КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

Угрозы визуальной схожести в доменной и почтовой адресации

Вадим Михайлов
Консультант по инфраструктуре
Вебинар
09 июля 2024

cctld.ru | кц.рф

.RU .РФ

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Определения

RFC 6365: Terminology Used in Internationalization in the IETF

Язык

Способ коммуникации людей

Скрипт

Набор графических символов, используемых для написания одного или более языков

Письменность

Набор правил использования одного или более скриптов, чтобы писать на отдельно взятом языке

Символ

Минимальная единица письменности

Глиф

Графическое изображение символа

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Омоглифы

Омоглиф – от древнегреческого ὁμός – «одинаковый», и γλυφή – «знак»

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Омоглифы

Омоглиф – от древнегреческого ὁμός – «одинаковый», и γλυφή – «знак»

– латинская «o» (U+006F), кириллическая «о» (U+043E) и греческая «ο» (U+03BF)

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Омоглифы

Омоглиф – от древнегреческого ὁμός – «одинаковый», и γλυφή – «знак»

– латинская «o» (U+006F), кириллическая «о» (U+043E) и греческая «ο» (U+03BF)

– расширенная латиница a (U+0061) – ä (U+00E4)

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Омоглифы

Омоглиф – от древнегреческого ὁμός – «одинаковый», и γλυφή – «знак»

– латинская «o» (U+006F), кириллическая «о» (U+043E) и греческая «ο» (U+03BF)

– расширенная латиница a (U+0061) – ä (U+00E4)

– цифра «0» (U+0030) и заглавная буква «O» (U+004F)

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Омоглифы

Омоглиф – от древнегреческого ὁμός – «одинаковый», и γλυφή – «знак»

– латинская «o» (U+006F), кириллическая «о» (U+043E) и греческая «ο» (U+03BF)

– расширенная латиница a (U+0061) – ä (U+00E4)

– цифра «0» (U+0030) и заглавная буква «O» (U+004F)

– строчная m (U+006D) и рядом rn (U+0072 и U+006E)

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Лигатура

Лигатура – от латинского *ligature* – «связка»

– латинская «æ» (U+00E6) сочетает буквы «a» (U+0061) и «e» (U+0065)

– латинская «ffl» (U+FB04) является соединением букв «f» (U+0066), «f» (U+0066) и «l» (U+006C)

– кириллическая «љ» (U+0459) представляет собой соединение букв «л» (U+043B) и «ь» (U+044C)

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Омографы

Омограф – от древнегреческого ὁμός – «одинаковый», и γράφω – «писать»

– на латинице «*mama*» (U+006D U+0061 U+006D U+0061) и на кириллице «*mama*» (U+0442 U+0430 U+0442 U+0430)

– на латинице «*pay*» (U+0070 U+0061 U+0079) и на кириллице «*pay*» (U+0440 U+0430 U+0443)

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Паронимы

Паро́нимы – от древнегреческого παρα — «около; рядом», и ὄνυμα — «имя»)

– адресат и адресант

– экскаватор и эскалатор

– live и leave

– Кастанаевская и Кустанайская

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Фишинг

Создание вредоносных ресурсов и привязка к ним доменных имен максимально похожих на легитимные

<u>При помощи омоглифов:</u>

– gosuslugi.ru и gosus**l**ugi.ru

– paypal.com и paypa**l**.com

– bank.com и b**ä**nk.com/ba**ń**k.com/ba**ñ**k.com

– госуслуги.рф и госуслу**т**и.рф

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Фишинг

Создание вредоносных ресурсов и привязка к ним доменных имен максимально похожих на легитимные

<u>При помощи омографов:</u>

– pay.com (Latin) и pay.com (Кириллица)

– cop.online (Latin) и cop.online (Кириллица)

– *mama.shop* (Latin) и *mama.shop* (Кириллица)

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Фишинг

Создание вредоносных ресурсов и привязка к ним доменных имен максимально похожих на легитимные

<u>При помощи лигатур:</u>

– crownbank.org и crovvnbank.org

– raiffeisen.com и raiffeisen.com

– стальпром.ею и сталъпром.ею

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Фишинг

Создание вредоносных ресурсов и привязка к ним доменных имен максимально похожих на легитимные

Typosquatting:

– bank.ru и bark.ru

Combosquatting:

– авито.рф и авито-услуги.рф

TLDsquatting:

– bank.com и bank.co

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

Business Email Compromise – многоступенчатые атаки связанные с компрометацией корпоративной переписки

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

Business Email Compromise – многоступенчатые атаки связанные с компрометацией корпоративной переписки

Сценарии

– Взломанный реальный контакт

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

Business Email Compromise – многоступенчатые атаки связанные с компрометацией корпоративной переписки

Сценарии

– Взломанный реальный контакт

– Фиктивный доверенный контакт

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

Business Email Compromise – многоступенчатые атаки связанные с компрометацией корпоративной переписки

Сценарии

– Взломанный реальный контакт

– Фиктивный доверенный контакт

– Фиктивный хорошо известный контакт

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

Business Email Compromise – многоступенчатые атаки связанные с компрометацией корпоративной переписки

Реализация

– Взлом почты

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

Business Email Compromise – многоступенчатые атаки связанные с компрометацией корпоративной переписки

Реализация

– Взлом почты

– Использование уязвимостей клиента

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

Business Email Compromise – многоступенчатые атаки связанные с компрометацией корпоративной переписки

Реализация

– Взлом почты

– Использование уязвимостей клиента

– Подделка заголовков писем

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

Business Email Compromise – многоступенчатые атаки связанные с компрометацией корпоративной переписки

Реализация

– Взлом почты

– Использование уязвимостей клиента

– Подделка заголовков писем

– Использование схожих адресов

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

Business Email Compromise

some@example.com

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

Business Email Compromise

some@**example.com**

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

some@example.com

some@exarnple.com

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

some@example.com

some@exarnple.com

sorne@example.com

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

some@example.com

some@exarnple.com

sorne@example.com

some@example.com

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Business Email Compromise

some@example.com

some@exarnple.com

sorne@example.com

some@example.com

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Статистика

ФБР Internet Crime Report 2022-2023

BEC – $2 946 830 270

Фишинг – $18 728 550

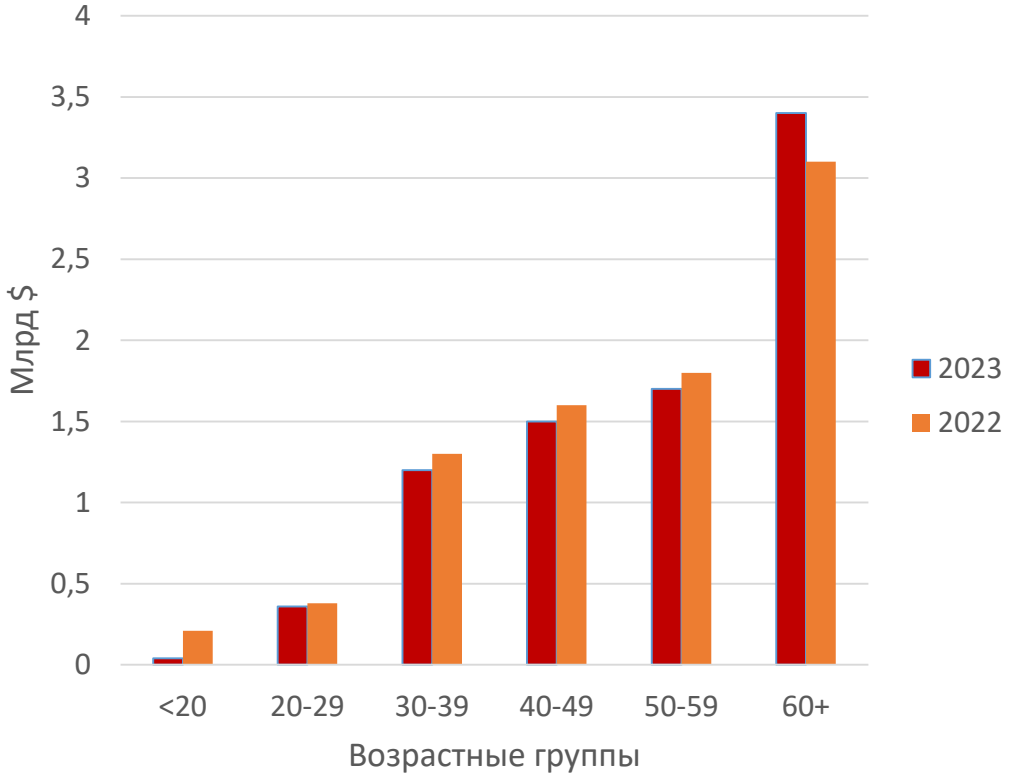
Статистика

ФБР Internet Crime Report 2022-2023

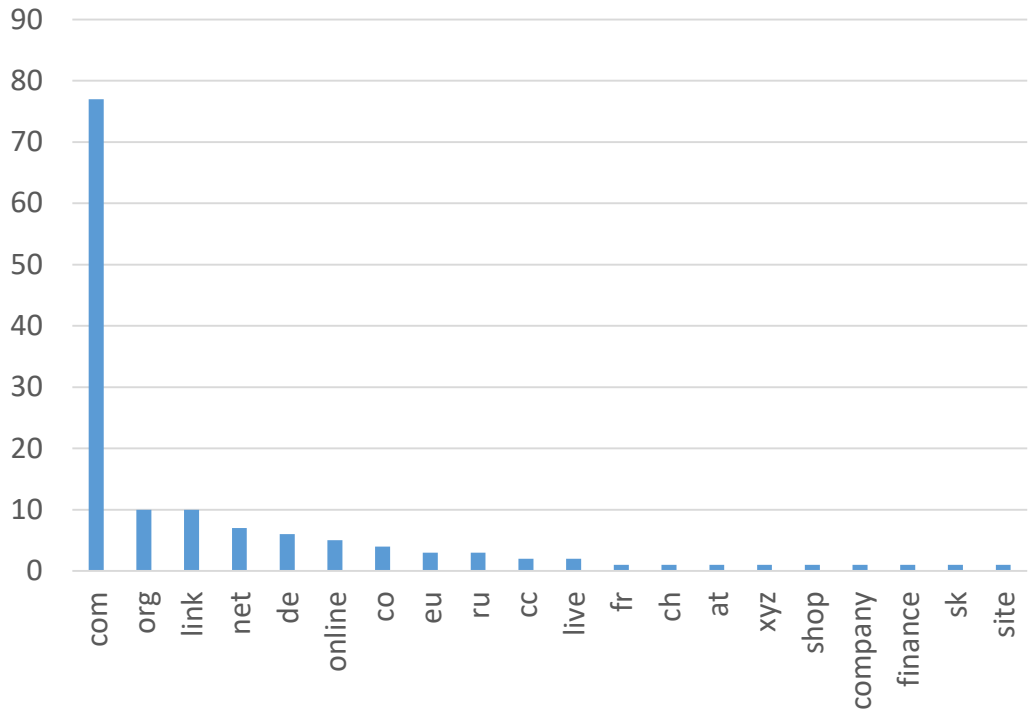
$12.5 МЛРД

BEC – $2 946 830 270

Фишинг – $18 728 550

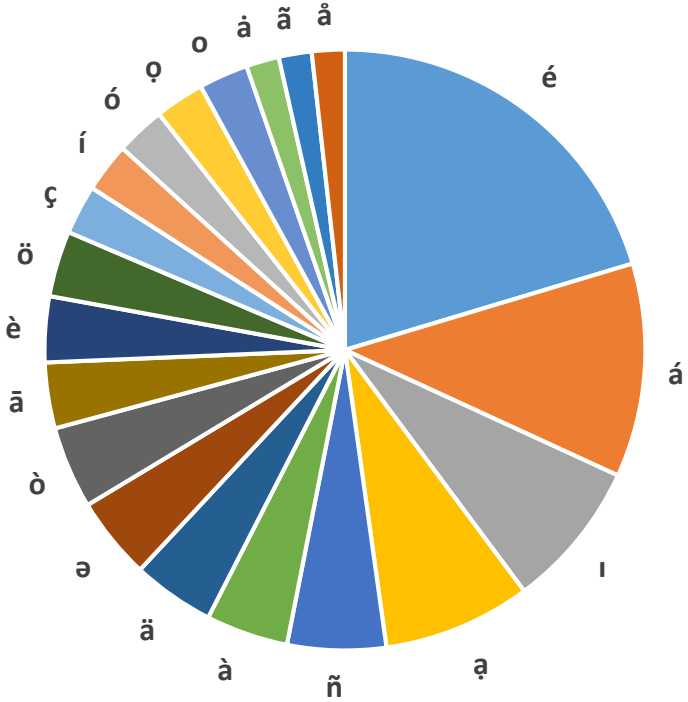


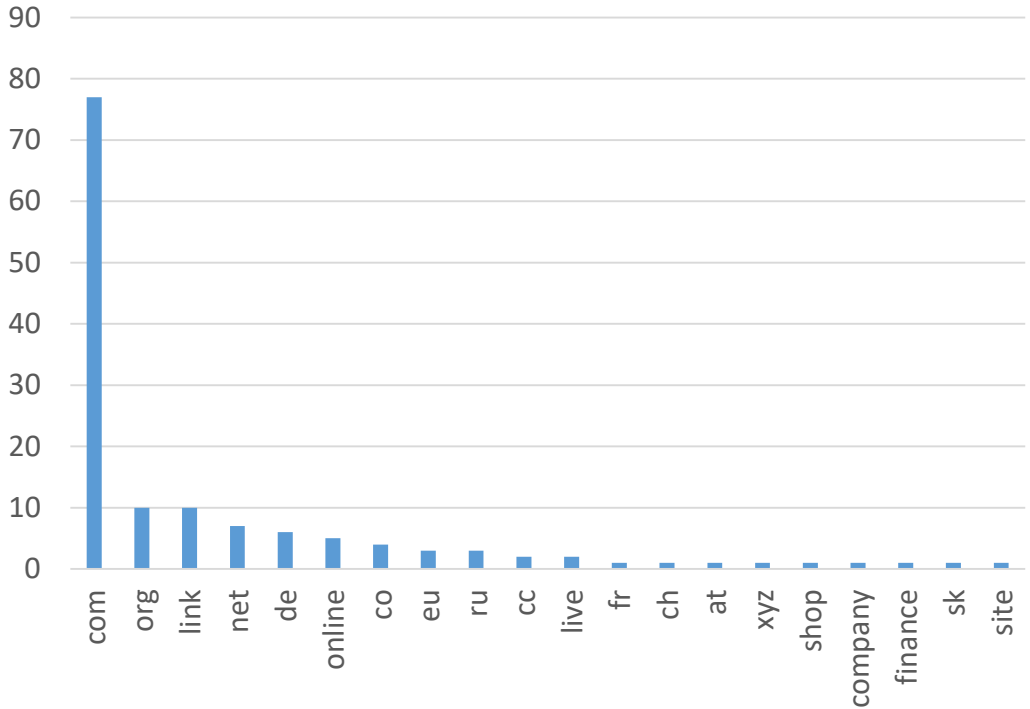
Статистика


90
80
70
60
50
40
30
20
10
0
com
org
link
net
de
online
co
eu
ru
cc
live
fr
ch
at
xyz
shop
company
finance
sk
site

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Статистика





Кейсы

— Фишинговый ресурс компании Adobe

adoḅe.com – распространение трояна BetaBot

Кейсы

— Фишинговый ресурс компании Adobe

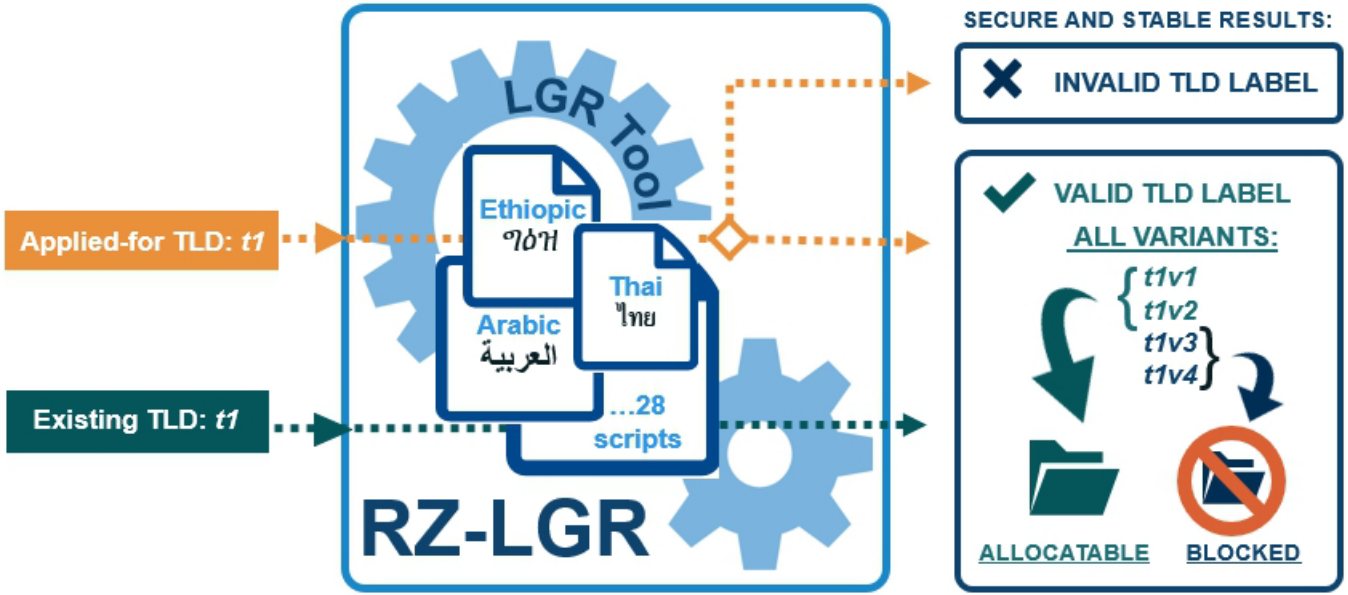
adobe.com – распространение трояна BetaBot

— Уязвимость в ПО Apple CVE-2018-4277

«ԁ» (U+A771) отображалась как «d» (U+0064)

Решения

— На уровне ICANN – Label Generation Rules



Решения

— На уровне ICANN – Label Generation Rules

— На уровне Регистратур – запрет кросскрипта и IDN-таблицы


bank.com


bank.плата.com

.РФ – только русский алфавит
.RU – только базовая латиница

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Решения

— На уровне ICANN – Label Generation Rules

— На уровне Регистратур – запрет кросскрипта и IDN-таблицы

— На уровне Регистраторов – homoglyph bundling

для **bank.com**
регистрация и bänk.com, bańk.com, bañk.com…

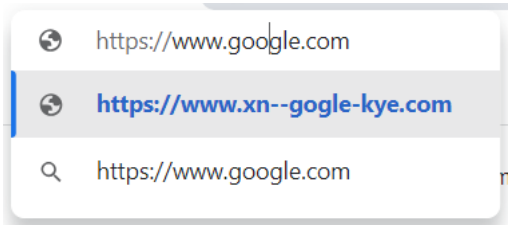
Решения

— На уровне ICANN – Label Generation Rules

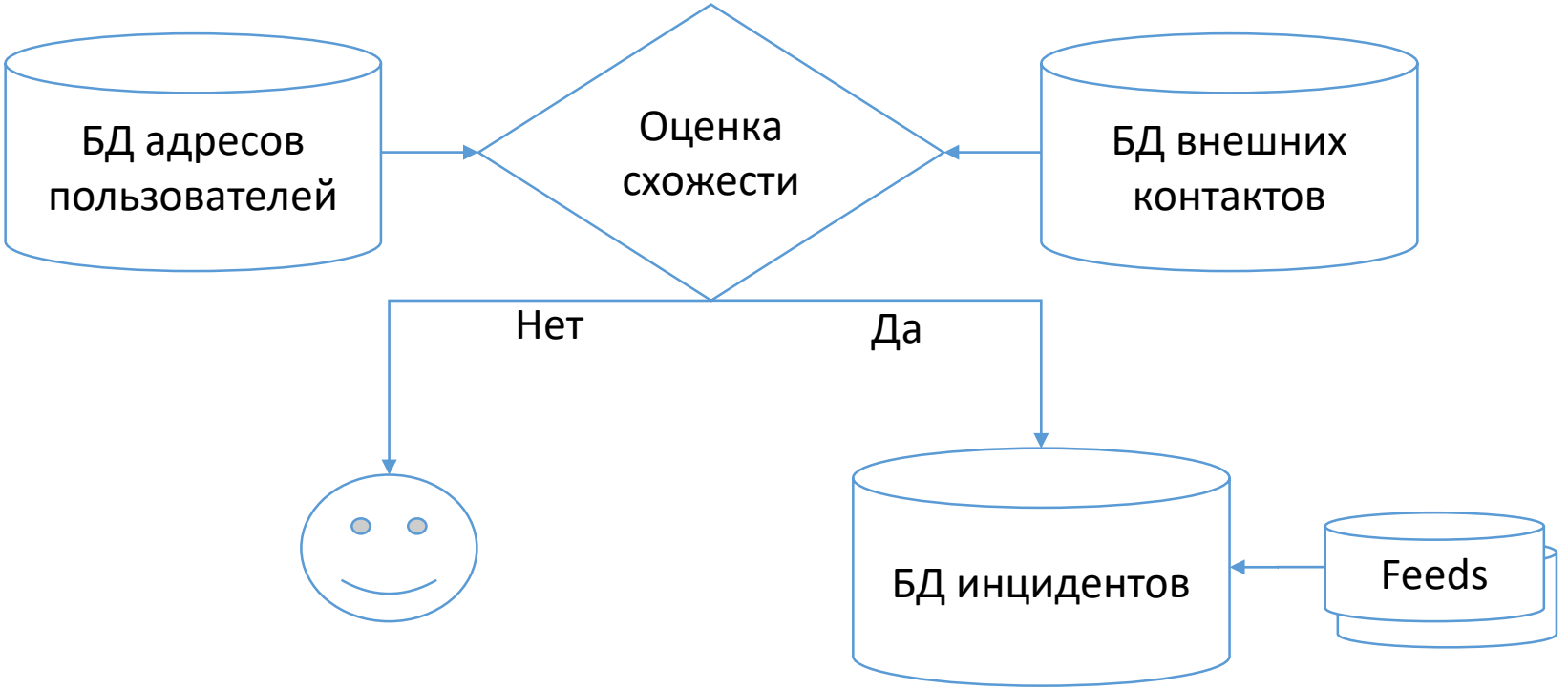
— На уровне Регистратур – запрет кросскрипта и IDN-таблицы

— На уровне Регистраторов – превентивные регистрации

— На уровне разработчиков ПО – средства нотификации пользователей



Методики


БД адресов пользователей
Оценка схожести
БД внешних контактов
Нет
Да
БД инцидентов
Feeds

Методики

Оценка схожести доменов или почтовых адресов

строковое расстояние (Дамерау — Левенштейна)

к	о	т
к	о	д

расстояние = 1

	к	о	т	и	к	
с	к	о	т	и	н	а

расстояние = 3

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Юникод

Нормализация

Неоднозначность кодирования символов

ñ = U+00F1

ñ = n ~ = U+006E U+007E

niño != niño

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Юникод

Нормализация

Приведение к каноническому представлению

– Normalization Form D (NFD)

Ṩ (U+1E69) → Ṡ (U+1E61) ̣ (U+0323) → S (U+0073) ̇ (U+0307) ̣ (U+0323)

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Юникод

Нормализация

Приведение к каноническому представлению

– Normalization Form D (NFD)

– Normalization Form C (NFC)

NFD + $n_{(U+006E)}$ $\tilde{}_{(U+007E)}$ → $\tilde{n}_{(U+00F1)}$

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Юникод

Нормализация

Приведение к каноническому представлению

– Normalization Form D (NFD)

– Normalization Form C (NFC)

– Normalization Form KD (NFKD)

™(U+2122) → T(U+0054) M(U+004D)

ﹷ(U+FE37) → {(U+007B)

¼(U+00BC) → 1(U+0031) ⁄(U+2044) 4(U+0034)

ℍ(U+210D) → H(U+0048)

Юникод

Нормализация

Приведение к каноническому представлению

– Normalization Form D (NFD)

– Normalization Form C (NFC)

– Normalization Form KD (NFKD)

– Normalization Form KC (NFKC)

NFKD + NFC

Юникод

Нормализация

Приведение к каноническому представлению

– Normalization Form D (NFD)

– **Normalization Form C (NFC)**

– Normalization Form KD (NFKD)

– Normalization Form KC (NFKC)

http://www.unicode.org/reports/tr15/

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Заключение

– новые технологии = новые риски

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Заключение

– новые технологии = новые риски

– look-a-like атаки появились раньше IDN и EAI

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Заключение

– новые технологии = новые риски

– look-a-like атаки появились раньше IDN и EAI

– существуют механизмы противодействия

– разрабатываются новые механизмы

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Заключение

– новые технологии = новые риски

– look-a-like атаки появились раньше IDN и EAI

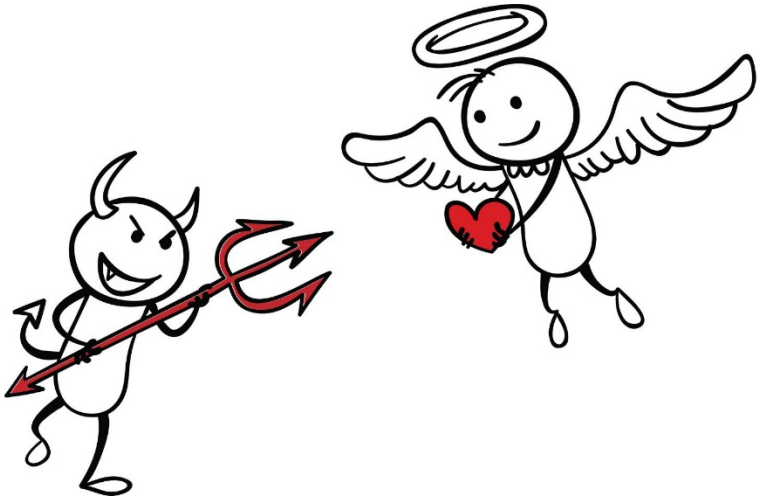
– существуют механизмы противодействия

– разрабатываются новые механизмы

– позволяют существенно снизить риски

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

Заключение



– борьба добра и зла будет всегда…

КООРДИНАЦИОННЫЙ ЦЕНТР
ДОМЕНОВ .RU/.РФ

СПАСИБО ЗА ВНИМАНИЕ!

Вадим Михайлов

mva@cctld.ru

мва@кц.рф