MOEX GROUP

MOEX.COM

Безопасный удаленный доступ. Эффективная защита в период массивных кибератак.

ПОДГОТОВЛЕНО: **СЕРГЕЙ ДЕМИДОВ**
ДИРЕКТОР ДЕПАРТАМЕНТА ОПЕРАЦИОННЫХ РИСКОВ, ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И НЕПРЕРЫВНОСТИ БИЗНЕСА

12/10/2022

Кто мы?

Что из себя представляет MOEX Group?

Какая наша роль в экономике РФ?

Структура

MOEX GROUP

ФИН УСЛУГИ

Торги

Клиринг

Расчеты

НТБ
Товарная биржа

Московская Биржа
Фондовый рынок
Валютный рынок
Денежный рынок
Срочный рынок

НКО НКЦ (АО)
Клиринговый центр
Центральный контрагент на всех рынках

НКО АО НРД
Центральный депозитарий
Расчетный центр

Физические лица

Профессиональные участники рынка ценных бумаг

Клиенты участников торгов

Банки

Компании реального сектора

Разработчики ПО

ФОИВ'ы

ИТ инфраструктура, телекоммуникации, разработка ПО

Результаты


Торги
Клиринг
Расчеты
Объем торгов в 2020
947 трлн руб.
+19% к 2019
Капитал НКЦ на конец 2020
73,2 млрд руб.
+4% к 2019
Активы на хранении на конец 2020
63,6 трлн руб.
+21% к 2019
Московская Биржа
Фондовый рынок
Валютный рынок
Денежный рынок
Срочный рынок
77%
Национальная товарная биржа (НТБ)
Рынок зерна, сахара и др.
Объем гос. интервенций в 2020
21 млрд руб.
+107% к 2019
100%
НКО НКЦ
Клиринговый центр
Центральный контрагент на всех рынках
НРД
Центральный депозитарий
Расчетный центр
Регистратор финансовых транзакций
99,9%

Инфраструктура

Инфраструктура Московской Биржи – инструмент **денежно-кредитной политики Банка России**, а также инвестирования средств бюджета и пенсионных фондов и регулирования рынка зерна

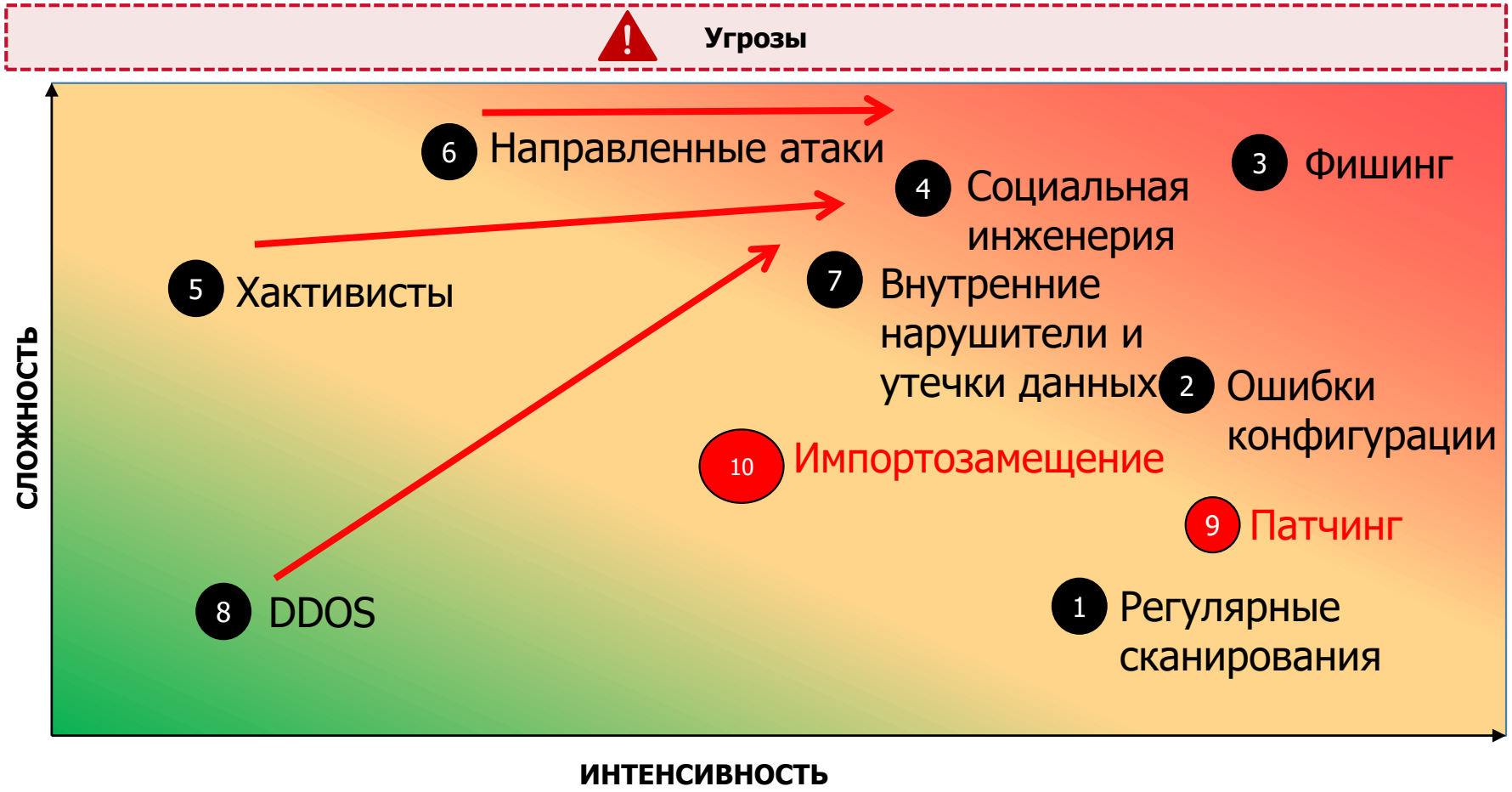
Центральный Банк России	▪ Денежно-кредитная политика	▪ Валютные операции (спот/своп) *(с 1992)* ▪ Прямое РЕПО с Банком России *(с 1996)* ▪ Депозитные и кредитные операции *(с 2004)* ▪ Облигации Банка России *(с 2004)*	2,6 трлн руб., -41% к 2019 2,8 трлн руб., +10 раз к 2019 40,2 трлн руб., -11% к 2019 5,2 трлн руб., -15% к 2019
Министерство Финансов	▪ Размещение государственных облигаций	▪ Рынок государственных облигаций *(с 1993)*	5,3 трлн руб., 158% к 2019
Федеральное Казначейство	▪ Инвестирование средств бюджета	▪ Депозитные операции *(с 2012)* ▪ РЕПО с Федеральным Казначейством *(с 2019)* ▪ Депозитные аукционы с ЦК по размещению средств единого казначейского счета *(с января 2021)*	6,7 трлн руб., -7% к 2019 22,3 трлн руб., +1000 раз к 2019
Пенсионный Фонд России (ПФР)	▪ Инвестирование пенсионных средств под управлением ПФР	▪ Депозитные операции *(с 2013)*	202 млрд руб., -30% к 2019
Внешэкономбанк (ВЭБ)	▪ Инвестирование пенсионных средств под управлением ВЭБ	▪ Депозитные аукционы *(с 2009)*	280 млрд руб., -20% к 2019
Министерство сельского хозяйства	▪ Регулирование рынка зерна	▪ Интервенции на рынке зерна *(с 2002)* ▪ Расчет трех ценовых индексов зерновых культур: пшеницы, ячменя и кукурузы *(с апреля 2021)*	21 млрд руб., +107% к 2019

Безопасный удаленный доступ. Эффективная защита в период массивных кибератак.

Как изменились угрозы в 2022 году?

Какие риски несет в себе удаленный доступ?

Основные угрозы кибер-безопасности Московской Биржи и как они изменились в 2022 году



Риск №1

Размытый периметр безопасности

При массовой удаленной работе невозможно зафиксировать, что именно является периметром безопасности. Фактически отпечаток корпоративных систем и данных распространяется на рабочие места конечных пользователей, зачастую находящиеся вне полного контроля администраторов и/или служб информационной безопасности

Как можно снизить риск?

- Оценка рисков, определение профиля риска
- Фокус на критически важной инфраструктуре
- При использовании личных устройств проверка базовых требований безопасности на хосте, с которого идет подключение
- Virtual Desktop Infrastructure (VDI)
- Сегментация сети исходя из профиля риск

Риск №2

Атаки на инфраструктуру удаленного доступа

После массового перехода на удаленную работу произошло сразу несколько инцидентов, когда злоумышленники пользовались тем фактом, что большинство сотрудников находятся на удаленной работе, и в результате организация оказывается более уязвимой к атакам на инфраструктуру удаленного доступа

Как можно снизить риск?

- Регулярные тесты защиты от DDOS
- Проведение crash-тестов изнутри сети
- Разделение сетевого оборудования, обслуживающего периметр и ядро сети
- Сохранение критических функций внутри периметра

Риск №3

Контроль за сотрудниками

При массовой удаленной работе эффективность отслеживания состояния сотрудников и их мотивации существенно снизилась, гораздо сложнее стало улавливать тот момент когда сотрудник демотивируется и готов перейти на «темную сторону силы»

Как можно снизить риск?

- Внедрение специализированных решений, в том числе для оценки «вовлеченности» сотрудников
- Валидация привилегированного доступа
- Отработка сценарного анализа рисков ИБ/”Know Your Malicious Actor”
- Пересмотр мотивации ключевого персонала
- Контроль аномалий при доступе к данным

Риск №4

Внимательность сотрудников

Находясь вне рабочего места, сотрудники зачастую менее сфокусированы и могут легче поддаваться на уловки злоумышленников. При этом, понимая подобный риск, злоумышленники интенсифицируют рассылки с вредоносными ПО.

Как можно снизить риск?

- Пересмотр подходов к обучению сотрудников
- Новые форматы тестов
- Геймификация
- Горячая линия ИБ
- Нематериальное стимулирование

Риск №5

Игнорирование принципов физической безопасности

Сам принцип удаленной работы во многом размывает принципы физической безопасности.

Как можно снизить риск?

- Риск профилирования персонала в зависимости от степени потенциальной угрозы
- Включение геолокации для сотрудников «под риском»
- Биометрическая идентификация и биометрический контроль
- Создание для сотрудников понятных правил поведения: «в аэропорту», «в кафе», «дома» и т.д.
- Запрет локального хранения конфиденциальной информации

Риск №6

Использование для доступа недоверенных устройств

В концепции BYOD, даже при использовании всех необходимых средств и мер безопасности внутри периметра, конечная безопасность может зависеть от того, как пользователь позаботился о безопасности своего собственного устройства.

Как можно снизить риск?

- Средства контроля за состоянием хоста
- Средства MDM (Mobile Device Management)
- Повышение осведомленности персонала о рисках BYOD
- Пересмотр стратегии удаленного доступа для персонала с привилегированным доступом

Как полностью избежать рисков?

НИКАК!

СПАСИБО
ЗА ВНИМАНИЕ

+7 (495) 363-32-32