ICC International Cybersecurity Congress | СБЕРБАНК

ICC 2019

Международный конгресс по кибербезопасности

icc.moscow

ICC International Cybersecurity Congress | СБЕРБАНК

Making
the digital world
a safer place

Дмитрий Медведев

Председатель Правительства
Российской Федерации

Международный конгресс по кибербезопасности уже второй год собирает представителей государственных структур, международных организаций, бизнеса, экспертов по безопасности со всего мира. Несколько лет назад мы начали готовиться к наступлению цифровой эры и не заметили, что уже вовсю в ней живем. Цифровые сервисы поменяли государственные услуги, образовательные и медицинские возможности. В России один из самых высоких показателей проникновения интернета, мобильной связи и развития электронных услуг, а стоимость доступа в Сеть одна из самых низких в мире. Рост экономики Рунета составляет до 15% в год.

Однако цифровизация, бурный рост технологий, инновационные достижения, как известно, создают риски и угрозы. По оценкам аналитиков, потери мировой экономики от кибератак в 2019 году могут увеличиться до 2,5 триллиона долларов. Одними государственными усилиями проблему киберугроз не решить — к этому процессу должны подключиться все, в том числе представители бизнеса. Сегодняшний открытый диалог показывает, что вместе мы действительно сможем продвинуться вперед в борьбе с киберпреступностью и киберугрозами. Уверен, что это мероприятие станет еще одним шагом в наше безопасное цифровое будущее.

Герман Греф

Президент, председатель правления,
Сбербанк

В эпоху глобальной цифровой трансформации защита всех элементов современных систем становится вопросом критической важности. Для ее обеспечения необходимы не только мощные внутренние компетенции, но и эффективная международная кооперация. В рамках такого сотрудничества открытость, готовность делиться информацией о потенциальных угрозах и случаях успешных атак помогают делать правильные выводы и работать превентивно. Именно это и является одной из главных идей Конгресса — не поиск самостоятельного решения проблемы, а расширение глобальной коалиции против киберпреступников.

Станислав Кузнецов

Заместитель председателя правления,
Сбербанк

На Второй Международный конгресс по кибербезопасности прибыло свыше 2500 делегатов из 65 стран. Нам предстоят два дня увлекательной работы (более 60 сессий, семинаров, докладов), в ходе которых каждый участник получит уникальную возможность поделиться опытом, обменяться мнениями, наладить деловые связи и сотрудничество. Главным лозунгом форума должны стать слова, связанные с доверием, взаимодействием и улучшением коммуникаций.

Содержание

Ключевые выводы

Развитие международной коллаборации

Киберпространство не имеет границ, поэтому эффективная защита невозможна без международного, межотраслевого сотрудничества и основанной на доверии коллаборации. Особенно важную роль в этом играет государственно-частное партнерство.

Обмен информацией об угрозах

Атаки становятся все более продвинутыми и сложными для определения. Киберпреступники могут месяцами находиться в IT-инфраструктуре компании и оставаться незамеченными. Такие атаки наносят колоссальный ущерб — особенно когда речь идет об объектах критической инфраструктуры. Необходимо модернизировать устаревшие системы, внедрять новые методы защиты и активно обмениваться информацией об угрозах с другими организациями.

Повышение киберграмотности пользователей

Государство должно защищать права граждан в киберпространстве, повышать уровень цифровой гигиены населения: успех многих кибератак напрямую связан с неподготовленностью пользователей.

Развитие правовой экосистемы

Чтобы повысить устойчивость к киберугрозам, необходимо разработать национальные и международные правила и стандарты по кибербезопасности.

Преодоление кадрового голода

В отрасли ощущается серьезный дефицит специалистов. Наращивание кадрового потенциала — одна из первостепенных задач общества в ближайшие годы.

Выход на уровень топ-менеджмента

Вопрос обеспечения кибербезопасности выходит за рамки ответственности технических специалистов. Стратегические решения по кибербезопасности должны перейти в ведение руководства компаний и организаций как интегральная часть риск-менеджмента и корпоративного управления.

Имплементация security by design

Развитие технологий происходит по устаревшей схеме: элементы безопасности воспринимаются как дополнение к системе, а не как ее составная часть. Глобальная информатизация и развитие цифровой экономики требуют перехода к модели security by design, когда защитные меры внедряются уже на этапе разработки.

Прогнозирование и предотвращение кибератак

Превентивные меры и возможность прогнозировать угрозы — следующий этап эволюции подходов к кибербезопасности. Чтобы надежно защищать цифровые активы, компании и государства должны вслед за профильной отраслью сделать предотвращение кибератак одним из своих основных приоритетов.

2729
участников

36
партнеров

65
стран

637
организаций

66
мероприятий деловой программы

102
спикера

Панельные дискуссии

Panel discussions

Открывающая пленарная сессия

Путь к глобальной киберустойчивости: только вместе?

The road to cyber resilience — a walk together?

Всемирная сеть — пространство, в котором уже сейчас живет более 4 миллиардов человек. Мы формируем там свою цифровую личность, совершаем действия, которые ранее были возможны только в реальном мире, храним и ежедневно передаем колоссальные объемы данных. Для новых поколений кибермир становится основным пространством для взаимодействия: он быстрее, полон информации и открывает бескрайние возможности для развития. При этом он очень хрупок — стратегии защиты реального мира складывались тысячелетиями, а здесь мы только начинаем их формировать. И у нас нет на это тысячелетий. Как защитить новый диджитал-мир от цифровых угроз? Это задача для каждого государства по отдельности или общий вызов для всего мира? Какой подход выбрать?

Модератор

Миша Гленни
Журналист-расследователь,
ведущий эксперт по киберпреступности

Спикеры

Константин Носков
Министр цифрового развития, связи и массовых коммуникаций Российской Федерации

Ханс-Вильгельм Дюнн
Президент, Совет по кибербезопасности (Германия)

Юрген Сторбек
Директор (1999–2004), Europol

Владислав Онищенко
Руководитель, Аналитический центр при Правительстве Российской Федерации

Омер Фатих Саян
Заместитель министра транспорта и инфраструктуры Турецкой Республики

98%

*должен составить уровень проникновения интернета в России к 2024 г.**

Будущее России и мира за цифровой экономикой и глобальной информатизацией.

В сфере кибербезопасности существует серьезный дефицит кадров, и общество понимает необходимость их подготовки.

Телекоммуникационная отрасль — глобальная индустрия, от которой зависит развитие интернет-пространства, поэтому обеспечение ее безопасности должно происходить в тесном сотрудничестве между бизнесом и правительствами.

Рост и усложнение киберугроз связаны с развитием технологий, поэтому кибербезопасность становится стратегически важным фактором благополучия государства.

Основные задачи в области глобальной кибербезопасности:

- *наращивание кадрового потенциала,*
- *развитие технологий и сотрудничества,*
- *обмен данными об угрозах,*
- *защита критической инфраструктуры,*
- *выработка международных стандартов и правил.*

~3 млн

*специалистов по кибербезопасности требуется сегодня мировому сообществу***

* Константин Носков.
** Ханс-Вильгельм Дюнн.

Панельная дискуссия

Стратегии кибербезопасности: национальная безопасность

Cybersecurity strategies: public services

Киберпреступность — одна из наиболее серьезных угроз нашего века. Решить эту проблему на уровне отдельных стран не получится: географически распределенные группировки порой располагаются на разных континентах и подпадают под юрисдикцию целого ряда государств. Разный уровень технологического развития, зрелости правовой базы в этой области и геополитическая турбулентность осложняют процесс взаимодействия и успешной борьбы с кибер-группировками. Можем ли мы изменить ситуацию? Или преступники так и будут на шаг впереди?

Модератор

Андрей Безруков

Президент, Ассоциация экспорта технологического суверенитета

Спикеры

Крейг Джонс

Директор по расследованию киберпреступлений, INTERPOL

Альберто Эрнандес Морено

CEO, Национальный институт кибербезопасности (Испания)

Леонид Левин

Председатель комитета Государственной думы Российской Федерации по информационной политике, информационным технологиям и связи

Михаил Гальперин

Уполномоченный Российской Федерации при Европейском суде по правам человека, заместитель министра юстиции Российской Федерации

Джулиан Воже

Заместитель руководителя политики и анализа, Munich Security Conference Foundation

62%

*государств не имеют стратегии по кибербезопасности**

Киберпреступность — серьезный вызов и большая проблема, решение которой предполагает развитие государственно-частного партнерства. Сотрудничать должны не только правительства, но и правоохранительные органы разных стран. Например, международным судам нужна помощь в формировании понятных, открытых стандартов оценки электронных доказательств и борьбе с их фальсификацией.

Руководители транснациональных технологических корпораций призывают государства и международные регуляторы активнее участвовать в управлении глобальным киберпространством. Необходимо как можно быстрее выработать международные правила и стандарты, создать единый профильный орган регулирования.

В последние годы злоумышленники все чаще атакуют не только корпорации и физических лиц, но и социально значимые объекты. Нужны превентивные меры, возможность на основе имеющегося опыта прогнозировать угрозы и создавать устойчивые механизмы информационного обмена.

Борьба с «интернет-офшорами» требует совместных усилий: преступники должны понимать, что, сменив домен, они не уйдут от ответственности, так как нарушают международные правила.

В 5 раз

*выросло число атак на государственные и частные активы в Испании с 2014 по 2018 г.**

* Альберто Эрнандес Морено.

Панельная дискуссия

Стратегии кибербезопасности: финансовая отрасль

Cybersecurity strategies: financial industry

Банки, платежные системы, кредитные учреждения, денежные средства — все это составляет кровеносную систему экономики, обеспечивающую жизнедеятельность мирового сообщества. Нарушение работы хотя бы одного звена влечет за собой сбой всей системы, поэтому безопасность финансовой отрасли является критически важным фактором. Учитывая глобальную цифровизацию, вопрос кибербезопасности и здесь выходит на первый план, а повышенное внимание со стороны мошенников значительно увеличивает риски потерь. Как правильно построить стратегию безопасности в финансовых организациях? Как совместно оградить отрасль от проблем и уменьшить риски клиентов? Можем ли мы предсказать будущие угрозы и уже сейчас начать выстраивать защиту?

Модератор

Станислав Кузнецов
Заместитель председателя правления, Сбербанк

Спикеры

Сунил Сешадри
Старший вице-президент и директор по информационной безопасности, Visa

Георгий Лунтовский
Президент, Ассоциация банков России

Михаил Алексеев
Председатель правления, ЮниКредит Банк

Даниэла Жижич
Директор по безопасности и защите данных, Eurobank

Традиционные стратегии по обеспечению кибербезопасности не защищают от целевых атак. Участникам финансового рынка необходимо разрабатывать новые методы защиты и сотрудничать с другими организациями — как с частными компаниями, так и с государственными структурами.

Один из ключевых трендов в кибербезопасности — ставка на предвидение угроз и предупреждение атак.

Защита клиентов — важнейшая задача для финансовых организаций. Она решается через повышение киберграмотности сотрудников, постоянный обмен информацией и опытом, использование нейронных сетей, увеличение расходов на безопасность.

Перед лицом общих угроз организациям банковской сферы нужно объединить усилия — в частности, оказывать помощь и поддержку менее крупным банкам, налаживать информационный обмен.

Коллаборация — ключевое слово в обеспечении кибербезопасности.

70%

*всех киберпреступлений совершается в финансовой сфере**

4 млрд

*кибератак зафиксировано в России за последний год**

2 трлн $

— *ущерб, который могут нанести кибератаки финансовому сектору**

Всего 7%

*IT-расходов приходится на кибербезопасность**

* Михаил Алексеев.

Панельная дискуссия

Стратегии кибербезопасности: критическая инфраструктура

Cybersecurity strategies: critical infrastructure

Сегодня кибератаки могут нанести гораздо более серьезный ущерб, чем физические действия, природные и техногенные катастрофы. Поэтому кибербезопасность критической инфраструктуры выходит на передний план: успешная атака на ее объекты может пошатнуть экономическую стабильность в стране и заметно ухудшить уровень жизни населения. Как защититься от подобных ситуаций? Что должно делать государство, а что — компании? И какую пользу может принести международное сотрудничество в этой области?

Модератор

Евгений Ковнир
Генеральный директор, АНО «Цифровая экономика»

Спикеры

Юсеф Аль Улян
Вице-президент по информационным технологиям, Saudi Aramco

Андрей Ивашко
Директор, Национальный координационный центр по компьютерным инцидентам

Игорь Ляпунов
Вице-президент по информационной безопасности, Ростелеком

Лотар Реннер
Управляющий директор по кибербезопасности в Европе, Африке и на Ближнем Востоке, Cisco

Игорь Милашевский
Генеральный директор, ГЛОНАСС

Обеспечивать безопасность критической инфраструктуры — значит как минимум иметь устойчивую к атакам систему управления инфраструктурой, создать в ней недоступную для внешнего воздействия доверенную среду и регулярно проводить мониторинг безопасности всего периметра.

Защита критической инфраструктуры имеет две ключевые особенности:

- ***Цель атак — доступ к управлению процессами** в организации (в том числе технологическими) и их контролю. Такая атака развивается медленно, злоумышленники на каждом этапе тщательно маскируются. Единственный способ обнаружить их — это проводить мониторинг информационных систем и выявлять аномалии, отклонения от нормы.*
- ***Защищаемые объекты имеют разное назначение:** это системы управления сетями связи, производством, энергетикой и т. д. Ключевая характеристика каждой из этих систем — надежность, но все они устроены по-разному, и это усложняет разработку и исполнение требований к их безопасности.*

Киберпространство трансгранично — эффективная защита невозможна без надежного сотрудничества, в ходе которого партнеры будут совместно обрабатывать данные, искать угрозы и устранять уязвимости. Все это обязательно нужно учитывать при формировании стратегии по модернизации производственного цикла критической инфраструктуры и созданию новых решений.

90%

*международных компаний готовы делиться данными о киберугрозах с вендором**

14%

— *доля атак на критическую инфраструктуру в общем количестве кибератак***

* Лотар Реннер.
** Игорь Ляпунов.

Панельная дискуссия

Стратегии кибербезопасности: прорывные технологии

Cybersecurity strategies: disruptive technologies

Киберпреступность, как и технологический прогресс, не стоит на месте. Мошенники ежедневно находят все новые уязвимости, оттачивают навыки взлома и социальной инженерии, разрабатывают вредоносное ПО для проникновения даже в самые защищенные системы. Все это создает критические риски для многих организаций и стимулирует к созданию новых методов защиты. Сможем ли мы догнать преступников и обеспечить глобальную киберзащиту?

Модератор

Сергей Плуготаренко
Директор, Российская ассоциация электронных коммуникаций

Спикеры

Даня Таккар
Вице-президент по Азиатско-Тихоокеанскому региону, Ближнему Востоку и Африке, Trend Micro

Дмитрий Самарцев
CEO, BI.ZONE

Лу Чу Кионг
Заместитель директора, Центр по инновациям, Университет Малайи

Александр Ханин
Генеральный директор, VisionLabs

Джорджи Ратц
Директор, IBM Security Systems в Европе

Успех в борьбе с киберпреступлениями во многом зависит от возможности быстро идентифицировать атаку. Поэтому нужны технологии, в том числе с использованием искусственного интеллекта, которые помогут быстро зафиксировать взлом и отреагировать на внедрение.

Пользователь — самое слабое звено в цепочке обеспечения киберзащиты организации и ее клиентов. В 2019 году более 80% атак на клиентов банков совершалось с помощью социальной инженерии. Если раньше преступники выбирали в качестве мишени в основном пожилых людей, то в 2019-м фокус атак сместился на 25–30-летних.

3 месяца

*уходит в среднем на обнаружение факта кибератаки**

23%

*всех атак в 2018 г. составили атаки на физических лиц***

Система образования не поспевает за развитием технологий и потому должна взаимодействовать с бизнесом, ведь именно корпорации аккумулируют передовые знания и опыт.

В области технологий кибербезопасности отчетливо просматриваются следующие тренды:

- *рост числа бизнес-задач, которые решаются с помощью искусственного интеллекта, в частности компьютерного зрения;*
- *стирание границ между онлайн- и офлайн-миром (digital ID);*
- *установка на frictionless — «максимальное количество услуг с минимальным количеством телодвижений».*

* Даня Таккар.
** Сергей Плуготаренко.

Панельная дискуссия

Стратегии кибербезопасности: телекоммуникации

Cybersecurity strategies: telecommunications

Телекоммуникационная отрасль неразрывно связана с развитием интернета. Обеспечив связью население планеты, операторы сделали возможным мгновенный контакт между людьми в разных частях света, открыли безграничные ресурсы Всемирной сети, где можно в считаные минуты найти практически любые данные. Постоянное развитие этой сферы позволяет действовать все быстрее, обеспечивает все больше возможностей — в том числе киберпреступникам. Способны ли мы защитить пользователей, не замедляя темпа эволюции технологий?

Модератор

Борис Глазков
Вице-президент по стратегическим инициативам, Ростелеком

Спикеры

Аллан Салим Кабанлонг
Глава департамента кибербезопасности и сопутствующих технологий, Министерство информационных технологий и коммуникаций Республики Филиппины

Жаклин Керно
Партнер в сфере кибербезопасности, Ernst & Young

Йогеш Малик
Технический директор, VEON

Валерий Шоржин
Член правления, вице-президент по цифровым бизнес-решениям, МТС

Модернизация телекоммуникационной отрасли — рост цифровизации, появление средств обработки больших данных, в том числе с использованием искусственного интеллекта, — меняет модель угроз. Если раньше целью злоумышленников была сама сеть, затем личные данные пользователей, то сейчас — цифровые активы.

Операторы связи сегодня одновременно работают с сетями 2G, 3G, 4G и 5G, что делает невозможной выработку единых требований по их безопасности и значительно усложняет процесс защиты каждого типа сети.

Грамотность пользователей зачастую оставляет желать лучшего, поэтому операторы регулярно рассылают уведомления с информацией о зараженных устройствах и вредоносных ссылках, блокируют опасные ресурсы.

500 млн

*переходов по вредоносным ссылкам блокируют телеком-операторы ежегодно**

50%

*пользователей следуют рекомендациям операторов связи и устанавливают антивирусы**

5G

— *стандарт мобильной связи, рассчитанный на широкое использование не только людьми, но и устройствами*

* Валерий Шоржин.

Панельная дискуссия

P2P-переводы: где безопасность?

P2P transfers — where is security?

Модератор

Артем Калашников
Начальник, ФинЦЕРТ

Спикеры

Виктория Никитина
Начальник отдела нормативного регулирования информационной безопасности,
Банк России

Артем Сударенко
Заместитель начальника,
ФинЦЕРТ

Анна Гольдштейн
Руководитель центра программных решений,
Национальная система платежных карт

Дмитрий Гадарь
Вице-президент — директор департамента информационной безопасности,
Тинькофф Банк

Сервис P2P-переводов — переводов денежных средств с карты на карту — при всех очевидных достоинствах имеет ряд узких мест:

- *в случае ошибочного перевода деньги у принимающей стороны могут быть списаны в любой момент;*
- *банк плательщика не знает получателя — ему сложно проверить легитимность принимающей стороны.*

Технические средства защиты информации — основной способ сохранить данные в целостности и неприкосновенности. Но в случае с сервисом моментальных платежей есть нюансы, связанные с необходимостью поддерживать непрерывность бизнеса. Имплементация средств защиты в технологию, критичную с точки зрения времени, — отдельная, очень непростая задача.

30 систем

P2P-платежей действует на данный момент, 20 — готовится к запуску

Самое важное и сложное во внедрении P2P-сервиса — унификация правил. Задача решается путем создания нормативной документации, которая устанавливает общие для всех участников рынка подходы к использованию средств защиты информации и работе с антифродом.

Панельная дискуссия

Применение технологий искусственного интеллекта в кибербезопасности

AI technologies in cybersecurity

Модератор

Александр Ведяхин
Первый заместитель председателя правления, Сбербанк

Спикеры

Лу Чу Кионг
Заместитель директора, Центр по инновациям, Университет Малайи

Игорь Ляпунов
Вице-президент по информационной безопасности, Ростелеком

Сергей Гаричев
Проректор по исследованиям и разработкам, МФТИ

Алексей Натекин
Основатель открытого сообщества исследователей данных России, Open Data Science

Эйден У
Генеральный директор, Huawei в России

Григорий Кабатянский
Профессор, советник ректора по науке, Сколковский институт науки и технологий

Михаил Мамонов
Заместитель министра цифрового развития, связи и массовых коммуникаций Российской Федерации

Человек не справляется с растущим объемом киберугроз — помочь может искусственный интеллект (ИИ).

Области применения ИИ в кибербезопасности — задачи, связанные с анализом поведения пользователей или систем и выявлением отклонений от заданного образца. Например, ИИ используется в системах фрод-мониторинга, позволяющих отслеживать и блокировать мошеннические транзакции на основе данных подобного анализа.

В руках злоумышленника ИИ может стать инструментом атаки. Достижение баланса между желанием делегировать ИИ полномочия и опасением повысить уязвимость систем — один из ключевых вызовов в сфере кибербезопасности.

Потенциал ИИ в области киберзащиты еще предстоит раскрыть: для эффективного машинного обучения необходимы релевантные образцы атак, но сегодня лишь немногие из них подходят для этой цели.

14 секунд

*проходит в среднем между кибератаками**

6%

— *ежемесячный рост атак с использованием социальной инженерии в 2019 г.**

1,5 трлн $

— *потери мировой экономики от киберпреступлений в 2018 г.**

* Александр Ведяхин.

Брифинг

Cyber Polygon: подведение итогов

Cyber Polygon — summarizing the results

Брифинг, посвященный подведению итогов онлайн-тренинга Cyber Polygon и обсуждению перспектив совместного противостояния киберугрозам.

Модератор

Бруно Халопо
Глава департамента киберустойчивости Центра кибербезопасности, Всемирный экономический форум

Спикеры

Станислав Кузнецов
Заместитель председателя правления, Сбербанк

Дмитрий Самарцев
CEO, BI.ZONE

Жанболат Надыров
Председатель правления, Трансtелеком

Аллан Салим Кабанлонг
Глава департамента кибербезопасности и сопутствующих технологий, Министерство информационных технологий и коммуникаций Республики Филиппины

Жаклин Керно
Партнер в сфере кибербезопасности, Ernst & Young

Крейг Джонс
Директор по расследованию киберпреступлений, INTERPOL

Александр Барышников
Директор по IT, Новый банк развития БРИКС

Cyber Polygon — онлайн-учения по международной кооперации бизнеса в борьбе с цифровыми угрозами. Цель учений — поиск новых и совершенствование старых способов выявления инцидентов кибербезопасности, оперативного реагирования и ликвидации последствий кибератак, а также оптимизация технических и организационных форм взаимодействия.

В ходе Cyber Polygon была проведена симуляция нескольких распространенных типов атак на тренировочные инфраструктуры глобальных компаний-участников, а наблюдатели следили за успехами защитников в онлайн-трансляции.

На тренинге отрабатывались сценарии массированной DDoS-атаки, веб-инъекций и фишинга. Вначале участники защищались поодиночке, а затем с помощью платформы обмена данными. После подключения к ней эффективность работы выросла в 7 раз.

Подобные учения демонстрируют эффективность международного государственно-частного сотрудничества, способствуют грамотному выстраиванию принципов такого взаимодействия и вовлечению в него все большего числа специалистов.

12 млн
*человек по всему миру смотрели трансляцию Cyber Polygon**

24 страны
— *география зрителей*

234
компании-наблюдателя

Участники

Blue Team

SBERBANK · MTS · New Development Bank · Transtelecom · DICT

Red Team

BI.ZONE Cybersecurity

В 7 раз
*выросла эффективность работы участников при использовании платформы обмена данными***

* Станислав Кузнецов.
** Дмитрий Самарцев.

Основная пленарная сессия

Безопасный цифровой мир — будущее или утопия?

Secure digital world — possible future or wishful utopia?

Вот уже несколько столетий ученые, писатели и политики фантазируют о будущем планеты. Задаваясь вопросом, что ждет нас в эпоху беспрецедентного расцвета технологий, в девятнадцатом веке говорили о подводных лодках и летательных аппаратах, в двадцатом — об антропоморфных роботах и колонизации далеких планет. Но мы, свидетели этого будущего, видим нечто большее — бескрайний мир цифровых возможностей, существующий параллельно миру реальному. Он возник несколько десятилетий назад и только начинает развиваться — именно нам предстоит решить, каким будет это развитие: транспарентным и безопасным или полным цифровых угроз.

Модератор

Ник Гоуинг

Ведущий BBC World News (1996–2014), основатель и директор Thinking the Unthinkable

Спикеры

Герман Греф

Президент, председатель правления, Сбербанк

Алоис Цвингги

Член правления, руководитель Центра кибербезопасности, Всемирный экономический форум

Кайрат Келимбетов

Управляющий, Международный финансовый центр «Астана»

Максим Акимов

Заместитель председателя Правительства Российской Федерации

Эльвира Набиуллина

Председатель, Центральный банк Российской Федерации

Дмитрий Медведев

Председатель Правительства Российской Федерации

Проблема киберпреступности входит в пятерку глобальных рисков в рейтинге ВЭФ. Международное экспертное сообщество зачастую ставит ее выше, чем даже терроризм и экологические проблемы. Все плюсы цифровизации будут нивелированы, если мы не примем эффективные меры по борьбе с киберпреступностью.

Необходимо выработать общемировые стандарты обеспечения безопасности. Первые шаги уже сделаны. В конце прошлого года Генассамблея ООН приняла российскую резолюцию о противодействии использованию информационно-коммуникационных технологий в преступных целях и создании рабочей группы по международной информационной безопасности. Мы готовы к сотрудничеству, готовы делиться своими знаниями, накопленным опытом и выступаем за равноправный, справедливый миропорядок в цифровой сфере.

4 млрд

*человек пользуются интернетом**

5 млрд

*человек пользуются мобильными телефонами**

* Герман Греф.

Кибербезопасность должна стать неотъемлемой частью риск-менеджмента и корпоративного управления. Учитывая масштаб угрозы, этот вопрос неизбежно выйдет за пределы ответственности технических специалистов — стратегические решения важно принимать на уровне руководства корпораций.

10 млн

*экземпляров вредоносного ПО появляется в интернете каждый месяц**

65%

респондентов, опрошенных в начале 2019 г., сказали, что подвергались кибератакам (два года назад таких было 40%)

Цифровая эра открывает необозримые перспективы и создает глобальные угрозы. Это должны понимать все, от глав государств и компаний до обычных граждан.

Чтобы обеспечить надежную защиту от киберугроз, помимо внедрения технических мер необходимо:

- *создавать трансграничные сети доверия;*
- *повышать уровень цифровой гигиены населения;*
- *провести тотальную деполитизацию цифровой повестки.*

* Герман Греф.

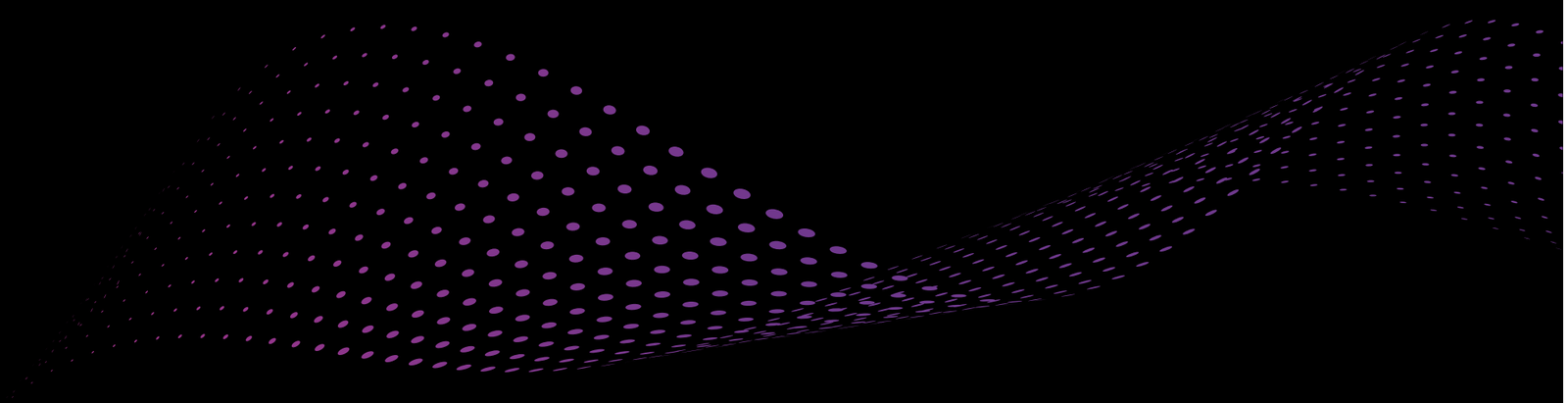
Тематические секции

Topical sessions

Правовые аспекты кибербезопасности

Legal environment

На секции обсуждались правовые аспекты кибербезопасности, а также вопросы международного сотрудничества в целях законодательного противодействия киберпреступности.



Томас Рид

Профессор, Институт новейших международных исследований, Университет Джонса Хопкинса

Атрибуция кибератак

Attributing cyberattacks

Атрибуция атак — фундамент кибербезопасности, от прочности которого зависит безопасность государства. Начиная с 2013 года ряд правительств и компаний добились значительных успехов в установлении источников компьютерных вторжений, создав прецеденты, которые имели конкретные правовые последствия, например, в страховой отрасли. Появляются новые нормы и практики — о последних тенденциях в атрибуции кибератак рассказал профессор Томас Рид.

Атрибуция кибератак состоит из двух аспектов: технической задачи и проблемы доказательства. Решение этих задач требует длительного сотрудничества с различными организациями и внимательного изучения всех сторон дела.

Самые сложные атаки — попытки взлома критической инфраструктуры. Для их атрибуции нужны знания и навыки, доступные очень небольшому числу специалистов. Однако именно благодаря им можно распознать действия злоумышленников и обнаружить утечку данных.

Качество атрибуции зависит от объема времени и ресурсов, потраченных на раскрытие инцидента, а также от того, насколько хорошо скрываются те, кто стоит за атакой. Очень важную роль также играет контекст кибератаки — иногда можно проследить корреляцию с какими-либо сторонними событиями, что может помочь в расследовании инцидента.

Грег Радд
CEO, CREST Australia & New Zealand

Правовое регулирование в безграничном и неуправляемом виртуальном мире: реально ли это?

Legislating a borderless, ungoverned virtual world — is it possible?

«Где международные законы по кибербезопасности?» Одни государства предлагают заключать договоры, обязательные на международном уровне, другие продвигают региональные конвенции; разные формы партнерства возникают между государством и бизнесом. Тем не менее уровень участия в международном правотворчестве по вопросам кибербезопасности остается низким. Похоже, мировое сообщество не получило толчок такой силы, чтобы сплотиться для противодействия реальной и крайне серьезной опасности кибер-конфликта. Чтобы прийти к соглашению по кибербезопасности, у нас остается все меньше времени.

Для борьбы с киберпреступностью нужны независимые от государств глобальные структуры, которые будут принимать и применять международные законы по кибербезопасности, в том числе устанавливать стандарты атрибуции атак и определять меры наказания для преступников.

37,5%

онлайн-трафика подверглось кибератакам в 2018 г.

В мире насчитывается:

> 5 млрд

пользователей мобильных телефонов

> 4 млрд

интернет-пользователей

> 3 млрд

пользователей соцсетей

Текущая ситуация в правовом поле осложняется тем, что не во всех странах хакерство считается преступлением. Различия в культуре, менталитете и стратегических приоритетах делают выработку международных норм еще более трудоемкой задачей. Однако именно создание таких законов станет следующим серьезным шагом на пути к победе над киберпреступностью.

Брюс Макконнелл
Исполнительный вице-президент,
Институт «Восток — Запад»

Можно ли привлечь к ответственности за незаконные действия в интернет-пространстве?

Can malicious actors be held accountable for illegal acts in cyberspace?

Предположим, что государства согласны с правилами использования кибероружия — например, не атаковать критически важную инфраструктуру в мирное время. Что происходит, когда государство нарушает одно из этих правил, — можно ли определить в этом случае ответственное лицо? Используемые и обсуждаемые правоприменительные методы включают дипломатические заявления и угрозы, экономические санкции, обвинительные заключения, публичные упреки, совместные расследования, отзыв дипломатов, а также военные и информационные контрмеры. Такие методы приносят незначительные результаты и к тому же оказывают дестабилизирующий эффект. Брюс Макконнелл описал один из возможных режимов контроля, который позволит повысить безопасность и упрочить стабильность в киберпространстве.

Для контроля норм поведения в цифровом пространстве и использования киберинструментов существуют такие организации, как Global Commission on the Stability of Cyberspace (GCSC). Миссия GCSC — поддерживать решения, направленные на обеспечение безопасности и стабильности в киберпространстве.

Увеличивая стоимость кибератак, компании делают их невыгодными для преступников. Добиться этого можно следующими способами:

- *сканировать клиентские устройства и требовать улучшения их безопасности;*
- *отправлять уведомления хостингам, которые используют киберпреступники;*
- *распространять доказательства атрибуции атак;*
- *блокировать трафик, идущий от атакующего.*

Однако подобные действия со стороны организаций могут привести к удорожанию их услуг и репутационным издержкам. Сотрудничество с государством в этих вопросах поможет минимизировать масштаб негативных последствий.

GCSC

Global Commission on the Stability of Cyberspace — международная организация по контролю за поведением в киберпространстве

Среди стран, представленных в GCSC, — Россия, США, Бразилия, Великобритания, Германия, Израиль, Индия, Китай, Малайзия, Нигерия, Нидерланды, Сингапур, Франция, Эстония, ЮАР, Япония

Рафаэль Маман
Партнер по кибербезопасности
и цифровым стратегиям, PwC

Обеспечение кибербезопасности критически важных объектов инфраструктуры

Ensuring cybersecurity of critical infrastructure

Рафаэль Маман проанализировал историю кибервойн, последние разработки в области безопасности критически важных объектов инфраструктуры, а также основные проблемы на пути к обеспечению надлежащего уровня их защиты — «известные неизвестные» безопасности операционных технологий.

Чтобы обеспечить безопасность критической инфраструктуры, необходимо на государственном уровне выстроить комплексную стратегию киберзащиты, определить национальные центры кибербезопасности (например, CERT), а также разработать методы и инструменты контроля за исполнением предложенных мер. На операционном уровне следует уделять больше внимания технологическому инструментарию: осуществлять мониторинг IT-инфраструктур организаций, внедрять технологии распознавания в сетях промышленного интернета вещей, создавать специальные лаборатории.

Одно из обязательных условий успешной защиты инфраструктуры — четкое законодательное регулирование. В Израиле проанализировали стандарты других стран, свели их воедино и на основе этого создали комплекс регулятивных норм. Данный процесс был долгим и непростым, но результат — успешным.

Также в Израиле создают лаборатории для тестирования и контроля промышленных систем, что позволяет всем игрокам: операторам критической инфраструктуры, научным сотрудникам, государству, провайдерам технологии — проводить испытания перед вводом системы в эксплуатацию.

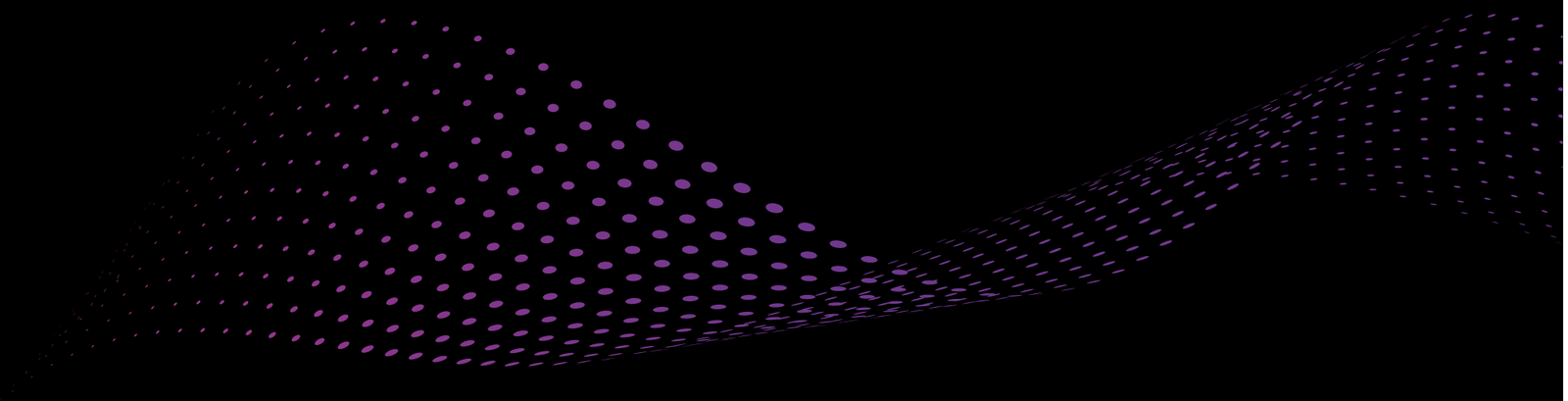
1982

— *год, когда, по мнению многих экспертов, была предпринята первая кибератака на критическую инфраструктуру*

Развитие киберпотенциала

Capacity building

На секции обсуждались вопросы повышения компетентности специалистов и наращивания глобального потенциала в области кибербезопасности, а также пути укрепления международного сотрудничества в данной сфере в целях усиления противодействия киберпреступности.



Гвидо Глушке
Директор Института безопасности,
Бранденбургский университет прикладных наук

Обучение кибербезопасности в сфере атомной и электроэнергетики

Cybersecurity education in the nuclear and energy sector

Гвидо Глушке рассказал об образовательных инициативах по кибербезопасности в сфере ядерной и электроэнергетики, о международных тренингах и других формах профессионального развития в этой области. Также в докладе затрагивался вопрос о вовлечении профильных преподавателей в энергетический сектор.

Одна из важнейших задач по обеспечению безопасности объектов атомной отрасли — это защита от цифровых угроз. Для подготовки специалистов в этой области МАГАТЭ в 2012 году открыло в Бранденбургском университете прикладных наук курс по обучению кибербезопасности.

Студенты курса изучают как управление ядерной и компьютерной безопасностью, так и международное право. Обучение дистанционное — таково условие МАГАТЭ, которое стремится охватить как можно больше стран.

Важный компонент образовательных программ по кибербезопасности — практические учения. Это масштабные мероприятия: подготовка к ним может длиться целый год. Первые учения проводились при участии НАТО.

При обсуждении вопросов кибербезопасности на международном уровне приходится преодолевать национальные и культурные различия. Наднациональные регуляторы нужны в том числе для того, чтобы ввести единую терминологию в сфере кибербезопасности и решить проблемы, связанные с отсутствием или различной интерпретацией нужных понятий в языках мира.

Ювал Еловичи
Директор Лаборатории телекоммуникационных инноваций, профессор факультета проектирования информационных систем, Университет имени Давида Бен-Гуриона

Построение глобальной киберэкосистемы: роль науки

Building a global cyber ecosystem: the role of the academia

Большинство экспертов считают, что для создания здоровой экосистемы кибербезопасности первостепенное значение имеет слаженное взаимодействие между бизнесом, наукой и военными, а также поддержка стартапов и наличие инвесторов. Ювал Еловичи подробно рассказал о вкладе науки в развитие таких экосистем, проиллюстрировав тезисы примерами из практики.

В Университете имени Бен-Гуриона особое внимание уделяется вопросам пересечения искусственного интеллекта и кибербезопасности — возможностям его использования в технологиях защиты и в изучении методов преступников. Пока в фокусе исследователей три направления:

- *защита от инцидентов (распознавание атак и несанкционированного доступа);*
- *проведение сложных операций по взлому и внедрению;*
- *модификация входных данных с целью обмана ИИ, защищающего систему.*

Израиль — один из лидеров в области внедрения инноваций, в том числе в кибербезопасности. Государство делает ставку на создание исследовательских центров, где наука сочетается с разработкой инновационных технологий, которые тут же проверяются на практике израильской полицией.

Денис Гамаюнов
Заведующий лабораторией интеллектуальных систем кибербезопасности, кафедра информационной безопасности факультета вычислительной математики и кибернетики, МГУ им. М. В. Ломоносова

Острова свободы: как университеты становятся точками роста киберпотенциала

Islands of freedom: how universities become growth points of cybersecurity capacity

Кибербезопасность предъявляет повышенные требования к технической эрудиции и глубине освоения различных областей прикладной математики и информационных технологий. В то же время эта сфера криминализирована, что значительно осложняет новичкам получение многих практических навыков. Опыт факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова и факультета компьютерных наук НИУ ВШЭ показывает, как сочетание академической свободы, науки, образования и бизнеса позволяет вертикально и горизонтально масштабировать кадровый потенциал в данной области.

Сегодня образовательный процесс ориентирован на скорейшее практическое овладение профессией. Если цель — научить разрабатывать защищенное ПО, студентов на практике учат искать и эксплуатировать уязвимости.

Необходимые знания и навыки приобретаются в университетах через собственно обучение, работу и игру. Студенты каждую неделю узнают что-то новое о кибербезопасности, а потом в игровой форме проверяют полученные знания: по выходным проводятся соревнования по этичному хакингу Capture The Flag (CTF).

В этом году стартует проект «Кибершкола МГУ»: талантливых старшеклассников будут собирать в команды, учить играть и мотивировать к дальнейшему обучению.

120

человек ежегодно записываются на курс по безопасности компьютерных систем, который читают в МГУ им. М. В. Ломоносова и НИУ ВШЭ

~100%

студентов после практического обучения идут работать в сферу кибербезопасности

В 6 раз

выросло число слушателей курса по безопасности в МГУ с 2010 г.

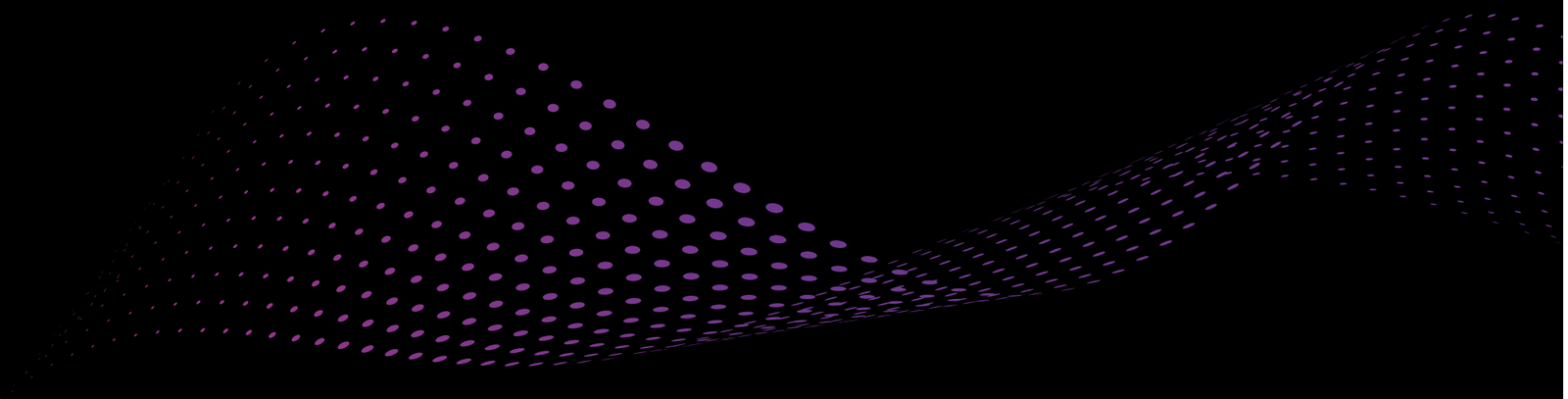
Security is fun

— *лозунг, стимулирующий студентов выбирать сферу кибербезопасности*

Изучая киберпреступников

Threat intelligence

На секции обсуждались актуальные цифровые угрозы и ключевые глобальные вызовы кибербезопасности, а также рекомендации по повышению общего уровня устойчивости к преступлениям в этой области.



Евгений Волошин
Директор блока экспертных сервисов,
BI.ZONE

Клиент не всегда прав

Customer is not always right

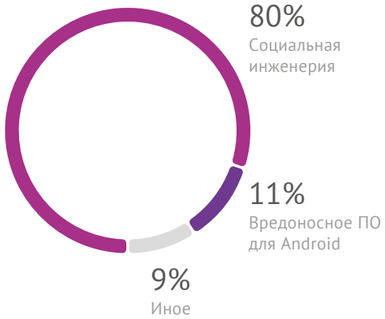
Евгений Волошин рассказал об эволюции кибератак, смещении фокуса злоумышленников со сложных технологических сценариев на социотехнические, а также о качественном изменении в подходах к социальной инженерии.

Реализация государственных и частных инициатив по обмену информацией об актуальных угрозах позволила в 10 раз уменьшить денежные потери банков.

В 2018 году число хищений из банкоматов сократилось на 40% — сегодня атаки проводятся в основном по цифровым каналам.

В 2019 году принципиально изменился вектор кибератак: если раньше они были нацелены на банки и коммерческие организации, то теперь на физических лиц. Злоумышленники делают ставку на приемы социальной инженерии: обзвоны, опросы, мошенничество в программах лояльности.

Атаки на банковских клиентов



7400

мобильных устройств в России еженедельно заражаются вредоносным ПО

76 млн ₽

было похищено из российских банков в 2018 г., что на порядок меньше, чем годом ранее

Руководство банков понимает, что защищаться нужно превентивно: анализировать сценарии атак, обмениваться индикаторами компрометации, телефонами и номерами карт злоумышленников — на региональном, федеральном и отраслевом уровнях.

78%

россиян пользуются банковскими услугами через мобильные приложения

ICC International Cybersecurity Congress | СБЕРБАНК

Дмитрий Волков
Технический директор и сооснователь,
Group-IB

Развитие целенаправленных атак на финансовый сектор

Evolution of targeted attacks on the financial sector

Доклад на основе расследования атак кибергруппировки Lazarus.

Основной метод хищения группировки Lazarus — специально разработанный троян, инструмент для сбора данных. Раньше троян занимался только разведкой: собирал данные, на основе которых принималось решение, атаковать данный компьютер или нет. Непосредственно для атаки запускалась другая программа. В июне 2017 года этот троян переписали на PowerShell, а в июле 2018-го — для macOS. В мае 2019 года появилась свежая версия трояна.

За последние полгода Lazarus обновила и значительно усовершенствовала инструментарий. Чтобы успешно отражать их, а также схожие атаки, необходимо:

- *защищать не только почтовый и веб-трафик, но и сотрудников, имеющих легитимный доступ в соцсети;*
- *обеспечить контроль целостности данных на компьютерах, так как Lazarus нередко уничтожает критически важные данные после успешной операции, запуская программы-шифровальщики;*
- *знать, что злоумышленники используют общедоступные средства вроде PowerShell Empire, MetaSploit, CobaltStrike и переписали на PowerShell все свои инструменты (а не только конкретный троян).*

Lazarus

— *одна из самых известных действующих киберпреступных группировок*

4 года

— *подтвержденный «стаж» преступной деятельности группировки Lazarus*

Тимур Биячуев
Руководитель управления исследования угроз,
«Лаборатория Касперского»

Тенденции развития продвинутых киберугроз

Advanced threat trends

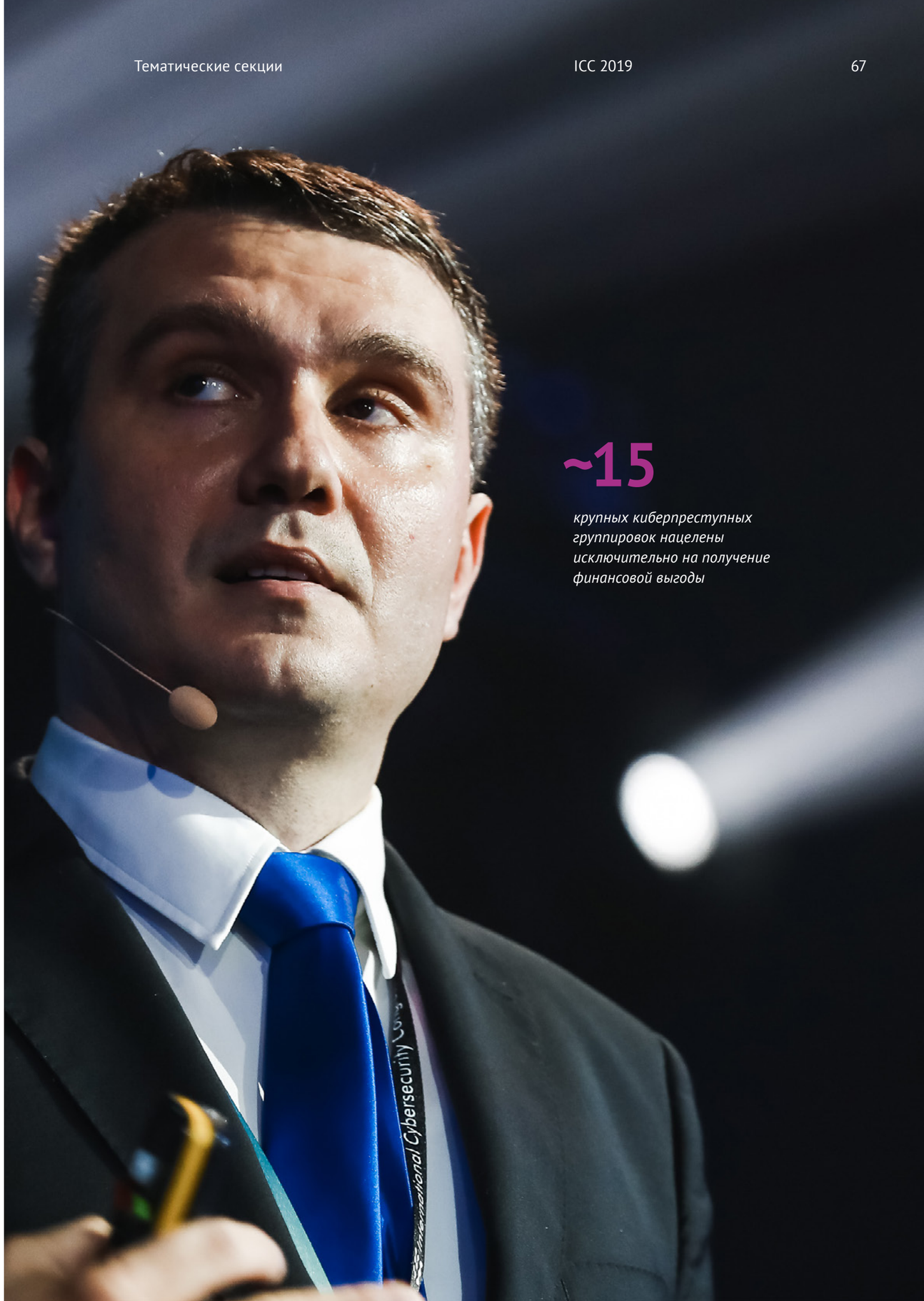
Чаще всего атакам подвергаются:

- *финансовая отрасль,*
- *телекоммуникации,*
- *промышленность (добывающая, ядерная, аэрокосмическая),*
- *медиа,*
- *правительство,*
- *военные,*
- *разведка.*

Ключевые тренды последних лет — атаки supply chain (атаки на цепочку поставок) и атаки на сетевое оборудование. Инциденты первого типа — серьезная проблема для крупных предприятий, использующих сотни наименований регулярно обновляемого специализированного софта, в который и внедряют вредоносные программы. Атаки второго типа опасны тем, что на сетевое оборудование нельзя поставить антивирусы и средства защиты, при этом обновить ПО на нем не так просто, как на обычных ПК.

Количество киберпреступных группировок неизменно растет, а их методы совершенствуются. В прошлом году были арестованы лидеры нескольких объединений. Однако, вместо того чтобы распасться, группы разбились на более мелкие и начали осваивать новые регионы и инструменты.

Для обеспечения безопасности нужны комплексные системы, в которых реализованы функции прогноза, предупреждения (в том числе отчеты Threat Intelligence), распознавания и быстрого реагирования на инциденты.



~15

крупных киберпреступных группировок нацелены исключительно на получение финансовой выгоды

Алексей Новиков
Директор экспертного центра безопасности,
Positive Technologies

Инцидент: как высоко подпрыгивать?

An incident. How to bounce high?

Общее число инцидентов неуклонно растет, как и их сложность. Однако с точки зрения расследования и реагирования все они делятся на три категории: интересные, среднестатистические и скучные. Перед какими инцидентами чаще всего пасует бизнес и почему? Бывают ли APT-атаки* скучными? Кто стоит за такими атаками и насколько сложно (дорого) их организовать? Как за последние год-полтора изменились атаки на организации различных секторов экономики? Можно ли противостоять атакам, которые мы считаем интересными? Стоит ли тратить время и ресурсы на противодействие примитивным и скучным? К чему стоит подготовиться уже сейчас?

Скучные инциденты возникают из-за базовых недостатков в инфраструктуре, протекают быстро, включают использование автоматического публичного инструментария. Часто игнорируются бизнесом.

Среднестатистические инциденты приводят к полной компрометации инфраструктуры, инструментарий обычно используется вручную. Бизнес чаще обращается в правоохранительные органы для расследования.

Интересные инциденты, по сути APT-атаки, всегда целевые, тщательно организованы и, как правило, успешны. Проведение таких атак предполагает получение полного и максимально длительного контроля над инфраструктурой.

Как противостоять злоумышленникам и APT-атакам?

- *Делиться информацией о действиях преступников и эффективных контрмерах.*
- *Хорошо знать инфраструктуру своей компании и способы ее защиты.*
- *Проводить полноценное расследование инцидентов, а не лечить симптомы.*
- *Точно классифицировать инциденты.*
- *Выстроить отвечающую современным вызовам систему кибербезопасности.*

* Advanced persistent threat — продолжительная атака повышенной сложности.

18%

скучных для расследования инцидентов

10%

среднестатистических инцидентов

72%

интересных инцидентов

43%

— *доля целевых атак в общем количестве инцидентов в I квартале 2019 г.*

Джонатан Фишбейн
Глава отдела технического маркетинга,
Check Point

Предсказать непредсказуемое: взгляд на киберугрозы-2019

Predicating the unpredictable: a look into 2019 cyberthreat landscape

Скорость происходящих в кибермире изменений практически не позволяет делать прогнозы. Способны ли мы действительно подготовиться к грядущим событиям? Не все, но многое можно узнать, если постоянно анализировать киберугрозы.

При анализе киберугроз обычно изучают мотивы, методы и объекты атак.

Большинство взломов совершается с целью хищения денежных средств, получения доступа к информации, нанесения ущерба и укрепления политического и коммерческого влияния. В 2019–2020 годах главным мотивом останутся деньги, также ожидается рост числа атак, цель которых — борьба за влияние.

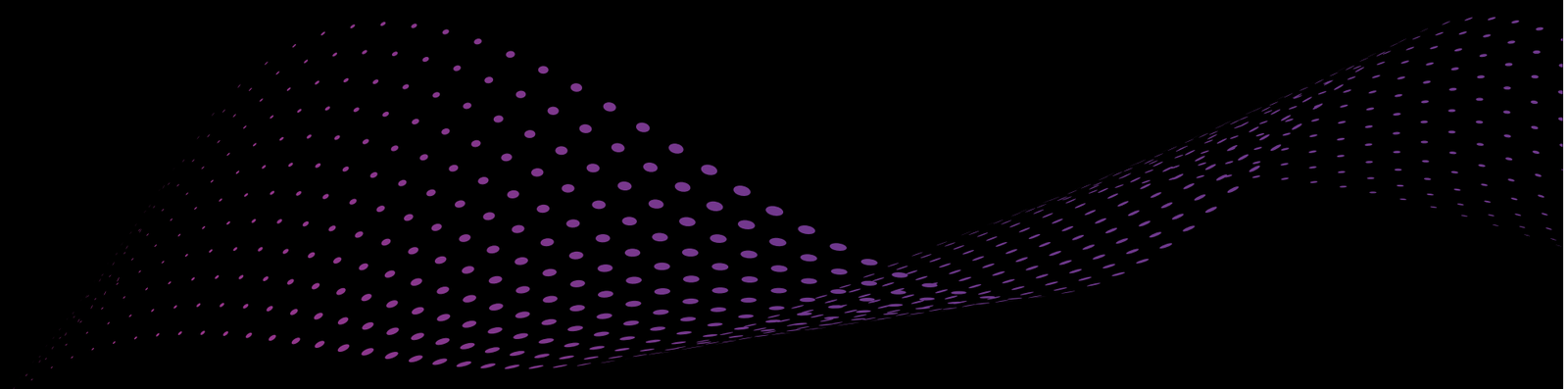
Основные методы злоумышленников включают распространение банковского вредоносного ПО и вирусов-вымогателей, а также криптоджекинг — использование устройства для генерации криптовалюты без ведома его владельца. В 2019 году эти тренды сохранятся, а количество нарушителей увеличится.

Объекты кибератак — это ПК, сети, приложения, мобильные устройства, облачные хранилища. В 2019 году основной точкой входа станут IoT-девайсы, участятся случаи кражи электронных кошельков, будут предприняты первые попытки манипуляции системами искусственного интеллекта.

Прорывные технологии

Disruptive technologies

На секции обсуждались перспективы развития инновационных технологий в сфере кибербезопасности и вопросы укрепления сотрудничества в деле противодействия киберугрозам.



Клеменс Даннхейм
CEO, Objective Software

Транспорт будущего и его влияние на кибербезопасность

Future vehicular mobility transition and its impacts on cybersecurity

С момента внедрения технологии автономного вождения вопросам кибербезопасности уделялось мало внимания. Однако проблемы в этой сфере могут нанести ущерб брендам или даже стать причиной гибели пассажиров, а следовательно, подорвать доверие общественности к будущим концепциям мобильности. Постепенно индустрия начинает внедрять улучшения, особенно после того, как хакеры в порядке демонстрации взломали подключенные автомобили на общественном телевидении. Руководство автоконцернов должно научиться признавать проблемы и учитывать риски безопасности, возникающие на пути к светлому будущему.

Компании-производители, ранее поставлявшие лишь механические части для транспортных средств, становятся разработчиками ПО — как для управляемых машин, так и для беспилотников.

В системах автономного вождения должны быть реализованы:

- *четкое геопозиционирование,*
- *детальное моделирование окружающей среды,*
- *прогнозирование и принятие решений по выбору траектории,*
- *связь с облачными хранилищами для получения необходимой информации,*
- *доступ к банковским услугам.*

MBUX (Mercedes-Benz User Experience)

— *комплекс с элементами искусственного интеллекта, обновлениями «по воздуху» и самообучением, разработанный концерном Daimler*

Беспилотные автомобили подключают к общей сети, позволяя обмениваться данными друг с другом. Возникают риски, а с ними — необходимость защитить каналы связи между машинами, обеспечить их кибербезопасность.

Сергей Лебедь
Директор департамента кибербезопасности,
Сбербанк

Кибербезопасность в условиях цифрового хаоса

Cybersecurity in digital chaos

Есть два подхода к организации безопасности: один основан на требованиях к системе безопасности, второй — на управлении рисками.

При внедрении технологий защиты часто не учитывают особенности бизнеса и IT-инфраструктуры, что приводит к неэффективной защите: средства есть, персонал есть, а безопасность остается на низком уровне. Чтобы избежать подобных ситуаций, необходим подход, при котором безопасность выстраивается с учетом особенностей организации и умело использует синергию технологий безопасности и IT.

Уровень зрелости кибербезопасности не может быть выше уровня IT-зрелости. Базовые IT-процессы — фундамент для эффективных систем управления как IT-инфраструктурой, так и кибербезопасностью.

Есть два ITSM-процесса, без которых порядок в IT-организациях невозможен в принципе: это управление активами (asset management) и управление изменениями (change management).

В современном мире киберугроз, где практически всегда выигрывает атакующий, все более востребованным становится подход к управлению кибербезопасностью, при котором на передний план выходит задача быстрого восстановления после атаки (cyber resilience).

3 млрд

киберинцидентов произошло в 2018 г.

2 млн

— *дефицит специалистов по кибербезопасности во всем мире*

66 дней

в среднем требуется на восстановление после атаки

8,5 тыс

стандартов (RFC) регулируют совместимость и взаимодействие в интернете

Антон Окошкин
Технический директор,
BI.ZONE

Кибербезопасность в эпоху мобильности: защищая себя, защищаем бизнес

Cybersecurity in the era of mobility: protect business by protecting ourselves

Мобильность — один из ключевых трендов современного мира: удаленная работа, постоянные перемещения, необходимость использовать различные устройства и постоянно их обновлять, а также многое-многое другое, что вызывает головную боль у сотрудников, ответственных за кибербезопасность. При этом мобилен не только и не столько сам человек, сколько его «цифровые личности», которые тоже нужно как-то защищать. Все это заставляет задуматься о комплексном подходе к киберзащищенности человека. Стандартные средства больше не работают — нужно что-то новое.

Цифровая и физическая реальности уже практически неразделимы. Это касается и безопасности: повсеместное внедрение IoT-устройств и цифровизация различных процессов значительно расширяют ландшафт потенциальных рисков. Телефоны, ноутбуки, профили в соцсетях, на почтовых серверах и форумах, наше окружение (офис, дом, аэропорты, отели, транспорт, рестораны) — количество угроз в столь сложной системе стремится к бесконечности.

Для защиты сотрудников нужно информировать их, повышать уровень осведомленности в вопросах кибербезопасности, анализировать данные о цифровых следах и окружении в привязке к активности на устройствах.

Киберриски, связанные с персоналом, — прямые риски компании. Их нужно измерять и принимать во внимание, оценивая уровень защищенности.

4 секунды

проходит между появлением новых экземпляров вредоносного ПО

7 $

стоит в даркнете скрыть вредоносное ПО от большинства известных антивирусов

563 млн

пользовательских аккаунтов было скомпрометировано в результате всего лишь 3 утечек в 2018 г.

Иван Новиков
CEO, Wallarm

Машинное обучение по другую сторону баррикад информационной безопасности

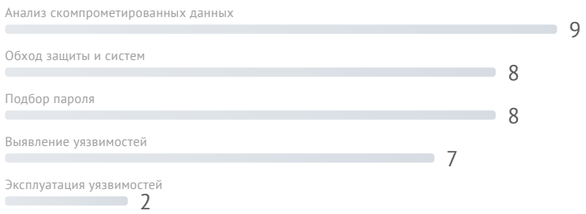
Machine learning on the other side of cybersecurity barricades

Машинное обучение широко применяется в технологиях противодействия кибератакам. Но что, если злоумышленники тоже начнут использовать его? Иван Новиков приводит примеры атак с использованием машинного обучения, а также техник обнаружения новых уязвимостей на их основе.

Технологии машинного обучения — одно из направлений искусственного интеллекта — могут быть использованы как для обеспечения кибербезопасности, так и для взлома.

С одной стороны, машинное обучение помогает выявлять атаки, аномалии, уязвимости, а также анализировать и приоритизировать риски. С другой — оно может быть использовано для обхода защиты, выявления и эксплуатации уязвимостей, подбора паролей, приоритизации и классификации скомпрометированных данных.

Текущее состояние машинного обучения для кибератак (по балльной шкале реализуемости)



9–10 баллов — готовые к производству инструменты для общей практики и специальных задач, наибольшее количество доказанных результатов.
7–8 баллов — существуют инструменты для общей практики, есть практические результаты.
5–6 баллов — инструменты пока неприменимы в общей практике, есть практические результаты.
3–4 балла — менее 5 исследований по теме.
0–2 балла — менее 2 исследований по теме.

Когнитивная наука

— *междисциплинарное направление, объединяющее философию, лингвистику, антропологию, нейробиологию, психологию и теорию искусственного интеллекта*

Кирилл Керценбаум
Директор по продажам,
Symantec Russia

Использование методов прогностического и статистического анализа для автоматизации процессов предиктивного реагирования на новые техники кибератак

The use of prognostic and statistical analysis methods for automating the processes of predictive response to new cyberattack techniques

Прогностические сценарии кибератак, будучи интегрированы с потоками журнальных данных, поступающих с разнообразных средств защиты и IT-инфраструктуры в целом, позволяют эффективно моделировать вектора атак и поведение злоумышленника. Это дает возможность автоматизировать процесс реагирования на инциденты в предиктивном режиме.

Модель адаптивной безопасности архитектуры включает 4 обязательных компонента:*

- *прогнозирование атаки,*
- *предотвращение,*
- *обнаружение,*
- *реагирование.*

Одни компании делают ставку на предотвращение, другие — на обнаружение. Но только прогнозирование позволяет обеспечить высокий уровень безопасности, не увеличивая расходы на средства защиты — за счет оптимизации процессов и анализа имеющихся данных.

Чтобы построить систему прогнозирования, нужно изменить формат хранения и обработки данных. Решить эту задачу позволяет подход под названием «озеро данных» (data lake):

- *основная информация поступает с собственных средств защиты;*
- *механизмы статистического анализа обрабатывают собранные с помощью телеметрии события;*
- *система выдает статистическую модель медианного поведения пользователя, показывает количество и критичность отклонений от нормы, проводит регрессивный анализ.*

В итоге система при минимуме ложных срабатываний сама идентифицирует инцидент и принимает решение.

250

*различных техник используют киберпреступники для подготовки и проведения атаки***

70

из них (максимальная доля) разработаны для обхода средств защиты

14

(минимальная доля) приходятся на техники получения доступа

12 этапов атаки***

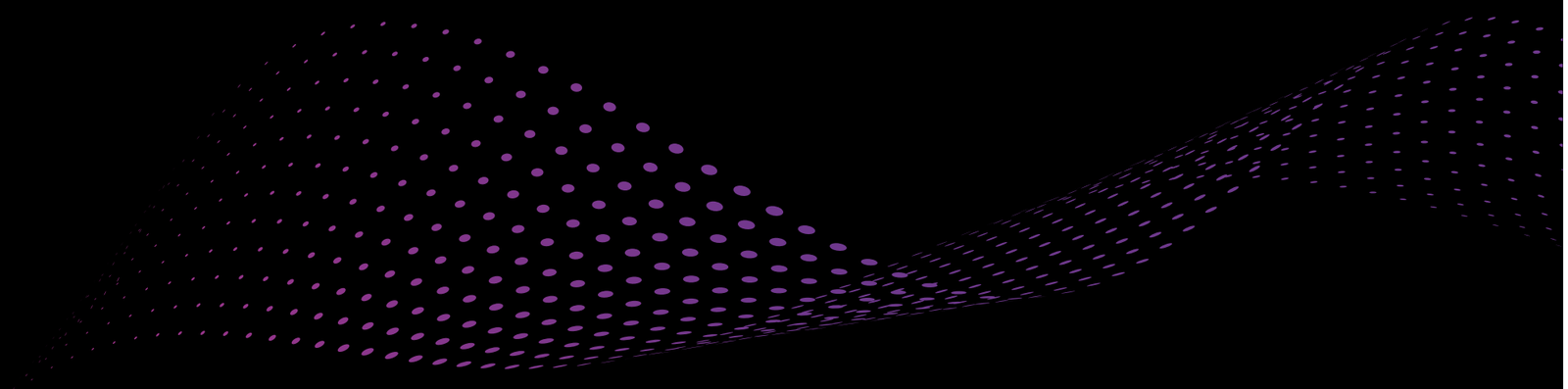
1. *Получение доступа*
2. *Внедрение*
3. *Закрепление*
4. *Эскалация привилегий*
5. *Обход средств защиты*
6. *Получение доступа (поиск учетных записей)*
7. *Обнаружение данных*
8. *Горизонтальное перемещение*
9. *Сбор данных*
10. *Похищение данных*
11. *Установка контроля над зараженной инфраструктурой*
12. *Воздействие*

* Разработана компанией Gartner.
** Данные компании MITRE.
*** Классификация MITRE.

Инвестиции в кибербезопасность

Investments in cybersecurity

На секции обсуждались вопросы инвестирования в индустрию кибербезопасности, а также ключевые направления развития инноваций в данной сфере.



Бен Баннерджи
Член правления, InnMind

Инвестиции: риск, доходность и влияние

Investments — risk, return & impact

Почему мы инвестируем и советуем институциональным и частным учреждениям, а также правительствам вкладываться в кибербезопасность? Каковы в этом случае риски, отдача и влияние на общество, экономику и другие сферы жизни? Стоит ли вообще инвестировать в кибербезопасность?

Кибербезопасность — один из ключевых вопросов и основных вызовов цифровой эры. Как и во многих других областях, профилактика в вопросах защиты от киберугроз работает эффективнее, чем борьба с последствиями атаки. Но это требует больших инвестиций.

Наиболее активно в кибербезопасность вкладываются компании технического и финансового секторов, госструктуры. Причем банки и госорганизации жестко не ограничивают расходы, понимая масштаб опасности.

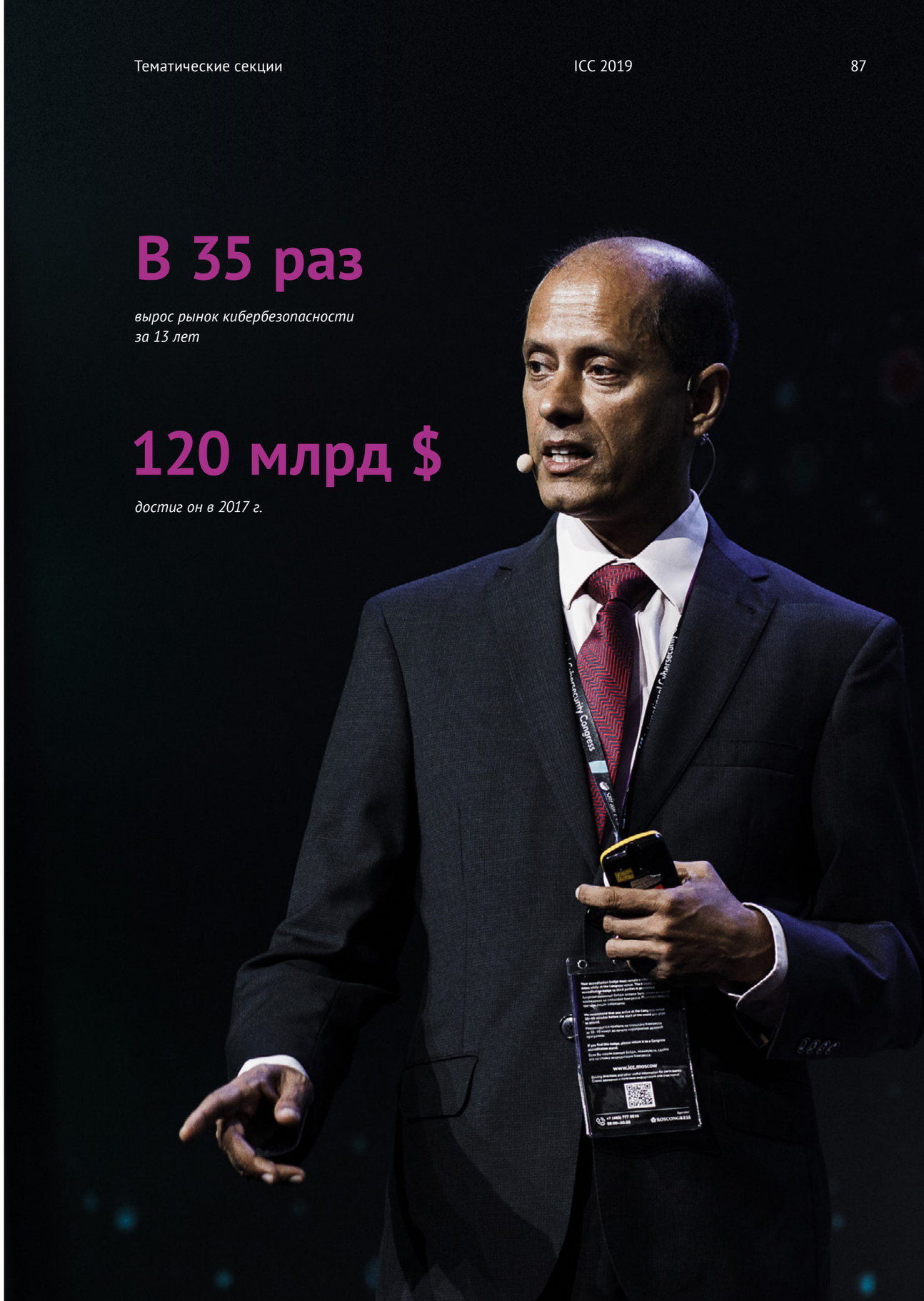
Инвестирование в кибербезопасность происходит практически так же, как и в любой другой сфере. Единственное, что здесь важно для инвесторов, — то, как воспринимает киберугрозы конечный пользователь. Если он не осознает риск и необходимость приобрести соответствующий продукт, то и не будет тратить на него деньги.

В 35 раз

вырос рынок кибербезопасности за 13 лет

120 млрд $

достиг он в 2017 г.



Василий Белов
Генеральный директор,
Skolkovo Ventures

Инвестиционные возможности в области кибербезопасности

Cybersecurity investment opportunities

Глобальный рынок инвестиций в кибербезопасность растет больше чем на 20% ежегодно. Один из активных участников этого рынка — инновационный центр «Сколково». Василий Белов рассказал об основных трендах и возможностях отрасли.

Инвестиции в кибербезопасность — один из наиболее быстрорастущих секторов венчурного рынка. Его драйверы — это технологии работы с большими данными (Big Data) и разработки в области искусственного интеллекта.

В первую очередь компании вкладываются в защиту облачных приложений и IT-инфраструктуры (промышленный интернет вещей, критическая инфраструктура).

Наряду с крупными игроками в этом сегменте есть и нестратегические покупатели, в основном банки. В 2018 году общий объем поглощений составил 23 млрд долларов.

На российском рынке тоже заключаются венчурные сделки, и они начинают привлекать внимание аналитиков.

Инвестировано в кибербезопасность в 2018 г.
6 млрд $

Прирост всего российского венчурного рынка
~0,4 млрд $

25%

— *средний рост инвестиций в кибербезопасность в 2018 г.*

Вадим Галеев
Заместитель генерального директора по развитию
и взаимодействию с резидентами, Иннополис

Иннополис — особая экономическая зона

Innopolis — special economic zone

Кибербезопасность — одно из ключевых направлений подготовки кадров Иннополиса. Специалистов по кибербезопасности выпускает Университет Иннополис, вопросами защиты от киберугроз занимаются многие резиденты.

Французская компания Schneider Electric известна как производитель электронных компонентов, но в Иннополисе она работает над цифровыми двойниками (цифровая копия объекта или процесса, созданная для сбора и повторного использования полученной информации о нем). Эта технология позволяет не только повысить эффективность реального объекта, но и улучшить его безопасность: механизмы защиты необходимо внедрять уже на стадии проектирования системы (security by design), и двойник помогает сделать это наиболее грамотно.

Японская Soramitsu разрабатывает собственный подвид блокчейн-протокола для систем передачи цифровых активов. Распределенный реестр — один из способов обеспечить безопасность по умолчанию (security by default — способ изначальной настройки системы, в котором приоритет отдается ее безопасности).

Российская UNITS специализируется на инновационных решениях, направленных на обеспечение безопасности данных в процессе их хранения и обмена, и тестирует свои разработки в США, Канаде и Восточной Европе.

2015
— *год основания Иннополиса*

80
компаний-резидентов

2000
рабочих мест

500
предоставляют партнеры

2 вакансии
на каждого специалиста

Олег Глебов
Директор по развитию международного бизнеса,
Центр речевых технологий

Биометрия в кибербезопасности: открывая возможности для инвестиций

Biometrics in cybersecurity as an investment opportunity

К 2022 году 70% крупных предприятий будут использовать биометрическую аутентификацию в проектах по управлению идентификацией и доступом (IAM).

Насколько безопасен этот метод, существуют ли риски компрометации биометрических данных и как эти риски влияют на инвестирование? Вытеснит ли биометрия традиционные технологии, когда станет неотъемлемой частью кибербезопасности? Олег Глебов рассказал о ключевых инновациях в средствах аутентификации, об обеспечении защиты от компрометации и подмены биометрических данных, а также о применении анализа звуковых потоков для защиты промышленных и индустриальных объектов.

Голосовое управление телефоном и другими устройствами, распознавание по голосу и лицу в банках — сферы, где биометрия применяется уже сегодня. Такая идентификация проще, удобнее и в чем-то более безопасна.

В ближайшее время в IT-системах будет реализована conversation UI — технология общения пользователя с компьютером в диалоговых окнах. Это будет разговор человека и машины на понятном человеку языке.

Рынок биометрии относительно новый, но очень перспективный и быстро растет. Он представляет большой интерес для компаний, занимающихся кибербезопасностью.

Три основных направления, где будет использоваться биометрия:

- *идентификация и аутентификация при доступе к определенным системам;*
- *идентификация сотрудников (сбор информации, поиск инсайдеров, верификация нарушений со стороны персонала);*
- *новые виды интерфейсов — голосовое взаимодействие с системами, чат-боты.*

Биометрическая защита нужна не только бизнесу, но и обычным пользователям. Сегодня физическая и кибербезопасность — видеонаблюдение, мониторинг голоса, защита от вредоносного ПО — разведены и реализуются в разных плоскостях. Но уже очень скоро эти типы угроз будут неотделимы друг от друга.

50%

всех запросов в интернете до конца 2020 г. будут либо автоматическими, либо голосовыми — но не набранными с клавиатуры

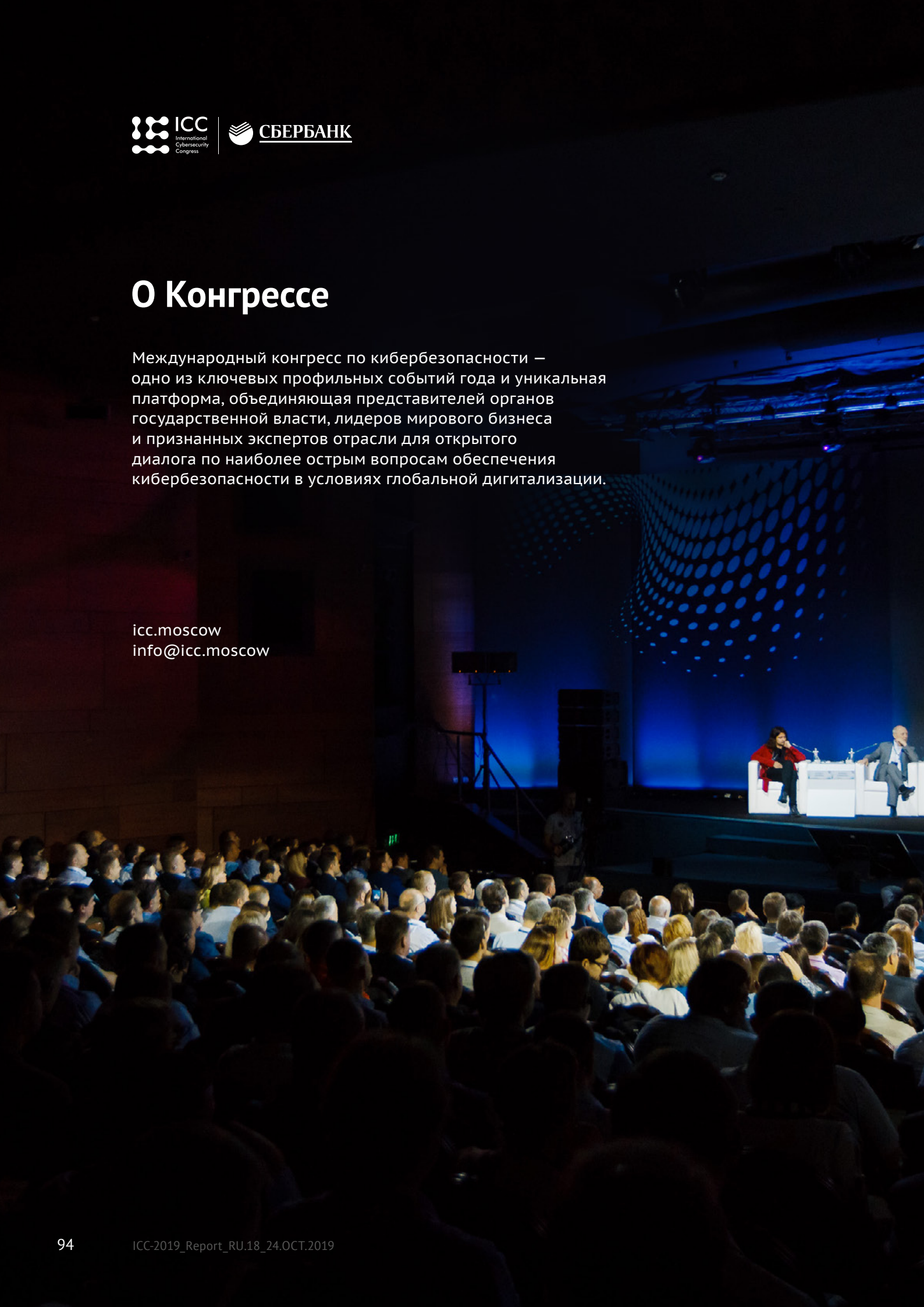
30%

запросов будут поступать с устройств без экрана, то есть с исключительно голосовым управлением

ICC International Cybersecurity Congress | СБЕРБАНК

О Конгрессе

Международный конгресс по кибербезопасности — одно из ключевых профильных событий года и уникальная платформа, объединяющая представителей органов государственной власти, лидеров мирового бизнеса и признанных экспертов отрасли для открытого диалога по наиболее острым вопросам обеспечения кибербезопасности в условиях глобальной дигитализации.



icc.moscow
info@icc.moscow