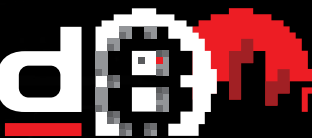


phd  
Positive  
Hack  
Days



**DIGITAL BET**

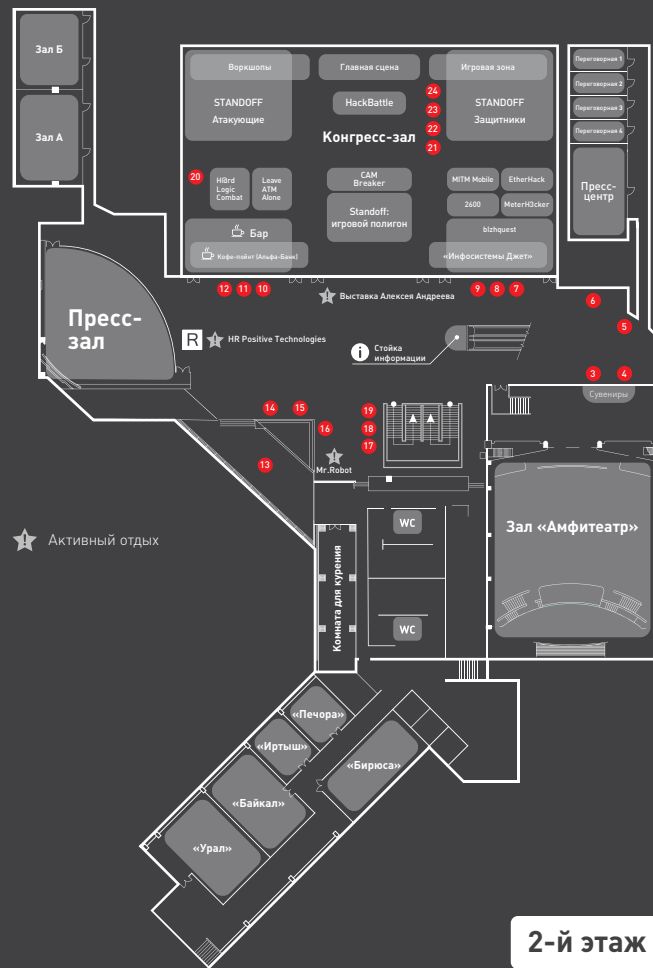
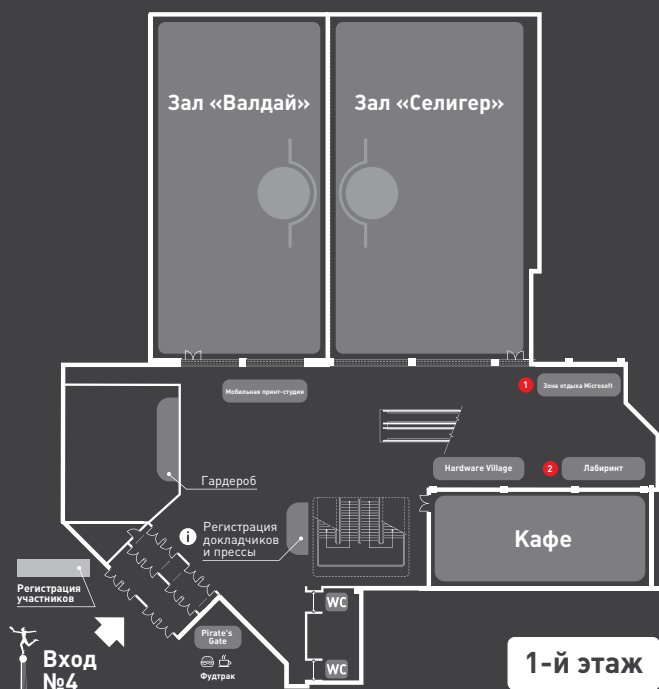
15 - 16 MAR 2018



**ПРОГРАММА ФОРУМА**


[phdays.com](http://phdays.com)


Международный форум по практической информационной безопасности



- |                |                      |                   |                              |                    |                               |
|----------------|----------------------|-------------------|------------------------------|--------------------|-------------------------------|
| 1 Microsoft    | 5 «Ростелеком»       | 9 Сбербанк        | 13 MONT                      | 17 Softline        | 21 Сервионика и Софтпрпм      |
| 2 «Ростелеком» | 6 R-Vision           | 10 Solar Security | 14 ICL                       | 18 Phoenix Contact | 22 «Перспективный мониторинг» |
| 3 Axoft        | 7 MOXA               | 11 Group-IB       | 15 ARinteg                   | 19 Orator Labs     | 23 «АСП Лабс»                 |
| 4 IBM          | 8 «Ангара» и «Гарда» | 12 Advantech      | 16 «Лаборатория Касперского» | 20 «Физприбор»     | 24 «Информзащита»             |


# 15 мая

 Технический доклад

 Бизнес-доклад

 Секция

 Hands-on lab

 Fast track Young School

 Development

Зал «Амфитеатр»		Зал «Валдай»	Пресс-зал	Зал «Селигер»	Воркшопы		Зал А	Зал Б	Зал «Урал»
10:00	RE: search	Новая версия thar: хешируйте на здоровье без Google <b>Леонид Юрьев</b> Создай свой cloud shell <b>Герман Наместников</b> Судебная экспертиза в ИБ <b>Евгений Царев</b> Shodan для SOC <b>Андрей Дугин</b>	Diameter-уязвимости в межоператорских сетях 4G и LTE <b>Сергей Машуков</b>	Подставь свой девайс под интернет <b>Ноам Ратхаус</b>	10:00	Все в порядке: век информационной безопасности окончен <b>Елле Нимантсфердрит</b>	Рокет-джамп от практической безопасности к соответствию формальным требованиям <b>Дмитрий Десятков и Юлия Омеляненко</b>		10:40 Открытие PDUG
11:00		Автоматизируй, если сможешь: как не сойти с ума, внедряя инструментальные контроли в процессы SDLC <b>Кирилл Самосадный и Андрей Петухов</b>	Как сделать мобильник из SDR <b>Вадим Яницкий и Петр Крысик</b>	Не опубликованный Shadow Brokers имплант DarkPulsar <b>Андрей Долгушев и Алексей Шулмин</b>	11:00		Как обойти IDS с netcat и Linux <b>Кирилл Шипулин</b>		Можно ли обобщить анализатор исходных кодов? <b>Иван Кочуркин</b>
11:30	Шесть разгневанных заказчиков, или Чего не хватает российской индустрии ИБ <b>Борис Сисим и Максим Филиппов</b>				11:30				
12:00		Личная жизнь на рабочем месте <b>Михаил Емельяников</b>	Нейрохирургия для промышленных роутеров. Защищенность Sarian OS <b>Данила Парнищев</b>	Внутренний язык декомпилятора Hex-Rays: микродод Ильфак <b>Гильфанов</b>	12:00			Каша из топора для защитника: как защититься тем, что есть под рукой <b>Андрей Иванов, Microsoft</b>	Мифы и легенды безопасной разработки <b>Юрий Шабалин</b>
13:00	Директор по ИБ в ближайшем будущем: возможности и риски <b>Эдди Шварц</b>		Своими руками: корпоративная безопасность «на коленках» <b>Данил Бородавкин</b>	Процессорные модули IDA Pro: есть новизнок Nios II <b>Антон Дорфман</b>	13:00		Threat intelligence и incident response на автомате <b>Игорь Сметанев и Андрей Чететкин, R-Vision</b>		Защищенность целочисленных типов в C++ <b>Игорь Собинов</b>
13:30		Безопасность КИИ: практические аспекты <b>Муслим Междлумов, «Ростелеком»</b>			13:30				
14:00	Управление рисками в ИБ: тема на хайпе или необходимый инструмент управления? <b>Сергей Денидов, Роман Чаплыгин, Дмитрий Гадарь, Андрей Погодин</b>		В чем был неправ ЭНЦШТЭЙ? <b>Сергей Гордейчик</b>	Безопасность и телеком: стало лучше или хуже? <b>Дмитрий Курбатов</b>	14:00	Настраиваем SELinux <b>Иван Агарков</b>		Общедоступное и неочевидное: Практика OSINT: методы и кейсы <b>Максим Авдюнин, «Перспективный мониторинг»</b>	Обнаружение уязвимостей в теории и на практике, или Почему не бывает идеального статического анализатора <b>Ярослав Александров, Александр Чернов, Екатерина Трошина</b>
14:30					14:30				
15:00			Обмани меня: анализируем скрытые каналы управления вредоносным ПО <b>Денис Колегов</b>	Что происходило с IoT-хапипотом за полтора года <b>Тан Ким Чан</b>	15:00				Идеальный статический анализ <b>Владимир Кочетков</b>
15:30	Безопасность применения биометрических технологий <b>Денис Горчаков</b>		Дырявые облака M2M: как ломают IoT <b>Андрей Бирюков</b> HomeNack: хакеры следят за вами через бытовую технику LG <b>Роман Заикин</b> Прокачай свой рекон: как заработать на кроссовки там, где уже побывали 700 байхантеров <b>Игорь Лырчиков</b> Особенности проведения аудита безопасности корпоративной IT-инфраструктуры <b>Иван Пискунов</b>	Взлом аутентификации по-крупному <b>Науэль Грисолия</b>	15:30				
16:00		Нужно ли защищать блокчейн?			16:00			Технология sandbox: вопросы к производителям anti-APT <b>Никита Дуров, Check Point</b>	Круглый стол: SAST и его место в SDLC Positive Technologies, SolidLab, Mail.ru, Solar Security, PVS-Studio, ИСП РАН
16:30			Развитие информационной безопасности в странах СНГ <b>Арман Абдрасилев, ЦАРКА</b>		16:30				
17:00				УМНЫЕ ЖИВУТ ДОЛЬШЕ. Технологии разума в современном кибероружии <b>Андрей Масалович</b>	17:00				
17:30		Безопасность блокчейна, уязвимости технологии и инструменты аудитора смарт-контрактов <b>Марат Рахимов</b>			17:30				

# 16 мая



Технический доклад



Бизнес-доклад



Секция



Hands-on lab



Fast track Young School



Development

Зал «Амфитеатр»		Зал «Валдай»		Пресс-зал		Зал «Селигер»		Воркшопы		Зал А		Зал Б		Зал «Урал»	
10:00	Цифровизация – угроза или шанс? <b>Дмитрий Фиогинов</b>	Системы безопасности на службе зла <b>Сергей Голованов</b>	Составление списков атакующих IP-адресов с помощью метода довушек <b>Евгений Сагатов</b> IoT: чем грозит и как защитить <b>Андрей Дугин</b> Переход на строгую CSP <b>Вадим Горбачев</b> Вирусы в Казахстане – насколько они опасны? <b>Олег Биль</b>	Шпион-лазутчик дома, или Как испугать кошку через UDP <b>Леонид Кролле и Георгий Зайцев</b>	10:00	Threat hunting своими руками на базе open source <b>Теймур Хейрхабаров</b>		Практика использования динамической бинарной инструментации в Malware-анализе <b>Артур Пакулов, HackerU</b>							
11:00		Как пережить небезопасность мобильных приложений <b>Густаво Сорондо</b>	Все что вы хотели узнать про нормативную базу, КИИ, но боялись спросить <b>Дмитрий Кузнецов</b>	Большие данные в advanced security analytics <b>Игорь Котенко</b>	11:00		Тестирование исходного кода. Подход SAP <b>Владислав Климов, SAP</b>		LibProtection: 6 месяцев спустя <b>Владимир Кочетков</b>						
11:30	Антипленарка <b>Алексей Качалин</b>				11:30										
12:00		Как мы шли к безопасному IPv6 <b>Фернандо Гонт</b>	Криптографические алгоритмы для усиления стойкости блокчейна <b>Сергей Кренделев</b>	Безопасное использование облаков: по каким правилам играем? <b>Лев Шумский (независимый эксперт) и Андрей Акинин (Web Control)</b>	12:00	Threat intelligence и incident response на автомате <b>Игорь Сметанев и Андрей Четочкин, R-Vision</b>	Новые тенденции в области ИБ. Как решают вопросы ИБ серьезные ребята <b>Григорий Галкин, MONT</b>	Основы безопасности алгоритмов консенсуса в блокчейне <b>Евангелос Дейрмендзоглу</b>							
13:00	Атрибуция кода целенаправленных атак <b>Костин Райю</b>	Как IP spoofing уничтожает интернет <b>Евгений Богомазов и Павел Брагин</b>	Анализируем FinSpy <b>Сергей Тарасов и Никита Прошин</b>	13:00	Повесть о взломе <b>Владан Николич, X-Force Red IBM</b>		Уязвимости и атаки на смарт-контракты <b>Арсений Реутов</b>								
14:00	Безопасность кредитно-финансовых организаций <b>Алексей Качалин, Сбербанк</b>	Базы уязвимостей: извода тысячи тонн словесной руды <b>Александр Леонов</b> А это чей сервис? Управление уязвимостями в крупной инфраструктуре <b>Михаил Парфенов</b> Объединяем сканеры под одной крышей <b>Михаил Аксенов</b> Можно ли обеспечить адекватный мониторинг без SIEM <b>Эмиль Алтынбаев</b> Атаки на технологии ML/AI и с их использованием <b>Алексей Сизов и Евгений Колесников</b>	Industry 4.0: Безоружный поход в будущее? <b>Роман Краснов, Positive Technologies</b>	Умный автомобиль как оружие <b>Штефан Танасе и Габриэл Чирлиг</b>	14:00	Как поймать зловред в сетевую воронку <b>Красимир Цветанов</b>	Новые технологии информационной безопасности <b>Дмитрий Пудов, Angara Technologies Group</b>	Защита привилегий – фундамент интегрированной платформы безопасности <b>Андрей Акинин, Web Control</b>	Подводные камни параметризации и объектного подхода <b>Владимир Кочетков</b>						
15:00					15:00					Биометрическая аутентификация: обход корпоративной системы распознавания лиц <b>Маттиас Дег</b>	Method Hooking в Android <b>Александр Гузенко</b>				
15:30	Что нужно сделать, чтобы SOC наконец-то заработал?! <b>Владимир Бенгин</b>	Искусственная безопасность: сколько и какого интеллекта нужно, чтобы строить защиту?	Программа bug bounty и как ее запустить <b>Игорь Булатенко</b>	15:30											
16:00									Безопасность аппаратных кошельков <b>Сергей Волокитин</b>	16:00	Криминалистика против изворотливых хакеров <b>Грег Творек, CQURE</b>	Продай CISO-технологию за 7 минут	Как создать быстрый WAF. Построение высокопроизводительной системы анализа сетевого трафика <b>Михаил Бадин</b>		
16:30									Уязвимости в телефонных банках: раскрытие личных данных и кража денег со счетов <b>Александр Колчанов</b>	16:30					
17:00									Явно о неясном, или Чем еще опасны интерфейсы управления серверами <b>Алексей Морозов</b>	17:00					

