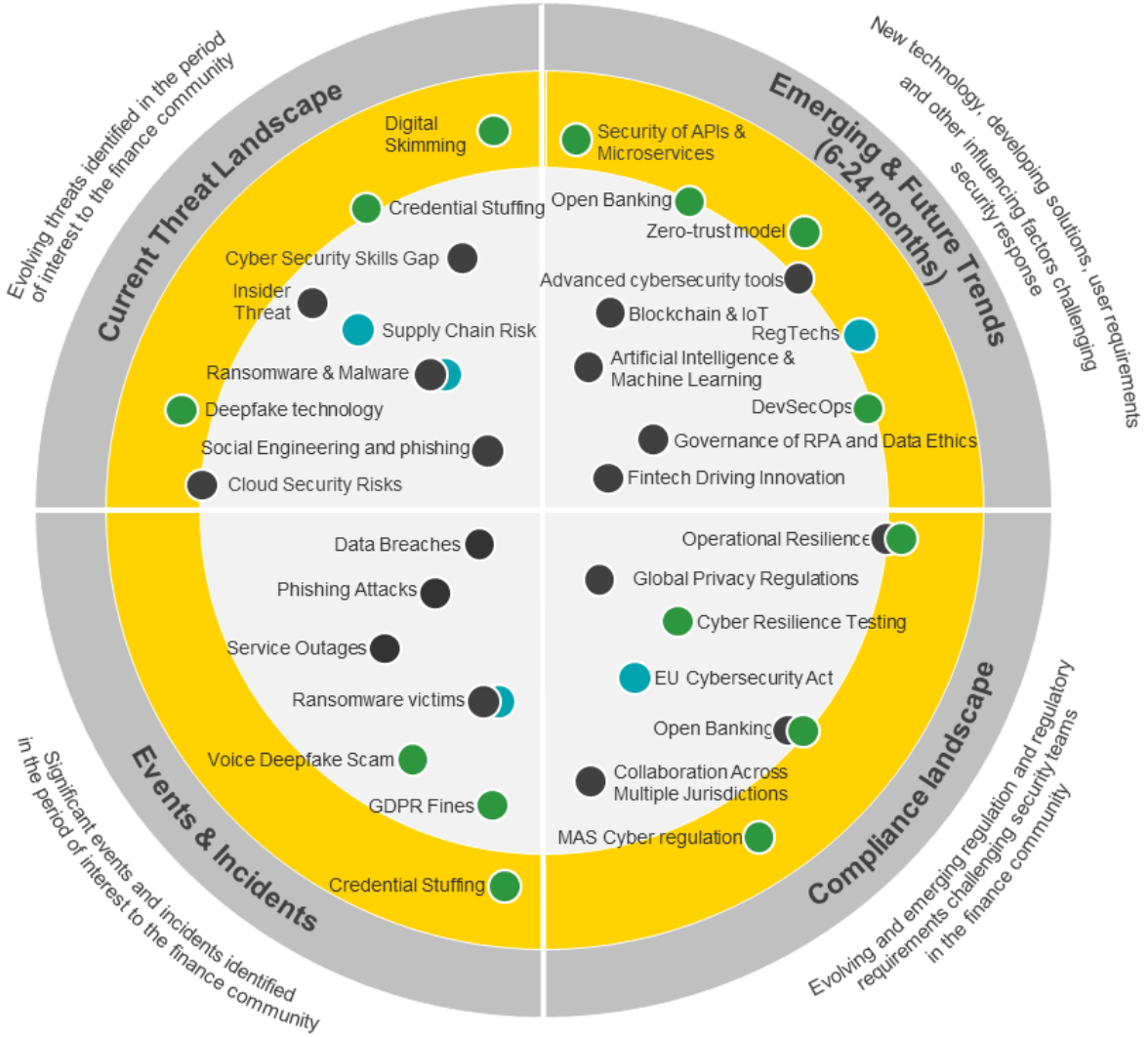
Риск-радар: кибербезопасность в финансовом секторе

Выборочный обзор за 2019 год

Совершенствуя бизнес,
улучшаем мир

Роман Чаплыгин
Департамент бизнес-консультирования

Радар рисков кибербезопасности в финансовом секторе



Риск-радар *- это обзор ключевых событий кибербезопасности, представляющих интерес для компаний финансовой сферы деятельности.*

Радар рисков кибербезопасности *предназначен для получения целостного и обширного понимания актуальных рисков и трендов в области цифровых технологий и защиты информации.*

Вся информация в обзоре собрана из открытых источников и не является выражением мнения EY.

Легенда

Настоящее Будущее

Сохраняющие свою актуальность

Набирающие актуальность

Вновь актуальные

Сектор 1 – Текущий ландшафт угроз (Current Threat Landscape)

1 Риски безопасности облачных сервисов (Cloud Security Risks)

Количество уязвимостей в программных контейнерах, выявленных в первой половине 2019, превышает на **46%** показатели предыдущего года и на **240%** - позапрошлого.

Основные проблемы:

- сложность и разнородность конфигурационных параметров
- некачественная настройка параметров безопасности
- уязвимости систем контейнеризации
- сложность управления и мониторинга
- «Теневое ИТ»
- регуляторные требования

Ключевые угрозы: cloudjacking, account hijacking, misconfiguration of cloud resources, data breaches, privileged user abuse, unauthorized application components, insecure interfaces and APIs, weak control plane, limited cloud usage visibility, and insider threat.

2 Риск цепочки поставок (Supply Chain Risk)

Наиболее уязвимые типы сервисов:

- мобильный банк – 50% увеличение количества атак в 2019 относительно 2018
- электронная почта – применение новых техник сокрытия фишинга (кодировка, изображения, смешивание текстовых символов с символами html)
- сервисы на базе облачных платформ – сложность в настройке параметров безопасности и управлении

Software update supply chain attacks - внедрение вредоносного ПО с использованием инструментов и каналов разработки и обновления ПО.

3 Социальная инженерия и фишинг (Social Engineering & phishing)

67% всех случаев компрометации с участием инсайдеров реализовано с использованием фишинга.

За последние 5 лет были совершены **фишинговые переводы на общую сумму более 12 млрд. долларов** и пострадало более 78 тыс. компаний США, Европы и Великобритании.

Наиболее популярны техники:

- подражание известным людям
- запросы на передачу данных
- запросы на перевод денег

4 Технологий Deepfake (Deepfake Technology)

Технология «Deepfake» позволяет людям манипулировать видео и аудиозаписями и использовать их в мошеннических целях. В то время как компании защищают бизнес процессы от Deepfake, эта технология успешно применяется в фишинговых атаках и социальной инженерии.

Сектор 1 – Текущий ландшафт угроз (Current Threat Landscape)

5 Вымогатели и вирусы (Ransomware & Malware)

Гипотетический стресс-тест компаний Lloyd's of London и Aon показал, что **в случае скоординированной кибератаки с использованием Ransomware совокупный объем страховых выплат может достигнуть 127 млрд. долларов США**.

Существует предположение, что **с развитием GDPR вымогатели будут учитывать размер потенциального штрафа** при определении цены выкупа.

Высокая критичность этого риска также обусловлена высокими затратами на восстановление и распространённостью инструментов Ransomware, в том числе в виде сервисов **Ransomware-as-a-Service (RaaS)**.

Fileless Malware - летом этого года отмечен очередной всплеск атак с использованием «бестелесных вирусов».

6 Подстановка авторизационных данных (Credential Stuffing)

Данная угроза стала популярной в 2018 году и продолжает активно развиваться и применяться как для монетизации краденных данных так и для взлома.

Во второй половине прошлого года было совершено более **2,8 миллиарда автоматических атак с использованием ботов**, многие из которых использовали техники Credential Stuffing. **При уровне успеха от 1% до 3% это приносит до 4 млрд. долларов США убытков**.

7 Недостаток знаний в области кибербезопасности (Cyber Skills Gaps)

Оценочно **к 2022 году нехватка специалистов по кибербезопасности составит около 1,8 млн человек**, при этом 75% сегодняшних кандидатов на такие позиции нуждаются в дополнительном повышении квалификации.

Существенную роль играет уровень осведомленность высшего менеджмента в данной области.

Основными способами повышения грамотности и экспертизы в области безопасности являются инструменты «продвинутого» обучения, управления талантами и развития корпоративной культуры. Также **отмечаются попытки использования Искусственного интеллекта и Машинного обучения для снижения требований к кандидатам и решения отдельных задач кибербезопасности**.

8 Цифровой скимминг (Digital Skimming)

Исследователи RiskIQ сообщают, что **криминальный синдикат Magecart скомпрометировал более 2 миллионов веб-сайтов и взломал более 18 000 хостов**.

Сектор 2 – Актуальные тенденции и тренды (Emerging & Future Trends)

1 Кибербезопасность разработки DevOps (DevSecOps)

DevSecOps обеспечивает внедрение методов кибербезопасности в конвейер DevOps.

По мнению аналитиков Gartner, **к 2021 году 80% разработчиков будут использовать DevSecOps, что в 5 раз больше показателей 2017 (15%) года**.

GitHub запустил функцию автоматического обновления безопасности пользовательских репозиториев.

2 Финтех инновации (Fintech Driving Innovation)

Финтех инновации это новые цифровые продукты и сервисы, созданные с применением больших данных, искусственного интеллекта, машинного обучения, IoT, blockchain, др. Такие продукты создают существенную конкуренцию для классических финансовых сервисов за счет своей гибкости, сниженных издержек, скорости доставки и более выгодных условий.

Примеры: пост оплата за покупки в интернет (**Klarna**), мониторинг и защита цифровой личности (**EverSafe**), ИИ финансовый консультант (**Pefin**).

3 Управление роботизация и этика (Governance of RPA and Data Ethics)

Программная роботизация позволяет сократить длительность выполнения рутинных операций на 70% и исключить ошибки человеческого характера.

Система управления RPA соблюдение этики при автоматическом сборе и обработке данных, а также на минимизацию рисков связанных с доступом и обработкой конфиденциальной информации, мошенничеством, а также с техническими и логическими уязвимостями, присущими платформам и алгоритмам роботизации.

4 Безопасность микро сервисов и API (Security of APIs & Microservices)

В августе NIST опубликовал руководство по обеспечению безопасности микро сервисных архитектур (**NIST SP 800-204, Security Strategies for Microservices-based Application Systems**). Лучшие практики для безопасности микро сервисов включают: Defense in Depth, Tokens and API Gateways, Distributed Tracing and Session Management, Mutual SSL, OAuth.

5 Регуляторные технологии (RegTechs)

RegTech остается в области внимания и представляет интерес для финансовых институтов и регуляторов. **RegTech 3.0** направлен на оптимизацию взаимодействия с регуляторами и сокращение расходов ($270 млрд, 10% операционных расходов, 10-15% общего числа сотрудников) на обеспечение соответствия требованиям.

Сектор 2 – Актуальные тенденции и тренды (Emerging & Future Trends)

6 Модель нулевого доверия (Zero Trust Model)

Модель нулевого доверия заключается в предположении, что **все люди, устройства или организации - даже давние сотрудники - должны рассматриваться как источники потенциальных угроз**.

Архитектура безопасности в соответствии с моделью нулевого доверия подразумевает **защиту всех устройств и соединений и предоставление доступа только в случае установления доверия**, в том числе путем авторизации, пользователя, устройства, места, деятельности и т.п.

Архитектур нулевого доверия включают как классические средства защиты (VPN, DLP, DRM, SIEM, TI и т.д.), так и современные средства поведенческого анализа, адаптивной мульти факторной аутентификации, программной микро сегментации и др.

7 Открытый банкинг (Open Banking)

Open Banking - это процесс открытия внутренних сервисов и данных банков для использования внешними разработчиками. С использованием унифицированных и защищенных API-интерфейсов разработчики могут агрегировать данные из нескольких компаний и предоставлять новые продукты и сервисы как розничным, так и корпоративным клиентам.

8 Продвинутые средства защиты (Advanced cybersecurity tools)

Password-less Authentication – «магическая ссылка», токен, биометрия и т.п. **Next-Gen Anti-Virus** – защита от бестелесных вирусов с использованием AI и ML.

9 Блокчейн и интернет вещей (Blockchain & IoT)

Успешные практические примеры автоматизации и повышения эффективности банковских и логистических процессов (например: HSBC, Maersk). Основные области использования блокчейн:

- **автоматизация процессов,**
- **предотвращение мошенничества,**
- **оптимизация транзакционных издержек,**
- **безопасное ведение учета.**

Блокчейн в сочетании с IoT обеспечивает **контроль и учет изменений состояния физических активов** и прозрачное отображение этого состояния в финансовых инструментах.

10 Искусственный интеллект и машинное обучение (Artificial Intelligence & ML)

Банковская отрасль сосредотачивает свои инвестиции на **использования AI в автоматизированных системах обнаружения и предотвращения угроз, а также для анализе и расследовании случаев мошенничества**. Ожидается, что к 2023 году расходы на системы AI достигнут 97,9 млрд долларов США.

Сектор 3 – Киберинциденты (Events & Incidents)

1 Утечки данных (Data Breaches)

В 2019 году **Equifax** договорилась о мировом соглашении и урегулировании инцидента связанного с утечкой данных 147 млн. человек. В результате **425 мил. долларов США** будут использованы на предоставлении пострадавшим финансовой компенсации или бесплатных услуг.

Capital One – **утечка персональных данных 106 млн клиентов**, включая компрометацию номеров соц. страхования и банковских.

MasterCard – оповестила регуляторов Германии и Бельгии об **инциденте с программой лояльности** в результате которого имена, номера платежных карт, адреса электронной почты, домашние адреса, номера телефонов, пол и даты рождения тысяч клиентов стали доступны в Интернет.

Suprema – Biostar 2 – **утечка почти 30 млн. записей, содержащих биометрические данные** отпечатков и лиц, фото, имена, адреса, пароли и историю трудоустройства.

State Bank of India (SBI) не настроил параметры безопасности доступа на сервере в результате чего любой желающий мог получить доступ к финансовой информации миллионов клиентов.

2 Штрафы за нарушение требований GDPR (GDPR Fines)

Сумма 10 штрафов за нарушение требований GDPR в 2019 году составила 345 млн. фунтов стерлингов, при чем 3 из 10 составляют 90% этой суммы:

- **Google** – 44 млн. фунтов за отсутствие прозрачности, неадекватную информацию и отсутствие действительного согласия на персонализацию рекламы
- **British Airways** – 183 млн. фунтов за утечку данных
- **Marriott International** – 99 млн. фунтов за утечку данных

3 Фишинговые атаки (Phishing Attacks)

American Express - фишинговая атака по электронной почте с использованием техник сокрытия полной ссылки и домена позволила обойти механизмы защиты и украсть карточные данные.

Sure – атака на производителя мобильных телефонов с кражей банковских реквизитов и личных данных.

4 Голосовое мошенничество Deepfake (Voice Deepfake Scam)

Генеральный директор британской энергетической компании **совершил перевод на 220 тыс. евро по ложной просьбе** от имени его немецкого руководителя, голос которого был фальсифицирован с использованием **ИИ**.

Сектор 3 – Киберинциденты (Events & Incidents)

5 Сбои в предоставлении сервиса (Service Outages)

В декабре 2018, технические работы в **TSB** затянулись на несколько часов оставив **2 млн. пользователей без банковского сервиса**. Ситуация возникла в результате проблемной миграции на новую платформу и вызывала **проблемы в период с апреля по декабрь 2018**.

В январе 2019 в **Lloyds Banking Group «зависло» около 400.000** транзакций из-за сбоя в системе платежей **Faster Payments**. Повторные транзакции клиентов могли привести к начислению дополнительной комиссии.

В августе 2019, в ЦОД **Amazon AWS US-EAST-1** произошел сбой питания с последующим **выключением резервных генераторов и потере данных**. Сбой затронул 7,5% мощностей ES2.

В августе 2019 **клиенты банков Royal Bank of Scotland (RBS), Nationwide Building Society и Tesco Bank не могли получить доступ к своим счетам и оплатить по кредитам**. Инцидент пришелся на пик выплат по задолженностям и произошел в связи с сбоем ИТ сервисов американской платежной компании TSYS.

6 Жертвы вирусов-вымогателей (Ransomware victims)

Компания **Mondelez подала судебный иск на 100 млн. долларов США** на страховую компанию Zurich, отказавшуюся выплатить страховку после атаки NotPetya.

Eurofins Scientific - судебно-медицинская лаборатория предположительно **выплатила выкуп в результате кибератаки** в июне 2019.

Лейк-Сити, штат Флорида, **выплатил выкуп в биткойнах на сумму 460 000 долларов**.

Ривьера-Бич, штат Флорида, всего несколько недель спустя, **заплатил 600 000 долларов в качестве выкупа**.

7 Кража учетных данных (Credential Stuffing Attacks)

Кража имен пользователей и паролей от личных кабинетов клиентов финансово-страховой компании **State Farm**, после этого State Farm произвела сброс паролей скомпрометированных учетных записей.

Телекоммуникационная компания **Sky заблокировала учетные записи и попросила пользователей сбросить пароли после выявленной кибератаки** с использованием подстановки учетных данных. Разблокировка учетных записей производилась по телефону.

Сектор 4 – Регуляторный ландшафт (Compliance landscape)

1 Операционная устойчивость (Operational Resilience)

Банк Англии продолжает развивать **регулирование в области операционной устойчивости** путем подготовки рекомендаций, их обсуждения с профессиональным сообществом и апробацию, с последующей доработкой и созданием стандарта. Данное регулирование включает аспекты и кибер устойчивости.

ЕЦБ опубликовал официальный **документ по надзору в области киберустойчивости финансовых рынков**. Регулирование в этой области продвигается и основано на указаниях Банка международных расчетов и Международной организацией комиссий по ценным бумагам (Committee on Payments and Market Infrastructures - BIS and the Board of the International Organization of Securities Commissions).

European Banking Authority (EBA) – опубликовал **Guidelines on ICT and security risk management** комплексное руководство по безопасности, рискменеджементу и непрерывности, а также **Guidelines on outsourcing arrangements**, учитывающее современные тренды, технологи и риски.

2 Тестирование киберустойчивости (Cyber Resilience Testing)

CBEST - **комплексное руководство по проведению тестирования устойчивости** финансовых организаций к кибератакам. В настоящий момент является обязательным для банков Англии и тиражируется на страховые компании. Регуляторы Великобритании (Bank of England, FCA, PRA) используют этот подход для оценки стрессоустойчивости финансового сектора в целом.

TIBER-EU - **европейский аналог CBEST**, утвержденный ЕЦБ и Нацбанком Европы. Документ сфокусирован на создании постоянно действующих команд по тестированию защищенности (red team) и подразумевает активное взаимодействие со специально созданным регулятором центром компетенций TIBER-EU Knowledge Centre. Рекомендовано кросс-территориальное и кросс-организационное применение и тестирование.

CPMI-IOSCO (Комитет по платежам и рыночной инфраструктуры) опубликовал **отчет по результатам анализа практик и подходов по кибербезопасности**.

3 Кросс территориальное взаимодействие (Collaboration Across Multiple Jurisdictions)

Cyber Assessment Framework v3.0 – унифицированный регламент оценки уровня кибербезопасности, разработанный UK National Cyber Security Centre (NCSC). **Cybersecurity Profile** - инструмент по оценке уровня кибербезопасности, разработанный Financial Services Sector Co-ordinating Council (FSSCC).

Сектор 4 – Регуляторный ландшафт (Compliance landscape)

4 Кибербезопасность финсектора Сингапура (MAS Cyber regulation)

Руководство по управлению технологическими рисками (MAS Technology Risk Management Guidelines) – обновление документа от 2013 года с дополнением в части:

- управление и надзор
- прорывные технологии
- разработка ПО
- кибер устойчивость.

Уведомления о кибер-гигиене (Cyber Hygiene Notice) – набор базовых требований и рекомендаций по кибербезопасности для каждого типа организаций финсектора.

Атака Баше (Bashe attack) – отчет о сценарном анализе киберинцидента вызванного вирусным заражением. Сценарный анализ был проведен под руководством **Cyber Risk Management Project (CyRiM)** и показал, что ущерб может составить 193 млрд.. долларов США и отразиться на 600 тыс. компаний по всему миру.

Шен Атака (Shen Attack) – отчет о сценарном анализе кибератаки на порты Азиатско-Тихоокеанского региона. В случае воздействия на 15 ключевых портов этого региона ущерб от инцидента может достигнуть 110 млрд долларов США.

5 Открытый банкинг (Open Banking)

Consumer data right (CDR) – австралийское казначейство официально опубликовало набор стандартов в поддержку повышения уровня контроля и прозрачности обработки клиентских данных, а также реализации принципов Открытого банкинга. CDR содержит детальные технические рекомендации и примеры исходного кода.

Payment Service Direct 2 (PSD2) – европейские закон по взаимодействию банков и платежных сервисов, включая предоставление доступа к клиентским данным и требования безопасности с финальным сроком приведения в соответствие сентябрь 2019. Активно поддерживается European Banking Authority в части разъяснений, разработки технических стандартов и руководств.

6 Акт о кибербезопасности ЕС (EU Cybersecurity Act)

Инициирует создание общеевропейских стандартов по кибербезопасности и наделяет **Европейское агентство по безопасности сетей и данных (ENISA) полномочиями по координации действий по защите от кибератак и созданию общеевропейской системы сертификации**.

7 Международное регулирование приватности (Global Privacy Regulations)

GDPR: One Year On – отчет о результатах применения GDPR за последний год.

California Consumer Privacy Act - с 2020 года позволит потребителю требовать раскрытия источников сбора и сведений о продаже его ПДн.

Как использовать Риск-радар?

1

Убедитесь что ваша **оценка рисков кибербезопасности** учитывает, в том числе:

- индустриальный опыт и инциденты зарубежных компаний
- современные цифровые технологии и направления развития отраслевых стандартов, законов и требований
- результаты сценарного анализа, стресс-тестов и учений по кибербезопасности.

2

При планировании и реализации **мероприятий по кибербезопасности**:

- оценивайте своевременность перехода на продвинутые средства и способы защиты информации
- анализируйте и применяйте опыт и рекомендации зарубежных регуляторов и отраслевых сообществ
- учитывайте возможности аутсорсинга сервисов кибербезопасности.

3

Инвестируйте в повышение **киберустойчивости** путем:

- адаптации под современные модели создания продуктов и взаимодействия с клиентами
- бесшовной интеграции в бизнес и ИТ процессы
- оптимизации устоявшихся процедур и тестирования новых технологий.

Спасибо за внимание!

Роман Чаплыгин
директор, департамент бизнес консультирования, EY

Tel.: +7 (903) 272 1620
Email: Roman.Chaplygin@ru.ey.com

Источники информации:

www.bankofengland.co.uk
https://ico.org.uk/
www.ncsc.gov.uk
https://eba.europa.eu/
www.mas.gov.sg
https://irfrc.ntu.edu.sg/
www.accc.gov.au
www.iosco.org
https://consumerdatastandards.org.au/
https://fra.europa.eu/
https://fssc.org/

www.ft.com
www.forbes.com
www.zdnet.com
www.searchcloudsecurity.techtarget.com
www.computerweekly.com
www.scmagazine.com
www.bbc.com
www.pcmag.com
www.ftadviser.com
www.rsmuk.com
www.redscan.com
www.cpomagazine.com
www.mhlnews.com
www.globenewswire.com
www.tech.newstatesman.com
www.information-age.com
www.agio.com
www.abusix.com
www.computing.co.uk
www.itgovernance.co.uk
www.globenewswire.com
www.cnbc.com
www.finextra.com
www.cbronline.com
www.itconvergence.com
https://blog.protiviti.com/
http://business-review.eu/
www.plutora.com
www.businessinsider.de
www.nextgov.com
www.technologyreview.com
www.globalbankingandfinance.com
https://devops.com/
https://logrhythm.com/
https://portswigger.net/
www.bleepingcomputer.com
www.businessinsider.com
www.scmagazineuk.com
https://gizmodo.com/
www.propublica.org
www.uktech.news
www.finextra.com
www.lexology.com
www.cpomagazine.com
www.thecityuk.com
www.securitymagazine.com
www.sky.com
https://gdpr.report/
https://cofense.com/
www.wsj.com
www.ukauthority.com
https://bpi.com/
www.globalgovernmentforum.com
https://free.dataguidance.com/

EY | Assurance | Tax | Transactions | Advisory

EY является международным лидером в области аудита, налогообложения, сопровождения сделок и консультирования. Наши знания и качество услуг помогают укреплять доверие общественности к рынкам капитала и экономике в разных странах мира. Мы формируем выдающихся лидеров, под руководством которых наш коллектив всегда выполняет взятые на себя обязательства. Тем самым мы вносим значимый вклад в улучшение деловой среды на благо наших сотрудников, клиентов и общества в целом.

Мы взаимодействуем с компаниями из стран СНГ, помогая им в достижении бизнес-целей. В 20 офисах нашей фирмы (в Москве, Санкт-Петербурге, Новосибирске, Екатеринбурге, Казани, Краснодаре, Ростове-на-Дону, Тольятти, Владивостоке, Южно-Сахалинске, Алматы, Астане, Атырау, Бишкеке, Баку, Киеве, Ташкенте, Тбилиси, Ереване и Минске) работают 4500 специалистов.

Название EY относится к глобальной организации и может относиться к одной или нескольким компаниям, входящим в состав Ernst & Young Global Limited, каждая из которых является отдельным юридическим лицом. Ernst & Young Global Limited − юридическое лицо, созданное в соответствии с законодательством Великобритании, − является компанией, ограниченной гарантиями ее участников, и не оказывает услуг клиентам. Более подробная информация представлена на нашем сайте: ey.com.

Данная презентация предназначена для предоставления информирования и не может быть использована для анализа или выводов без дополнительной консультации с EY. EY не гарантирует и не подтверждает, что информация в данной презентации достаточна или релевантна для использования третьей стороной. EY не принимает и не несет никакой ответственности за использование Презентации в каких-либо иных целях или какими-либо иными юридическими или физическими лицами. Любое юридическое или физическое лицо, полагающееся на данные Презентации, принимает на себя соответствующие риски. EY снимает с себя всю ответственность по отношению стороне? которая приняла такое решение, или на которую такое решение повлияло. Заключение договора оказания услуг возможно только после успешного завершения внутренних процедур риск-менеджмента компании EY.

www.ey.com/ru