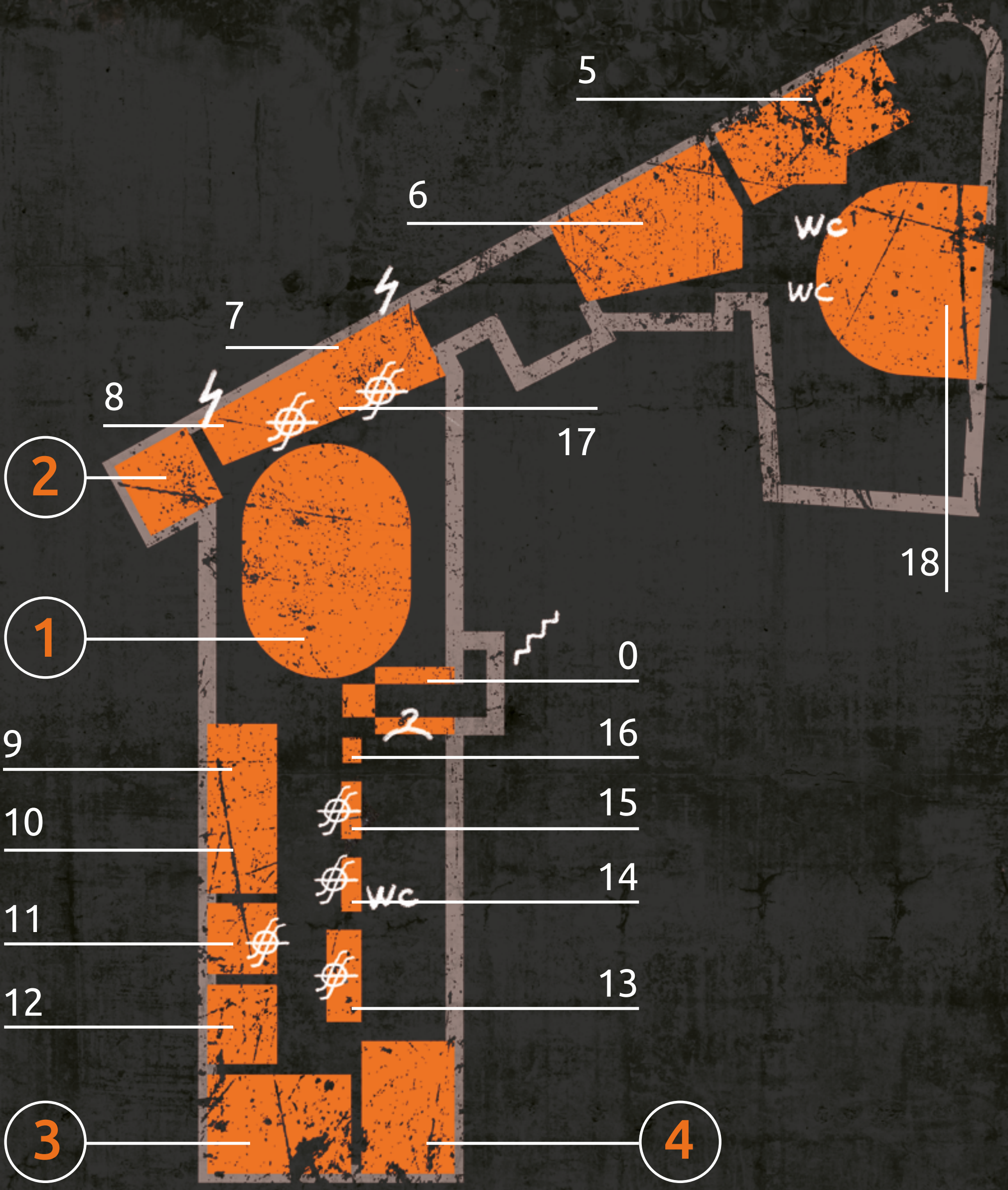
WELCOME TO OFFZONE

November 15 – 16, 2018

OFFZONE
2018

Location map



0	Registration
①	MAIN TRACK
②	HARDWARE.ZONE
③	WEB.ZONE / FAST TRACK
④	FINANCE.ZONE
5	Speaker room
6	Bar
7	LOUNGE.ZONE
8	Foosball “Zombies vs Survivors”
9	Qiwi
10	Wallarm
11	GAME.ZONE
12	Kaspersky Lab
13	BI.ZONE
14	Offcoin tanks
15	TATTOO.ZONE
16	Secret Shop
17	Pedal Powered Race Track
18	CTFZONE
⚡	Зарядные станции
#	Offcoin

November 15

	MAIN TRACK		HARDWARE.ZONE
11:30	Opening ceremony		
12:00	20 years of Information Security: researcher’s view Dmitry Sklyarov, Positive Technologies		
13:00	We will charge you. How to [b]reach vendor’s network using EV charging station Dmitry Sklyar, Kaspersky Lab	13:00	Quick guide to Software Defined Radio Aleksandr Alekseev, Independent researcher
14:00		14:00	Getting to know GnuRadio Daniil Pogorelov, Independent researcher
15:00	Wake up, Neo: detection of virtualization via speculative execution Innokenty Sennovsky, BI.ZONE	15:00	Introduction to Circuit Design Anton Kanyshev, Hardware designer
16:00	Vulnerabilities of mobile OAuth 2.0 Nikita Stupin, Mail.Ru Group	16:00	STM32 microcontrollers: Introduction Aleksandr Alekseev, Independent researcher
17:00	Lazarus group: a mahjong game played with different sets of tiles Michal Poslušný and Peter Kálnai, ESET	17:00	Hardware reverse: DIY Egor Litvinov, GS-Labs
18:00	HIDS as a service: deployment and control over 20 000 installations Ivan Agarkov, Wargaming	18:00	Fault Injection attacks on ARM MK Arseniy Zhgilev, BI.ZONE
19:00		19:00	

November 15

FINANCE.ZONE

13:00 **Cashless payments — how it works**
Dmitry Gadar, Tinkoff.ru

14:00 **Fraud evolution**
Igor Mityurin, Sberbank

15:00

16:00 **Android Malware Hunting: Novel “sandbox” techniques for identifying threat actors**
Boris Ivanov, BI.ZONE

17:00 **Antifraud**
Ekaterina Blinova, Yandex.Money

18:00

WEB.ZONE

13:00 **Another way to bypass WAF: Cheat Sheet**
Anton Lopanitsyn,
Bughunter and researcher

14:00 **DNS Rebinding in 2k18**
Mikhail Firstov and Andrey Skuratov,
FBK CyberSecurity

15:00

16:00 **HTTP/2**
Magomed Nurov, BI.ZONE

17:00 **XSS Exploiting**
Igor Sak-Sakovskiy, Positive Technologies

18:00 **Attacking the multi-layered web applications**
Omar Ganiev, Deteact

19:00

November 16

	MAIN TRACK		HARDWARE.ZONE
11:00	**Is biometrics technology mature enough for mass use?** Nikita Vdovushkin and Vladislav Lazarev, BI.ZONE	11:00	**Side Channel attacks** Innokenty Sennovsky, BI.ZONE
12:00	**Secrets Windows DPAPI** Konstantin Evdokimov, M-13	12:00	**Zigbee: Introduction** Egor Litvinov, GS-Labs
13:00	**Violation of the most valuable: attacks on license managers** Sergey Temnikov and Vladimir Daschenko, Kaspersky Lab	13:00	**How to intercept and process digital signals using nRF24** Daniil Pogorelov, Independent researcher
14:00		14:00	**How to launch GSM base station: Motorola and USRP** Daniil Pogorelov, Independent researcher
15:00	**Intel ME Manufacturing Mode — a phantom menace** Maxim Goryachy and Mark Ermolov, Positive Technologies	15:00	**Physical security: theory and practice of pick locking** Danila Zgonnikov, Independent researcher
16:00	**Getting your hands dirty: A practical approach towards learning secure coding through interactive problem solving** Anirudh Anand and Mohan Kallepalli, Flipkart	16:00	**How to make pick locks for different types of lock** Danila Zgonnikov, Independent researcher
17:00	**Hunting for Privilege Escalation in Windows Environment** Teymur Heirhabarov, Kaspersky Lab	17:00	
18:00			
18:30	**CTFZONE Award Ceremony and Conference Closing Remarks**		

November 16

FINANCE.ZONE

11:00 **For the sake of money. Payment endpoint's vulnerabilities**
Timur Yunusov and Yaroslav Babin,
Positive Technologies

12:00

13:00 **ATM Security**
Aleksey Stennikov,
Positive Technologies

14:00 **Online Banking Security**
Arkadiy Litvinenko, BI.ZONE

15:00

FAST TRACK

11:00 **Things Pro Suite — under the bonnet of Moxa IIoT gateway** Aleksandr Nochvay

11:30 **OAuth2.0@2018: You are doing it wrong**
Aleksey Chernykh

12:00 **Hacking Telephone Systems**
Himanshu Mehta

12:30

13:00 **Ins and outs of Cisco ASA debugging**
Ilya Kostyulin and Sergey Ovchinnikov

13:30 **MS Exchange relay attack**
Olga Karelova

14:00 **Story of one DevSecOps**
Denis Ratchenko, Alexey Guskov and Artem Bachevsky

14:30

15:00 **AppSec as a Code**
Anton Basharin and Yury Shabalin

15:30

16:00 **Scanner Orchestration Tool — one-click SDLC**
Ivan Elkin and Ilya Govorkov

16:30 **HWallet: the simplest Bitcoin hardware wallet**
Nemanja Nikodijevic

17:00 **IP reputation: doing it wrong**
Denis Gorchakov

17:30 **What's new about Android security?**
Yury Shabalin

18:00

Zones

MAIN TRACK

At the Main Track Maxim Goryachy and Mark Ermolov (report “Intel ME Manufacturing Mode – a phantom menace”) and Innokenty Sennovsky (“Wake up, Neo: detection of virtualization via speculative execution”) will talk about the sensational low-level vulnerabilities.

What methods are typically used by cybercriminals to escalate privileges in Windows? Common types of attacks on license managers. Techniques and tools used by Lazarus. Are biometric systems sufficiently developed for mass use and how to circumvent them. These are just a few of the topics that we will cover on the Main Track in the two days of the conference.

HARDWARE.ZONE

If you have long had a desire to try yourself in hardware and you were waiting for a sign, then this is it. The HARDWARE.ZONE speakers will explain in simple terms about the most interesting areas of hardware security: GnuRadio, introduction to circuitry, STM32 microcontrollers, side channel attacks, interception and processing of digital signals using nRF24 as an example, fault injection attacks on ARM MK and many other things (this zone will stay open for two days). And, of course, this is the place to get your favorite picklocks!

Zones

FINANCE.ZONE

In the FINANCE.ZONE we will understand how cyber security really works in the world of finance.

We'll start with the basics and try to figure out how its processing works, then move on to fraud and anti-fraud with real cases, and to round off the show, we'll dive into the technical details of breaking into and protecting financial systems and their individual components, and deal with security of ATM and RBS.

WEB.ZONE

We will analyze alternative ways to bypass WAF, consider what a DNS Rebinding attack in 2k18 is, understand inside working processes of HTTP / 2 and which attacks can no longer be performed, discuss approaches to analyzing multi-layered applications and, of course, talk about the operation of XSS in the WEB.ZONE.

May the web be with you!

FAST TRACK

The Fast Track is planned for the second day of the conference, so if you are interested in the line-up for the Fast Track, please check the schedule for the 16th of November.

In the first half of the day we'll discuss the execution of OAuth 2.0, DNS Exfiltration, as well as tools for running phishing operations for the Red Team. Also, here you will learn about the research done in breaching phone systems and study the workings of IIoT-gateways and Things Pro Suite.

Reports planned for the second part have been merged with the Defensive Track: if the words DevSecOps, SDLC and AppSec mean anything to you, know that we are waiting to hear your interesting questions for the speakers.

GAME.ZONE

Mix business with pleasure and relive the arcade experience. Engage in some of the worlds favourite games: Mortal Kombat XL, Worms TM:, Battlegrounds and TEKKEN 7 – battle your opponent and win OFFCOINS. Oh, yeah, and we also have not forgotten the good old Nintendo and SEGA consoles. It is definitely worth your while to stop by the GAME.ZONE and rip delight off your favourite games!

The badge card tasks

You don't need to look far for a smart device: your badge card can do many a cool thing. Check its capabilities and at the same time test your skills:

- test your skills by programming your badge card to play tanks against a computer or even against another card;
- exhibit ingenuity when playing Sokoban with your badge card;
- solve several interesting tasks right on the badge card!

More information about badge card is available at offzone.moscow/badge

Secret shop

Our souvenir shop owner knows a lot about post-apocalyptic trade. At his shop you can exchange your OFFCOINS for goods with the OFFZONE logo (word has it, that he's also got a weakness for Rubles).

Pedal Powered Race Track

An interactive competition on exercise bikes powering track cars. Participants pedal stationary bikes, thereby advancing their track cars towards the finish line. Whoever pedals the fastest, gets to finish first and earn OFFCOIN points!

Foosball "Zombies vs Survivors"

The post-apocalyptic kicker raises not only your adrenaline, but also OFFCOIN points on your badge card. Are you for zombies or on the side of survivors? Come practice snake shots and pin shots – it's not only the Red Team that can run a surprise attack.

Game “CTF Bookies”

Test your intuition: try to guess which of the participants of the final CTFZONE competition will get more points in a certain time interval. Find an administrator in the area dubbed BI.ZONE and place a bet. He will transfer part of the OFFCOIN points from your badge card to a telegram bot where you can choose your favorite team.

Lady luck played in your favor? The same administrator will transfer the winnings from the telegram bot back to your badge card.

You can find more details about the game at the BI.ZONE corner.

TATTOO.ZONE

The most artsy place to earn yourself some OFFCOIN. (Or you could just get a tattoo)
The Conference goers get to:

Tatter up a bison skin.
Tattoo is art, which takes years to master. But here you can try it out having zero artistic skill or vision. A beginner tattoo master will have a large bison-skin canvas, a tattoo gun with ink and needles, and some unique transferable stickers, which is a good outline of your first tattoo. We are going to nominate the best beginner tattoo artist every hour and award them OFFCOINS.

Spin the wheel of fortune and try your luck to win a tattoo, a set of stickers, OFFCOIN points, or maybe even another go at the wheel.

Take part in For Luck’s Sake — the ballsiest quiz to take to earn some OFFCOIN: requires drinking and aiming. By aiming we mean shooting at a wall presenting some tattoo designs – the one you pick off with thy pistol shall be your destiny to have engraved on thy body. But first, the participant must answer 3 questions related to various aspects of cybersecurity. Answer all correct and you shall be invited to come closer for aiming; answer any wrong and you will have to shoot from a farther point. The one brave enough to go all the way with the tat gets a stack of OFFCOINS.

Get a professional tattoo. It’s not all about gaming, is it? Get the details from the event organizers. And we promise a tonne of OFFCOINS for showing such commitment.

Organizer

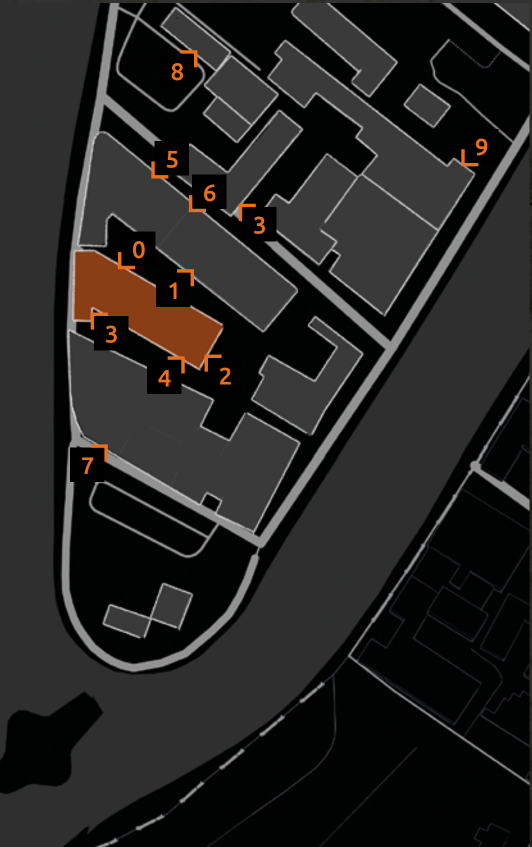
BI.ZONE
Cybersecurity

Media Partners

Partners

Community Affiliates

CAFES AND RESTAURANTS



0 **Progress bar,** European cuisine, 500—900 ₽
Bersenevskaya Naberezhnaya, 6, bldg. 3

1 **Syrovarnya,** Italian, Russian cuisine, 1500—2000 ₽
Bersenevskiy Pereulok, 2 bldg. 1

2 **Coffee 1316,** Cafeteria, 300—800 ₽
Bersenevskaya Naberezhnaya, 6, bldg. 3

3 **Urozhay,** Bar/Restaurant, 500-1500 ₽
Bersenevskaya Naberezhnaya, 6, bldg. 3

4 **Pita Gyros,** Greek cuisine/Fast food, 300—800 ₽
Bersenevskaya Naberezhnaya, 6, bldg. 4

5 **Dablbi,** Cafeteria, 500—1000 ₽
Bersenevskaya Naberezhnaya, 8/1

6 **Silver Panda,** Chinese, Asian cuisine, 300-500 ₽
Bersenevskaya Pereulok, 2 bldg. 1

7 **Bruce Lee,** Chinese cuisine, 700—1500 ₽
Bolotnaya Naberezhnaya, 3/2, bldg.4

8 **Magadan,** Fish and seafood, 1500—3000 ₽
Bersenevskiy Pereulok, 3/10 bldg. 8

9 **Shakti terrace,** Panasian cuisne, 1000—2000 ₽
Bolotnaya Naberezhnaya, 11, bldg. 1