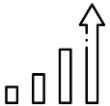
Предиктивные методы обеспечения ИБ

Зуев Владимир, АО «Россельхозбанк»

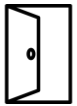
Ноябрь 2021 год

Окружающая обстановка в ИТ



Высокий темп развития и эволюции информационных технологий и цифровизация бизнеса

Рост размеров ИТ инфраструктуры и ИТ активов по всему миру



Повышение доступности вычислительных мощностей не только для бизнеса, но и для частных лиц

'21 МЕНЯЕМСЯ ВМЕСТЕ

Сложности для ИБ

- Рост числа применяемых средств защиты и обрабатываемых типов событий
- Стремительный рост числа обрабатываемых событий
- Наростающая сложность моделирования актуальных угроз и построения ландшафта защиты
- Необходимость в постоянном притоке квалифицированных кадров
- Необходимость развертывания и адаптации средств защиты со скоростью и гибкостью, соответствующей развитию бизнеса

'21 МЕНЯЕМСЯ ВМЕСТЕ

Что может дать предиктив?

- Исключение человеческого фактора (усталость, отвлеченность, эмоциональность)
- Способность за счет разных технологий обрабатывать большие объемы данных (как нормализованных, так и сырых)
- Нарастающая со временем эффективность анализа за счет постоянного машинного обучения
- Возможность обнаружения признаков актуальных атак в отрыве от «классического» сигнатурного анализа
- Адаптивность за счет обучаемости (один инструмент, способный закрыть несколько технологических «направлений»)

'21 МЕНЯЕМСЯ ВМЕСТЕ

Подходы к потреблению

Вендорный

- Более прост в использовании
- Имеет конкретный перечень решаемых задач
- Персонал, использующий инструменты в работе, может обучаться, основываясь на опыте вендора
- Менее гибок за счет закрытости настроек ИИ
- Зависимость эффективности инструмента от скорости ИИ и качества обучения, проводимого вендором

Собственная разработка

- Возможность тонкой и точной настройке в соответствии с решаемыми задачами конкретного субъекта защиты
- Прозрачность и понятность функционирования инструмента за счет собственной разработки и настройке
- Высокая сложность создания и поддержки жизненного цикла
- Необходимость в высококвалифицированном и редком на рынке персонале

Примеры наиболее распространенных сценариев использования по классам

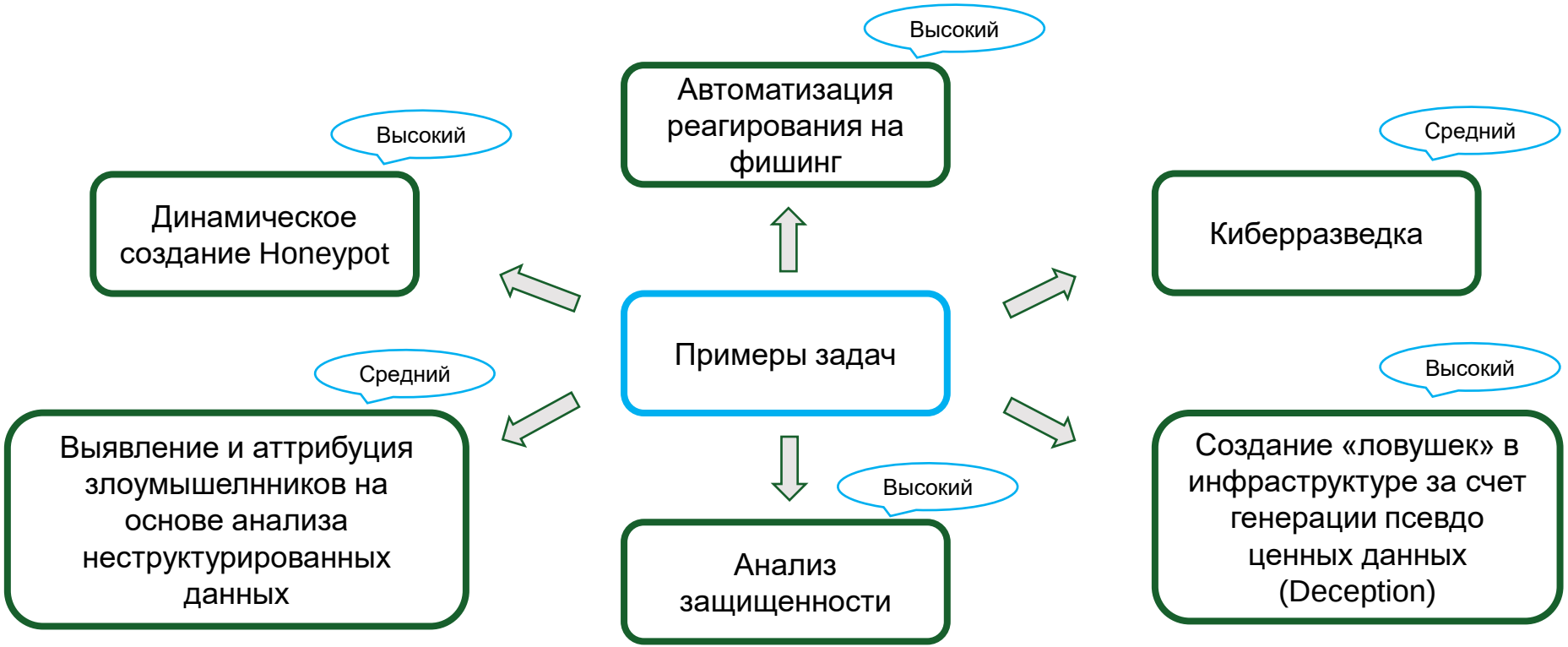
Поведенческий анализ пользователей и сущностей (User and Entity Behavior Analytics (UEBA))

Анализ сущностей (Identity Analytics (IdA))

Поиск угроз (Threat hunting)

'21 МЕНЯЕМСЯ ВМЕСТЕ

Дальнейшие возможности применения ИИ для развития мер защиты



'21 МЕНЯЕМСЯ ВМЕСТЕ

Выводы

Использование предиктивных методов на основе ИИ может стать подспорьем для построения защиты организации, но не является серебрянной пулей от всех рисков и угроз.

Технологии ИИ используются по обе стороны «баррикад», но не даёт ни одной из сторон весомого преимущества.

Вендорные решения – отличный способ дополнительно использовать опыт и экспертность разработчиков, самостоятельная разработка – путь для организаций с высоким уровнем зрелости и богатой ресурсной базой (как материальной, так и человеческой).

В будущем как предиктивные методы так и технологии ИИ в целом будут играть важную роль в ИБ. Вопрос лишь в том, на сколько велик будет разрыв между скоростью их внедрения в ИТ и в ИБ.

В настоящий момент наиболее реальным приминением данных технологий представляется автоматизация операционной деятельности для высвобождения человеческих ресурсов.

'21 МЕНЯЕМСЯ ВМЕСТЕ

Спасибо за внимание!

E-mail: zuevvm@rshb.ru
Tg: @Kpzrr

'21 МЕНЯЕМСЯ ВМЕСТЕ