SURVIVAL GUIDE

ZERO NIGHTS 2019 9 EDITION

HACKERS IN THE AREA ZERONIGHTS

ZeroNights – одна из главных конференций в сфере практической информационной безопасности в Европе.

Основная аудитория ZeroNights – технические специалисты, руководители и сотрудники служб ИБ, руководители отделов ИТ, программисты и все, кто интересуется прикладными аспектами отрасли.

За **9** лет конференцию посетили более **8000** участников и **300** спикеров из **20** стран. Более **200** партнеров поддержали мероприятие, а также мы получили около **4000** упоминаний в российских и зарубежных СМИ.

ДАТА И ВРЕМЯ

12–13 ноября, 9:30–20:00

МЕСТО

Санкт-Петербург, пр. Медиков, 3, клуб А2.

Сцена, на которую выходили легендарные рок-группы: Limp Bizkit, Smashing Pumpkins, New Order и другие.

ЧТО НУЖНО СДЕЛАТЬ ПЕРЕД КОНФЕРЕНЦИЕЙ?

- Проверить свои билеты на конференцию (электронные или печатные).
- Взять с собой документы (паспорт, водительские права, студенческий билет).
- Обязательно подписаться на соц. сети ZeroNights, чтобы быть в курсе всех оперативных изменений и новостей конференции, а также конкурсов от наших партнеров (**Telegram, Twitter, Instagram**).

РЕГИСТРАЦИЯ

12 ноября, 09:30. Клуб А2.

ПРЕДВАРИТЕЛЬНАЯ РЕГИСТРАЦИЯ

11 ноября, 15:00–21:00. Клуб А2

Первые 250 зарегистрированных участников получат приятный сувенир от организаторов ZeroNights.

ОФИЦИАЛЬНОЕ ОТКРЫТИЕ КОНФЕРЕНЦИИ

12 ноября, 10:30. Клуб А2

ДОКУМЕНТЫ

1. Если вы студент, обязательно возьмите с собой студенческий, его будет необходимо предъявить на регистрации.
2. Рекомендуем всем участникам взять с собой документы: паспорт или водительские права. Они понадобятся, чтобы арендовать оборудование для синхронного перевода. Или, если Вам повезло и Вы выглядите младше 18, документ попросит предъявить команда радушных, но крайне бдительных барменов.

ЧТО РАЗРЕШЕНО ПРОНОСИТЬ НА КОНФЕРЕНЦИЮ

Участники конференции могут взять с собой гаджеты, еду, безалкогольные напитки.

ЧТО ЗАПРЕЩЕНО ПРОНОСИТЬ НА КОНФЕРЕНЦИЮ

Попросят оставить за пределами клуба: алкогольные напитки, колюще-режущие предметы, взрывоопасные вещества.

КАК ДОБРАТЬСЯ

- от Аэропорта регулярные автобусы №39 и 39Э довезут вас до ближайшей станции метро – м. Московская (голубая ветка)

  Ценители комфорта могут вызвать такси. Убер в центр города обойдется около 600-800р.

- Если вы прибываете на Московский вокзал, в вашем распоряжении: ст. м. Площадь Восстания (красная ветка), переход с неё на ст. м. Маяковская (зеленая ветка), а также наземный транспорт в разные уголки города.

Ваша станция назначения – ст.м. Петроградская.

ВЕЧЕРИНКА

12 ноября, по завершении программы докладов состоится вечеринка для спикеров и участников, купивших расширенный билет. Если на вашем билете есть строчка “вход на вечеринку”, то вы точно туда проходите. Вечеринка начинается в 19:00 в зале «Спутник» клуба А2.

ZERO NIGHTS MARKET

Наверняка вы знаете, что мы запустили маркет уникального мерча ZeroNights. Свои предзаказы вы можете получить в первый день мероприятия. Market расположен на 1 этаже клуба, напротив стенда Сбербанка. Доступна оплата картой и наличными. Приготовьте, пожалуйста, заранее номер заказа.

ПРОГРАММА КОНФЕРЕНЦИИ

Мы очень стараемся, чтобы всё шло по плану, но на случай возможных изменений следите за нашим Telegram-каналом

ПРОГРАММА

12 НОЯБРЯ

ВРЕМЯ	MIN	ЗАЛ МИР*
09:30	60	Регистрация
10:30	30	Торжественная церемония открытия
11:00	45	**Александр Матросов (@matrosov)** "Hardware Security is Hard: how hardware boundaries define platform security"
12:00	45	**Юнтао Ван** "From JDBC URI to a New Remote Code Execution Attack Surface"
13:00	45	**Юхо Нурминен (@jupenur)** "app setAsDefaultRCE Client: Electron, scheme handlers and stealthy security patches"
14:00	45	**Ан "tint0" Трин (@_tint0)** "Dark sides of Java remote protocols"
15:00	30	**Якуб Врана (@jakubvrana), Кшиштоф Котович (@kkotowicz)** "Trusted Types & the end of DOM XSS"

15:40	30	**md4** "CiscoASA: From Zero to ID=0"
16:20	30	**Андрей Акимов (@e13fter)** "Launching feedback-driven fuzzing on TrustZone TEE"
17:00	15	**Эмиль Лернер** "Single byte write to RCE: exploiting a bug in php-fpm"
17:25	15	**Мария Недяк (@mariya_ns)** "Hacking Medical Imaging with DICOM"
17:50	15	**Алексей Коврижных (@a1exdandy)** "crauEmu – your IDE for code-reuse attacks"
18:15	15	**Роман Палкин (@chicken_2007)** "Malign Machine Learning Models"

В программе возможны изменения времени докладов и дополнения.
*** Внимание! Синхронный перевод доступен только зале Мир (RU – EN, EN – RU)**

ВРЕМЯ	MIN	ЗАЛ СПУТНИК* (DEFENSIVE TRACK)
09:30	60	Регистрация
12:00	45	**Андрей Беленко** "(Why) We Still Fail at Cryptography in 2019"
13:00	45	**Павел Каргапольцев** "Stories and lessons from daily incident response practice"
14:00	45	**Кирилл Демьянов** "Building CyberSecurity Platform based on Open Source"
15:00	45	**Игорь Грачев, Евгений Сидоров** "Improving application security and exploitation detection with AppArmor & Osquery"
16:00	30	**Андрей Скаблонский** "Threat hunting in call trace"
16:40	30	**Андрей Абакумов, Андрей Красичков** "Взгляд Blue Team на поиск 'секретов' в коде"
19:00		**Вечеринка для спикеров (вход только по VIP билетам)**

ПРОГРАММА 2 ДЕНЬ

13 НОЯБРЯ

ВРЕМЯ	MIN	ЗАЛ МИР*
10:00	60	Регистрация
11:00	45	**Мэтт Суиш (@msuiche)** "From Memory Forensics to Cloud Memory Analysis"
12:00	45	**LimitedResults (@LimitedResults)** "Fatal Fury on ESP32: Time to release Hardware Exploits"
13:00	45	**Кэ Лю (@klotxl404)** "Two Bytes to Rule Adobe Reader Twice: The Black Magic Behind the Byte Order Mark"
14:00	45	**Хоссейн Лотфи (@hosselot)** "A Monkey in the Sandbox: Exploiting Firefox Through IonMonkey JIT and Kernel Sandbox Escapes"
15:00	45	**Павел Черемушкин** "Opwnsource: VNC vulnerability research"
16:00	45	**Кай Джерн Лау (@sgniwx), Нгэнь Ан Куэнь (@capstone_engine)** "qiling.io: Advanced Binary Emulation framework"
17:00	45	**Цезарь Серрудо (@cesarcer), Эстебан Мартинес Файо (@estemf), Матиас Секвейра** "Practical LoRaWAN auditing and exploitation"
18:00	30	**CiscoPangPang** "Cisco to Disco!"
18:40	30	**Илья Шапошников (@drakylar)** "Oldschool way of hacking MicroDigital ip-cameras"
19:30	30	**Торжественная церемония закрытия**

В программе возможны изменения времени докладов и дополнения.
* Внимание! Синхронный перевод доступен только зале Мир (RU – EN, EN – RU)

ВРЕМЯ	MIN	ЗАЛ СПУТНИК* (WEB VILLAGE)
10:00	60	Регистрация
12:00	25	**Алексей "GreenDog" Тюрин (@antyurin)** "От мисконфига к суровым последствиям"
12:30	25	**Павел “sorokinpf” Сорокин (@sorokinpf)** "GraphQL applications security testing automatization"
13:00	25	**Валерий “krevetk0” Шевченко (@Krevetk0Valeriy)** "Принципы тестирования и баги, которые проглядели остальные"
13:30	25	**Алексей “SooLFaa” Морозов (@xSooLFaa)** "Blind SSRF"
14:00	25	**Викторина**
14:30	25	**Рамазан "r0hack" Рамазанов** "Эксплуатация инъекций в ORM-библиотеках"
15:00	25	**Сергей "BeLove" Белов (@sergeybelove)** "Будущее без паролей – про WebAuthN и не только"
15:30	25	**Paul Axe (@Paul_Axe)** "ZN PWN Challenge"
16:00	45	**Денис “ttffdd” Рыбин (@_ttffdd_)** "Аудитим зоопарк сервисов AWS"
17:00	25	**Андрей Пластунов** "ООП в mvc фреймворках. Как не сделать хуже, чем было"
17:30	25	**Антон “Bo0oM” Лопаницын (@i_bo0om)** "Охота на феникса"
18:00	25	**Викторина**

В программе возможны изменения времени докладов и дополнения.
*** Внимание! Синхронный перевод доступен только зале Мир (RU – EN, EN – RU)**

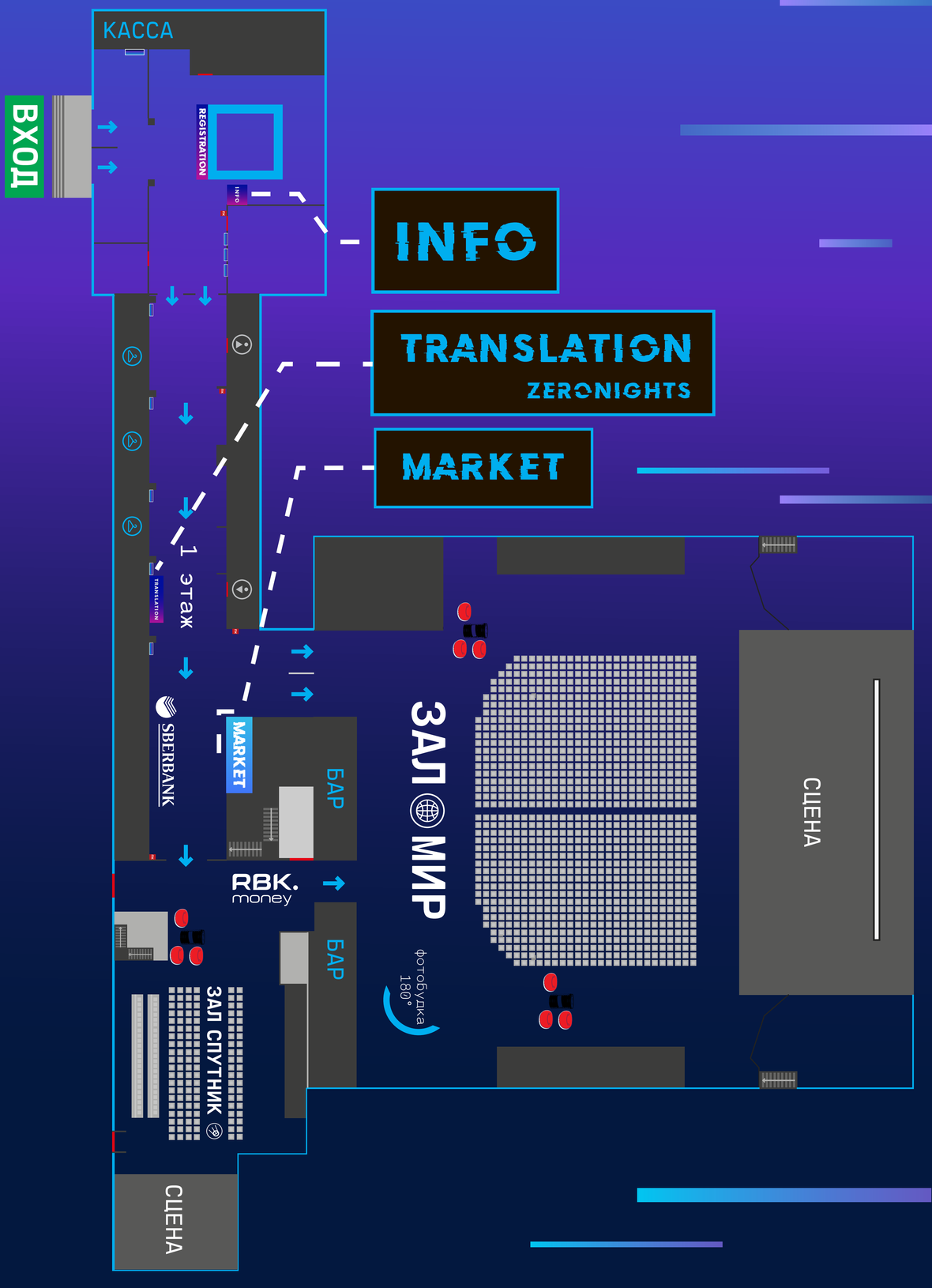
КОНКУРСЫ

На протяжении всей конференции партнеры ZeroNights будут проводить конкурсы и квизы. Участники, успешно выполнившие задания, получат ценные призы и сувениры. Полный список конкурсов и активностей можно найти здесь.

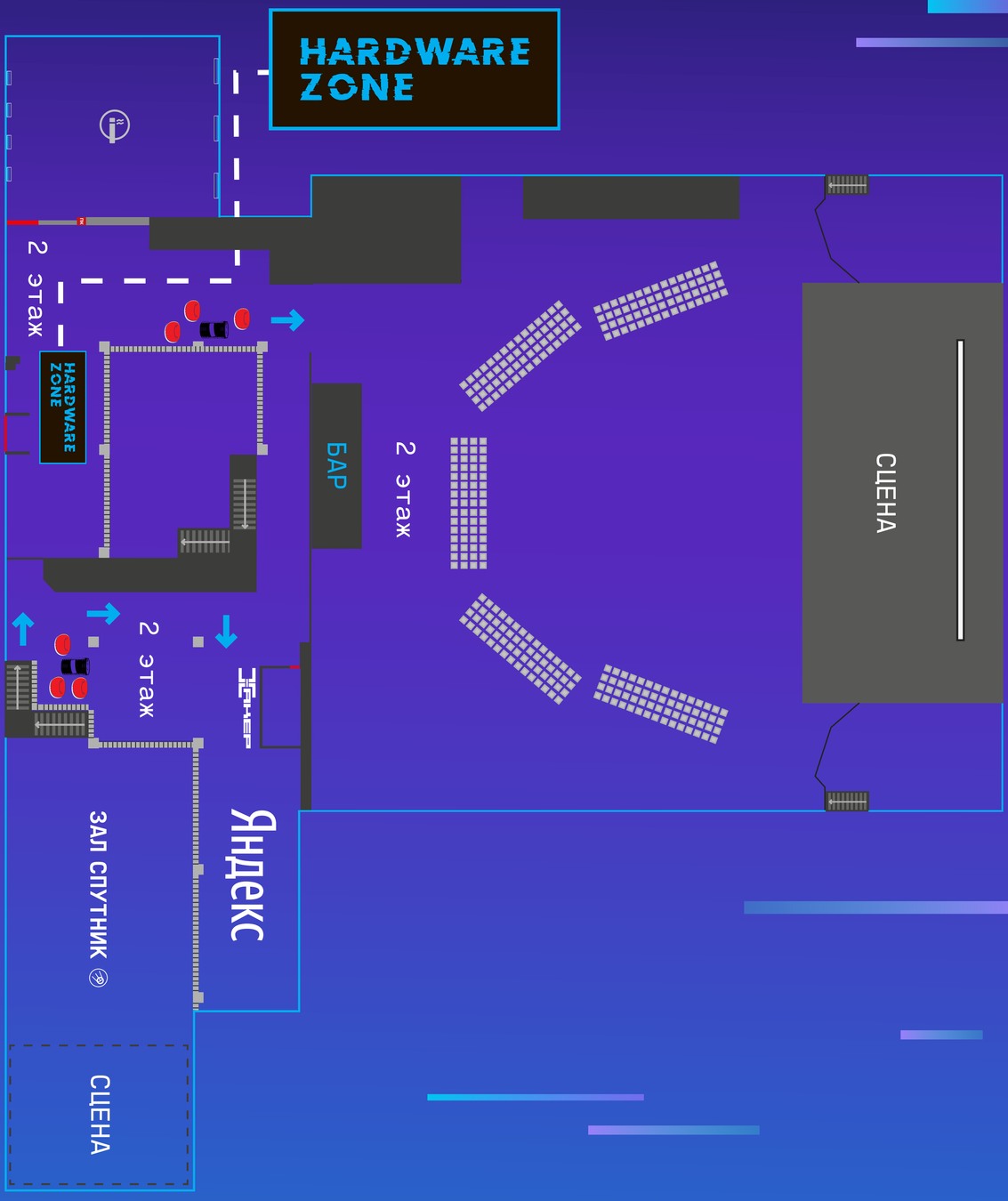
ATTENTION!

Советуем заранее установить приложение Kahoot! оно пригодится вам на конференции.

КАРТА ПЛОЩАДКИ



КАРТА ПЛОЩАДКИ 2 ЭТАЖ



ПАРТНЕРЫ

Яндекс

RBK. money

SECURE SOFTWARE SOLUTIONS

SBERBANK

@ mail

Digital Security