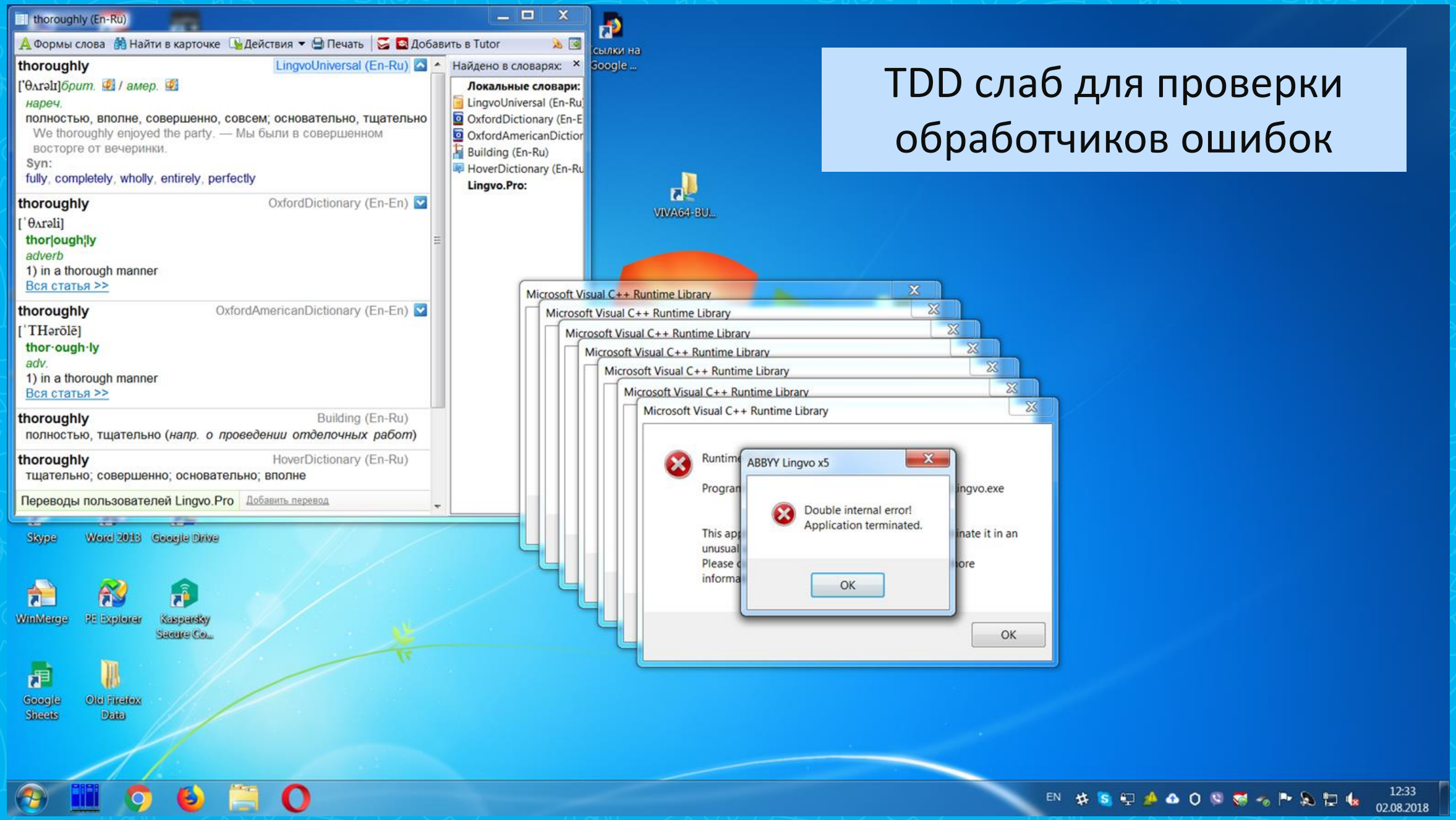


TDD слаб для проверки обработчиков ошибок




TDD слаб для проверки обработчиков ошибок
thoroughly (En-Ru)
Формы слова
Найти в карточке
Действия
Печать
Добавить в Tutor
thoroughly
LingvoUniversal (En-Ru)
['θʌrəlɪ]брит. / амер.
нареч.
полностью, вполне, совершенно, совсем; основательно, тщательно
We thoroughly enjoyed the party. — Мы были в совершенном восторге от вечеринки.
Syn:
fully, completely, wholly, entirely, perfectly
thoroughly
OxfordDictionary (En-En)
['θʌrəli]
thor|ough¦ly
adverb
1) in a thorough manner
Вся статья >>
thoroughly
OxfordAmericanDictionary (En-En)
['THərōlē]
thor·ough·ly
adv.
1) in a thorough manner
Вся статья >>
thoroughly
Building (En-Ru)
полностью, тщательно (напр. о проведении отделочных работ)
thoroughly
HoverDictionary (En-Ru)
тщательно; совершенно; основательно; вполне
Переводы пользователей Lingvo.Pro
Добавить перевод
Найдено в словарях:
Локальные словари:
LingvoUniversal (En-Ru)
OxfordDictionary (En-E
OxfordAmericanDictior
Building (En-Ru)
HoverDictionary (En-Ru
Lingvo.Pro:
Ссылки на Google ...
VIVA64-BU...
Microsoft Visual C++ Runtime Library
ABBYY Lingvo x5
Double internal error!
Application terminated.
OK
Skype
Word 2013
Google Drive
WinMerge
PE Explorer
Kaspersky Secure Co...
Google Sheets
Old Firefox Data
EN
12:33
02.08.2018

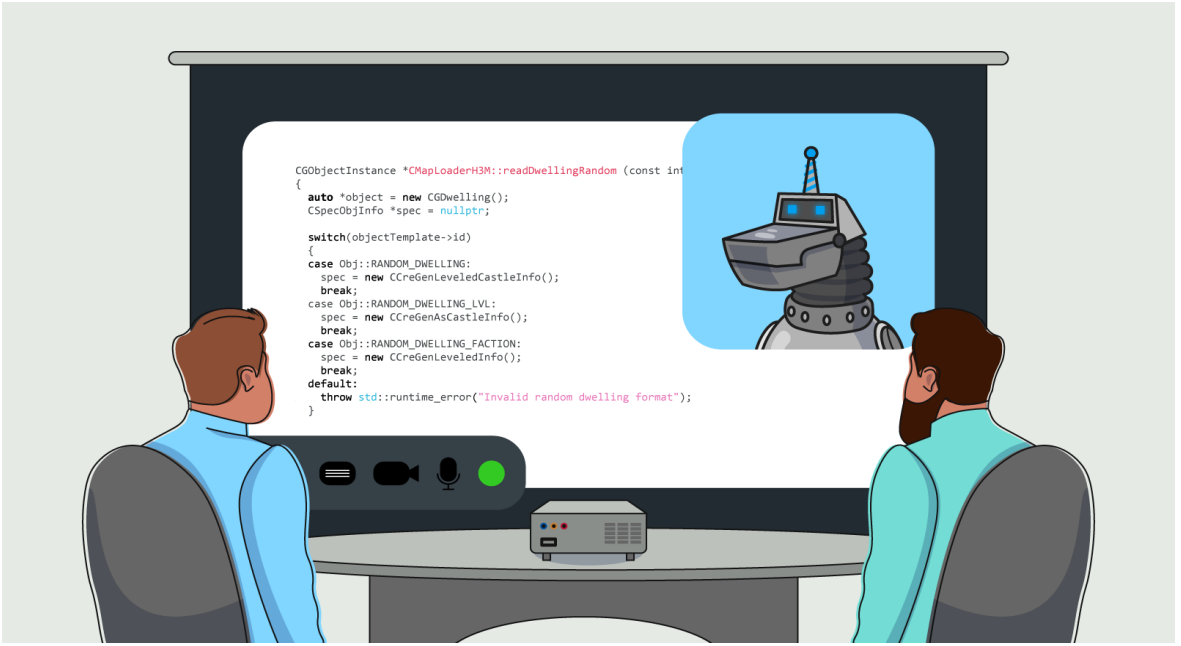
TDD слаб для проверки обработчиков ошибок



Статический анализ спешит на помощь

Статический анализ кода

- Автоматизированный обзор кода
- Нет никаких ***VS***
- Хорошо дополняет другие методологии выявления ошибок



Сильные стороны

- Проверка тестов
- Полное покрытие кода
  - Ну почти. Есть тонкие нюансы
- Улучшение качества кодовой базы в целом
- Выявление «невидимых ошибок» с точки зрения unit-тестов или динамического анализа
  - Не зависит от входных данных
  - «Предсказание багов» на пока работающем коде (например, 64-битные ошибки)

Примеры дополнения TDD

- Продемонстрирую на примерах ошибок, которые находил PVS-Studio в открытых проектах
- PVS-Studio – статический анализатор C, C++, C#, Java кода
- PVS-Studio: SAST, SCA, OWASP, SEI CERT, CWE, MISRA, AUTOSAR, Visual Studio, IntelliJ IDEA, Rider, CLion, Visual Studio Code, Qt Creator, DefectDojo, MSBuild, Ninja, Gradle, Keil µVision, DS-MDK, IAR Embedded Workbench, Docker, Jenkins, TeamCity, CircleCI, Travis CI, GitLab, GitHub Actions **и много других умных слов!**

PROOF-ы

Разминка:
ошибки в обработчиках ошибок

OpenJDK, C

```
ClassInstancesData  *data;
data = (ClassInstancesData*)user_data;

if (data == NULL) {
  data->error = AGENT_ERROR_ILLEGAL_ARGUMENT;
  return JVMTI_VISIT_ABORT;
}
```

PVS-Studio: V522 Dereferencing of the null pointer 'data' might take place. util.c 2424

Spoon, Java

```
try {
  return Class.forName("spoon.reflect.code." + name);
} catch (ClassNotFoundException ex) {
  throw new CtPathException(
    String.format(
      "Unable to locate element with name $s in Spoon model",
      name));
}
```

%1$s

PVS-Studio: V6046 Incorrect format. A different number of format items is expected. Arguments not used: 1. CtPathStringBuilder.java 54

Rosegarden, C++

```
bool FileSource::createCacheFile()
{
  ....
  } catch (DirectoryCreationFailed f) {
    return "";
  }
  ....
}
```

PVS-Studio: V601 The string literal is implicitly cast to the bool type. FileSource.cpp 902

Невидимое для unit-тестов

Android, C

```
static void FwdLockGlue_InitializeRoundKeys() {
  unsigned char keyEncryptionKey[KEY_SIZE];
  ....
  memset(keyEncryptionKey, 0, KEY_SIZE); // Zero out key data.
}
```

PVS-Studio: V597 CWE-14 The compiler could delete the 'memset' function call, which is used to flush 'keyEncryptionKey' buffer. The memset_s() function should be used to erase the private data. FwdLockGlue.c 102

Подробнее: https://cwe.mitre.org/data/definitions/14.html

Пока работающий код

```
typedef char my_bool;


my_bool
check_scramble(const char *scramble_arg, const char *message,
               const uint8 *hash_stage2) {
  ....
  return
    memcmp(hash_stage2, hash_stage2_reassured, SHA1_HASH_SIZE);
}
```

CVE-2012-2122 (**Не мы нашли, но могли бы**)

PVS-Studio: V642 Saving the 'memcmp' function result inside the 'char' type variable is inappropriate. The significant bits could be lost breaking the program's logic. password.c

```
filter->data_count++;
array = realloc(filter->data,
  sizeof(Edje_Part_Description_Spec_Filter_Data) *
  filter->data_count);
array[filter->data_count - 1].name = name;
array[filter->data_count - 1].value = value;
filter->data = array;
```

PVS-Studio: V522 There might be dereferencing of a potential null pointer 'array'. edje_cc_handlers.c 14249

Четыре причины проверять, что вернула функция malloc:
https://pvs-studio.ru/ru/blog/posts/cpp/0938/

Сложное/скучное для выявления unit-тестами

Hibernate, Java

```
annotationToXml.put( NamedNativeQuery.class, "named-native-query" );
annotationToXml.put( NamedNativeQueries.class, "named-native-query" );
annotationToXml.put( NamedStoredProcedureQuery.class, "named-stored-procedure-query" );
annotationToXml.put( NamedStoredProcedureQueries.class, "named-stored-procedure-query" );
annotationToXml.put( SqlResultSetMapping.class, "sql-result-set-mapping" );
annotationToXml.put( SqlResultSetMappings.class, "sql-result-set-mapping" );
annotationToXml.put( ExcludeDefaultListeners.class, "exclude-default-listeners" );
annotationToXml.put( ExcludeSuperclassListeners.class, "exclude-superclass-listeners" );
annotationToXml.put( AccessType.class, "access" );
annotationToXml.put( AttributeOverride.class, "attribute-override" );
annotationToXml.put( AttributeOverrides.class, "attribute-override" );
annotationToXml.put( AttributeOverride.class, "association-override" );
annotationToXml.put( AttributeOverrides.class, "association-override" );
annotationToXml.put( AttributeOverride.class, "map-key-attribute-override" );
annotationToXml.put( AttributeOverrides.class, "map-key-attribute-override" );
annotationToXml.put( Id.class, "id" );
annotationToXml.put( EmbeddedId.class, "embedded-id" );
annotationToXml.put( GeneratedValue.class, "generated-value" );
annotationToXml.put( Column.class, "column" );
annotationToXml.put( Columns.class, "column" );
annotationToXml.put( Temporal.class, "temporal" );
annotationToXml.put( Lob.class, "lob" );
annotationToXml.put( Enumerated.class, "enumerated" );
annotationToXml.put( Version.class, "version" );
annotationToXml.put( Transient.class, "transient" );
annotationToXml.put( Basic.class, "basic" );
annotationToXml.put( Embedded.class, "embedded" );
```

Тесты на заполнение контейнера константами? Такое себе занятие…

Hibernate, Java

```
private static final Map<Class, String> annotationToXml;
....
annotationToXml.put(AttributeOverride.class, "attribute-override");
....
annotationToXml.put(AttributeOverride.class, "association-override");
....
annotationToXml.put(AttributeOverride.class, "map-key-attribute-override");
```

- PVS-Studio: An item with the same key 'javax.persistence.AttributeOverride.class' has already been added. Check lines: 188, 186. JPAOverriddenAnnotationReader.java 188
- PVS-Studio: V6033 An item with the same key 'javax.persistence.AttributeOverride.class' has already been added. Check lines: 190, 186. JPAOverriddenAnnotationReader.java 190

```
public final R getSomeBuildWithWorkspace() {
  int cnt=0;
  for (R b = getLastBuild(); cnt<5 && b!=null;
       b=b.getPreviousBuild())
  {
    FilePath ws = b.getWorkspace();
    if (ws!=null)   return b;
  }
  return null;
}
```

PVS-Studio: V6007 Expression 'cnt < 5' is always true. AbstractProject.java 557

Отдельно среди сложно-скучного,
можно выделить функции сравнения

Зло живёт в функциях сравнения

Unreal Engine 4, C++

```
bool Compare(const FPooledRenderTargetDesc& rhs, bool bExact) const
{
  ....
  return Extent == rhs.Extent
    && Depth == rhs.Depth
    && bIsArray == rhs.bIsArray
    && ArraySize == rhs.ArraySize
    && NumMips == rhs.NumMips
    && NumSamples == rhs.NumSamples
    && Format == rhs.Format
    && LhsFlags == RhsFlags
    && TargetableFlags == rhs.TargetableFlags
    && bForceSeparateTargetAndShaderResource ==
         rhs.bForceSeparateTargetAndShaderResource
    && ClearValue == rhs.ClearValue
    && AutoWritable == AutoWritable;
}
```

PVS-Studio: V501 There are identical sub-expressions to the left and to the right of the '==' operator: AutoWritable == AutoWritable rendererinterface.h 180

А помимо статического анализа?

- Никто не тестирует функции сравнения…
- Оформление кода
- Генераторы тестов
  - Андрей Сатарин – EqualsVerifier, ErrorProne и все-все-все
  - https://youtu.be/jeCpYOEuL64

```
bool Compare(const FPooledRenderTargetDesc& rhs, bool bExact) const
{
  ....
  return    Extent           == rhs.Extent
         && Depth            == rhs.Depth
         && bIsArray         == rhs.bIsArray
         && ArraySize        == rhs.ArraySize
         && NumMips          == rhs.NumMips
         && NumSamples       == rhs.NumSamples
         && Format           == rhs.Format
         && LhsFlags         == RhsFlags
         && TargetableFlags  == rhs.TargetableFlags
         && bForceSeparateTargetAndShaderResource ==
              rhs.bForceSeparateTargetAndShaderResource
         && ClearValue       == rhs.ClearValue
         && AutoWritable     == AutoWritable;
}
```

"Табличное форматирование"
Стало лучше, но не идеально.
Стоит использовать, но это не отменяет необходимость статического анализа кода.

Сладкое: ошибки в тестах

```
Context.cs = 0x8c8d;
Context.fs = 0x8e8f;
Context.gs = 0x9091;
Context.ss = 0x9293;
Context.ds = 0x9495;
Context.ss = 0x9697;  .es
ArrayRef<uint8_t> ContextRef(
  reinterpret_cast<uint8_t *>(&Context), sizeof(Context));
```

PVS-Studio: V519 [CWE-563, CERT-MSC13-C] The 'Context.ss' variable is assigned values twice successively. Perhaps this is a mistake. Check lines: 110, 112. RegisterContextMinidumpTest.cpp 112

Data Distribution Service, C++

```
TEST_ASSERT(dsqp.service_cleanup_delay.sec = 4);
TEST_ASSERT(dsqp.service_cleanup_delay.nanosec = 2000);
TEST_ASSERT(dsqp.history_kind == KEEP_LAST_HISTORY_QOS);
TEST_ASSERT(dsqp.history_depth == 172);
TEST_ASSERT(dsqp.max_samples == 389);
TEST_ASSERT(dsqp.max_instances == 102);
TEST_ASSERT(dsqp.max_samples_per_instance == 20);
```

- V559 Suspicious assignment inside the condition expression of 'if' operator: dsqp.service_cleanup_delay.sec = 4. ut_parameterlistconverter.cpp 1295
- V559 Suspicious assignment inside the condition expression of 'if' operator. ut_parameterlistconverter.cpp 1296

```
for (int i = 0; i < 20; i++)
{
  ....
  if (i % 2 == 0)
  {
    thread1.Start();
    thread2.Start();
  }
  else
  {
    thread1.Start();
    thread2.Start();
  }
  ....
```

.NET Compiler Platform ("Roslyn"), C#

PVS-Studio: V3004 The 'then' statement is equivalent to the 'else' statement. GetSemanticInfoTests.cs 2269

Entity Framework, C#

```
for (var i = 0; i < result.Count; i++)
{
  ....
  for (var j = 0; j < expectedInnerNames.Count; j++)
  {
    Assert.True(
      result[i]
      .OneToMany_Optional.Select(e => e.Name)
      .Contains(expectedInnerNames[i])
    );
  }
}
```

PVS-Studio: V3081 The 'j' counter is not used inside a nested loop. Consider inspecting usage of 'i' counter. EFCore.Specification.Tests ComplexNavigationsQueryTestBase.cs 2393

Apache Hadoop, Java

```
currentSecretA = secretProviderA.getCurrentSecret();
allSecretsA = secretProviderA.getAllSecrets();
Assert.assertArrayEquals(secretA2, currentSecretA);
Assert.assertEquals(2, allSecretsA.length);
Assert.assertArrayEquals(secretA2, allSecretsA[0]);
Assert.assertArrayEquals(secretA1, allSecretsA[1]);

currentSecretB = secretProviderB.getCurrentSecret();
allSecretsB = secretProviderB.getAllSecrets();
Assert.assertArrayEquals(secretA2, currentSecretB);
Assert.assertEquals(2, allSecretsA.length);
Assert.assertArrayEquals(secretA2, allSecretsB[0]);
Assert.assertArrayEquals(secretA1, allSecretsB[1]);
```

PVS-Studio: V6072 Two similar code fragments were found. Perhaps, this is a typo and 'allSecretsB' variable should be used instead of 'allSecretsA'. TestZKSignerSecretProvider.java(316), TestZKSignerSecretProvider.java(309), TestZKSignerSecretProvider.java(306), TestZKSignerSecretProvider.java(313)

eLynx Image Processing SDK and Lab, C++

```
void checkFormatConversion::Test(....)
{
  static struct { bool _b1, _b2; } ms_2boolean[] = {
    { false, false },
    { false, true  },
    { true,  false },
    { true,  true  }
  };
  const int b2size = sizeof(ms_2boolean) / sizeof(ms_2boolean);
```

PVS-Studio: V501 There are identical sub-expressions 'sizeof (ms_2boolean)' to the left and to the right of the '/' operator. ImageVariant checkformatconversion.cpp 72

```
TEST(SharedMemoryTest, MultipleThreads) {
  ....
  int threadcounts[] = { 1, kNumThreads };
  for (size_t i = 0;
       i < sizeof(threadcounts) / sizeof(threadcounts); i++) {
  ....
```

PVS-Studio: V501 There are identical sub-expressions 'sizeof (threadcounts)' to the left and to the right of the '/' operator. base_unittests shared_memory_unittest.cc 231

Chromium, C++

```
std::string TestAudioConfig::TestValidConfigs() {
  ....
  static const uint32_t kRequestFrameCounts[] = {
    PP_AUDIOMINSAMPLEFRAMECOUNT,
    PP_AUDIOMAXSAMPLEFRAMECOUNT,
    1024, 2048, 4096
  };
  ....
  for (size_t j = 0;
    j < sizeof(kRequestFrameCounts)/sizeof(kRequestFrameCounts);
    j++) {
  ....
}
```

PVS-Studio: V501 There are identical sub-expressions 'sizeof (kRequestFrameCounts)' to the left and to the right of the '/' operator. test_audio_config.cc 56

Итоги

TDD это хорошо, но недостаточно

- Используйте статический анализ
- Используйте динамический анализ
- Изучите пользу внедрения автогенерируемых тестов
- Красивый код == меньше ошибок
  - Оформление
  - «Табличное» форматирование
  - Стандарты кодирования

Q&A

Андрей Карпов

PVS-Studio, DevRel