SURVIVAL GUIDE

ZERO NIGHTS 2019 EDITION

HACKERS IN THE AREA ZERONIGHTS

ZeroNights is one of the main conferences on practical aspects of cybersecurity in Europe.

It is meant for technical specialists, heads and members of security teams, heads of IT departments, programmers, and all those interested in the applied aspects of cybersecurity.

Since its foundation, the conference has welcomed more than **8000** participants and **300** speakers from **20** countries. It has been supported by more than **200** partners and received over **4000** mentions in the field-oriented media.

WHAT YOU MAY TAKE TO THE VENUE

Participants are allowed to bring gadgets, food, soft drinks.

WHAT YOU MAY NOT TAKE TO THE VENUE

Participants are not allowed to bring alcoholic beverages, bladed articles, explosive substances.

HOW TO GET TO THE VENUE

- From the airport using public transport, you need buses #39 and #393. Those will take you to the nearest metro – Moskovskaya (Blue line).
- You can also take a taxi. An Uber to the city center will cost you 600–800 rub.
- If you arrive at the Moskovsky railway station (Red line), you can take the metro (Ploschad Vosstaniya – Green line), or one of the many buses that go anywhere in the city.

Petrogradskay metro station, Prospekt Medikov 3

PARTY

On November 12, there will be a party for those who have special bracelets. If your ticket reads “party entrance”, you’ll get one. The party starts at 19:00 at the “Sputnik” hall.

ZERO NIGHTS MARKET

You certainly know that we have a market with branded apparel. Anything you ordered there, you can purchase and get during the first day of the event. You can find ZeroNights Market on the club's 1st floor in front of the Sberbank stand. Please, prepare your order number in advance. We accept cards and cash.

PROGRAM

You can also keep track of potential changes in it in our official Telegram channel.

DAY 1

NOVEMBER 12

TIME	MIN	HALL MIR*
09:30	60	Registration
10:30	30	Opening ceremony
11:00	45	**Alex Matrosov (@matrosov)** "Hardware Security is Hard: how hardware boundaries define platform security"
12:00	45	**Yongtao Wang** "From JDBC URI to a New Remote Code Execution Attack Surface"
13:00	45	**Juho Nurminen (@jupenur)** "app setAsDefaultRCE Client: Electron, scheme handlers and stealthy security patches"
14:00	45	**An Trinh (@_tint0)** "Dark sides of Java remote protocols"
15:00	30	**Jakub Vrana (@jakubvrana), Krzysztof Kotowicz (@kkotowicz)** "Trusted Types & the end of DOM XSS"

15:40	30	**md4** "CiscoASA: From Zero to ID=0"
16:20	30	**Andrey Akimov (@e13fter)** "Launching feedback-driven fuzzing on TrustZone TEE"
17:00	15	**Emil Lerner** "Single byte write to RCE: exploiting a bug in php-fpm"
17:25	15	**Maria Nedyak (@mariya_ns)** "Hacking Medical Imaging with DICOM"
17:50	15	**Alex Kovrizhnykh (@a1exdandy)** "crauEmu - your IDE for code-reuse attacks"
18:15	15	**Roman Palkin (@chicken_2007)** "Malign Machine Learning Models"

There may be time changes and updates to the program.
* Attention! Simultaneous translation is available in the Hall Mir only! (RU – EN, EN – RU)

TIME	MIN	HALL SPUTNIK* (DEFENSIVE TRACK)
09:30	60	Registration
12:00	45	**Andrey Belenko** "(Why) We Still Fail at Cryptography in 2019"
13:00	45	**Pavel Kargapoltsev** "Stories and lessons from daily incident response practice"
14:00	45	**Kirill Demyanov** "Building CyberSecurity Platform based on Open Source"
15:00	45	**Igor Grachev, Evgeny Sidorov** "Improving application security and exploitation detection with AppArmor & Osquery"
16:00	30	**Andrey Skablonsky** "Threat hunting in call trace"
16:40	30	**Andrey Abakumov, Andrew Krasichkov** "Blue Team's approach to discovering 'secrets' in code"
19:00		**Speaker party (VIP tickets only)**

PROGRAM DAY 2

NOVEMBER 13

TIME	MIN	HALL MIR*
10:00	60	Registration
11:00	45	**Matt Suiche (@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	**Ke Liu (@klotxl404)** "Two Bytes to Rule Adobe Reader Twice: The Black Magic Behind the Byte Order Mark"
14:00	45	**Hossein Lotfi (@hosselot)** "A Monkey in the Sandbox: Exploiting Firefox Through IonMonkey JIT and Kernel Sandbox Escapes"
15:00	45	**Pavel Cheremushkin** "Opwnsource: VNC vulnerability research"
16:00	45	**Kai Jern Lau (@sgniwx), Nguyen Anh Quynh (@capstone_engine)** "qiling.io: Advanced Binary Emulation framework"
17:00	45	**Cesar Cerrudo (@cesarcer), Esteban Martinez Fayo (@estemf), Matias Sequeira** "Practical LoRaWAN auditing and exploitation"
18:00	30	**CiscoPangPang** "Cisco to Disco!"
18:40	30	**Ilya Shaposhnikov (@drakylar)** "Oldschool way of hacking MicroDigital ip-cameras"
19:30	30	**Closing ceremony**

There may be time changes and updates to the program.
* Attention! Simultaneous translation is available in the Hall Mir only! (RU – EN, EN – RU)

TIME	MIN	HALL SPUTNIK* (WEB VILLAGE)
10:00	60	Registration
12:00	25	**Aleksei "GreenDog" Tiurin (@antyurin)** "From misconfigs to severe consequences"
12:30	25	**Pavel “sorokinpf” Sorokin (@sorokinpf)** "GraphQL applications security testing automatization"
13:00	25	**Valeriy “krevetk0” Shevchenko (@Krevetk0Valeriy)** "Principles in software testing and some bugs that others did not notice"
13:30	25	**Alexei “SooLFaa” Morozov (@xSooLFaa)** "Blind SSRF"
14:00	25	**Kahoot Quiz**
14:30	25	**Ramazan "r0hack" Ramazanov** "Operation of injections in ORM libraries"
15:00	25	**Sergey "BeLove" Belov (@sergeybelove)** "The future without passwords"
15:30	25	**Paul Axe (@Paul_Axe)** "ZN PWN Challenge"
16:00	45	**Denis “ttffdd” Rybin (@_ttffdd_)** "Doing AWS Zoo Audit"
17:00	25	**Andrei Plastunov** "Misusing oop in mvc frameworks. How to conveniently develop broken apps"
17:30	25	**Anton "Bo0oM" Lopanitsyn (@i_bo0om)** "Phoenix hunting"
18:00	25	**Kahoot Quiz**

There may be time changes and updates to the program.
* Attention! Simultaneous translation is available in the Hall Mir only! (RU – EN, EN – RU)

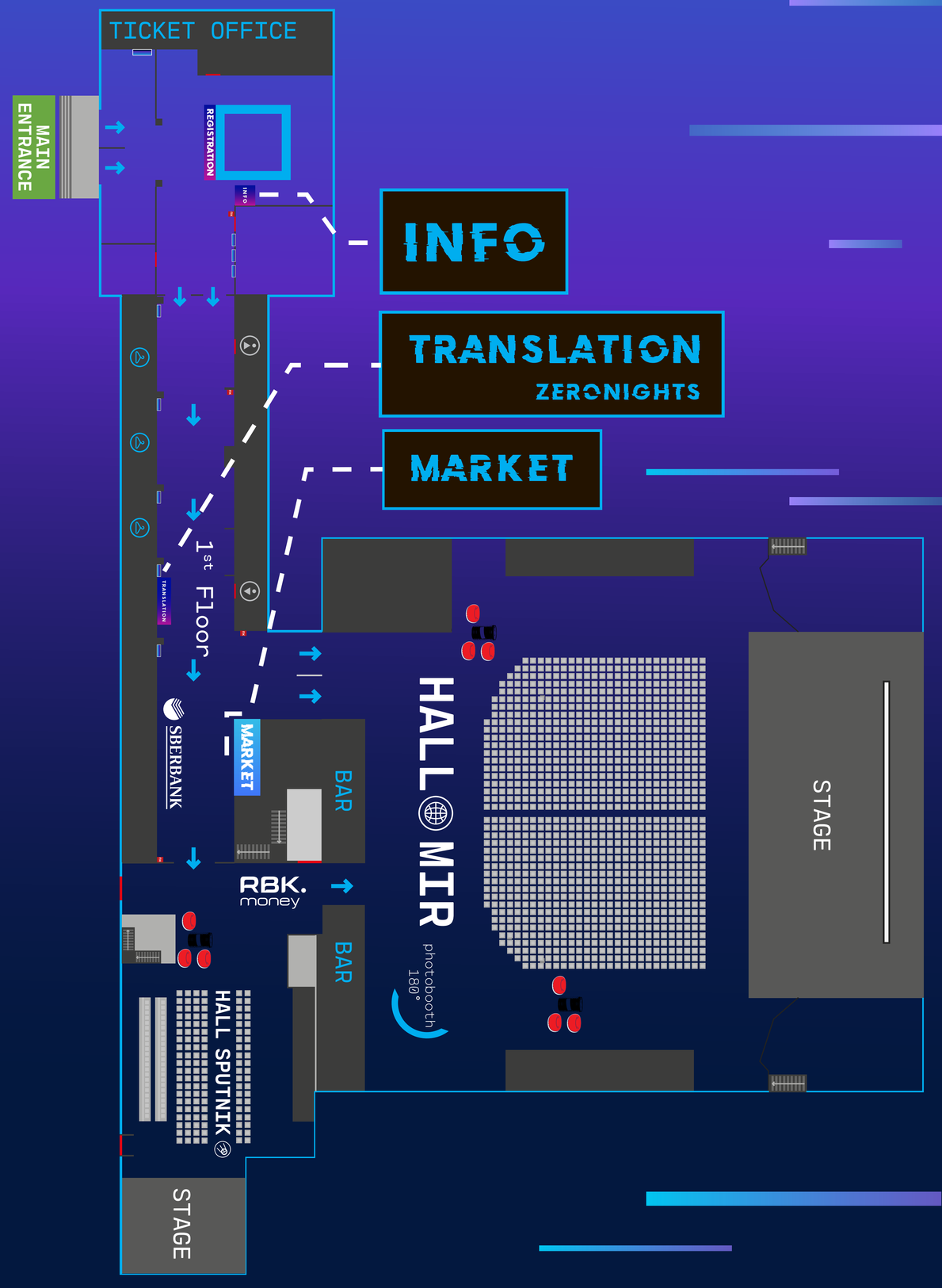
ACTIVITIES

During the conference, the partners of ZeroNights 2019 will hold quests and quizzes. The winners will get valuable prizes and souvenirs. The full list of activities can be found here.

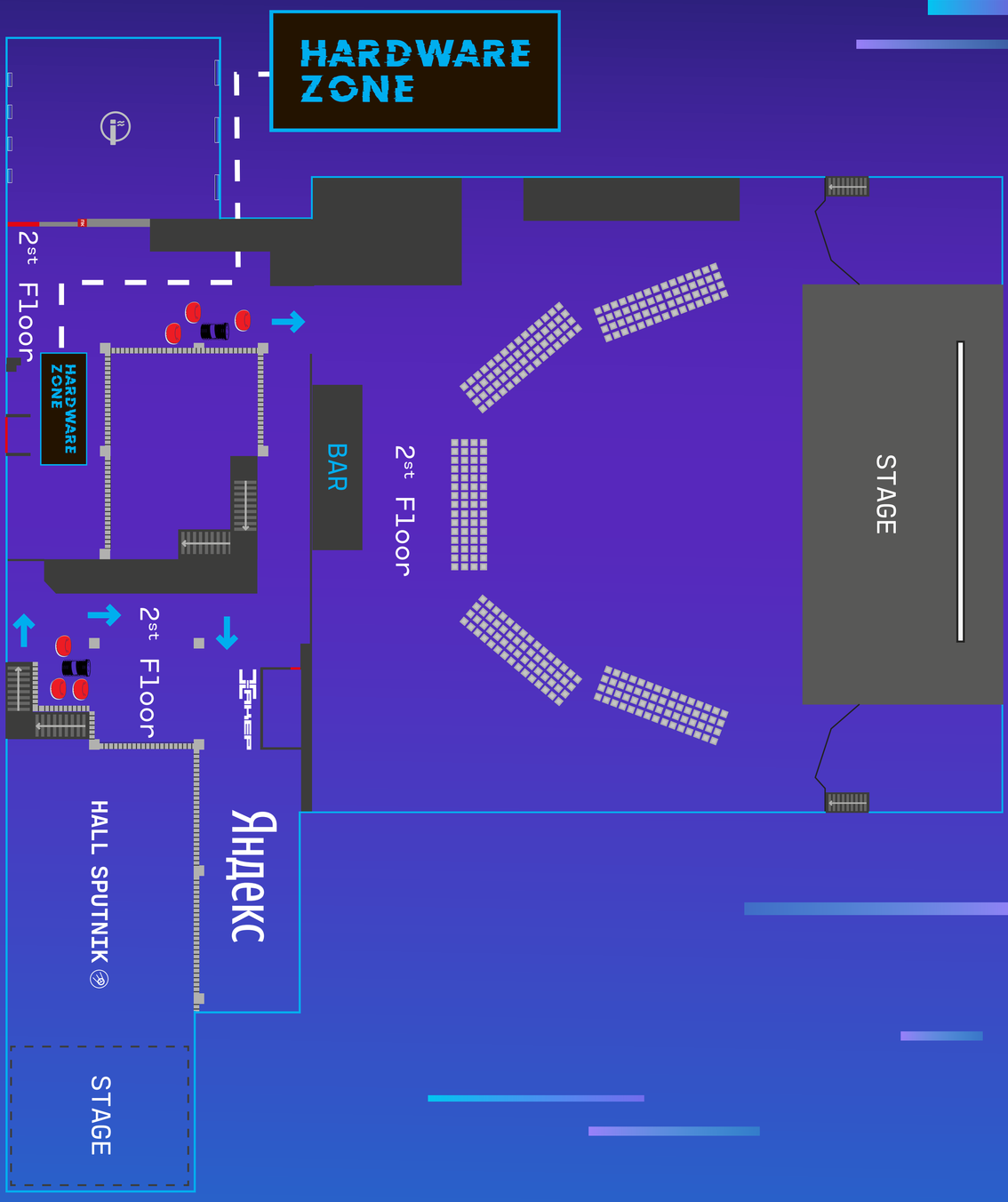
ATTENTION!

We recommend installing the Kahoot! application before the conference.

VENUE MAP



VENUE MAP 2ST FLOOR



PARTNERS

SECURE SOFTWARE SOLUTIONS

SBERBANK

mail

Digital Security