Информационная безопасность, ожидания и действительность

Специалисты по информационной безопасности резко возросли в цене по зарплате. От них ожидают решения задач существенного улучшения комфортности жизни и расширения пространства услуг массового пользователя-граждан нашего Союзного Государства. Целостность и достоверность информации может существенно способствовать выполнению этой задачи

Академия криптографии Российской Федерации

А.П. БАРАНОВ

Основные темы ожиданий

1. Блокчейн – эффективная технология для борьбы с коррупцией и обеспечение чистоты данных . Массовая надежная система
2. Искусственный интеллект(ИИ), как замена своему собственному. Чат GPT напишет любую докторскую диссертацию. Новый ход маркетологов: теперь у нас не ИИ , а компьютерный интеллект(КИ)
3. Нейронная сеть – аналог «крепких» нервов для всего. Фактически и составляет КИ и работает везде, включая защиту информации
4. Большие данные, т.к. кругом много информации и ее нельзя подделать. Можно монетизировать и построить экономику данных.
5. Универсальный квантовый компьютер(КК) обеспечит райское существование и он уже близок по времени. Он изменит криптографию
6. Корпоративная информационная безопасность(ИБ) сама собой перерастет в массовую- по направлениям конфиденциальности, целостности и доступности

Действующая реальность информационной безопасности и угрозы

- Блокчейн, практикующийся принцип безопасности в цифровых валютах, массовых системах удаленных голосований и др. ИБ удостоверяющего центра или оператор цифровой биржи
- Применение искусственного интеллекта в автоматизации функций устройств и процессов. Лингвистические модели и информационная агрессия
- Нейронные сети при распознавании образов, включая компьютерное зрение. Python - проблема импортозамещения
- Большие данные в применении к анализу спроса и оценки состояния гражданского общества. Возможность дезинформации. Корпоративные методы обеспечения ИБ массово практически не используются
- Квантовые компьютеры (КК)- гонка в разработке вариантов реализаций физических устройств. Вместо реальных криптозадач отвлечение на негодный объект - построение фантастических умозрительных конструкций. Аналогия уже была - гонка «Звездных войн».

Безопасный – опасный блокчейн 1

1. Суть блок-чейна в подписании блока информации электронными подписями(ЭР) различными рабочими местами
2. Алгоритмы реализации и порядок подписания отличаются и зависят от предназначения системы:
3. а) кадастр недвижимости пять ведомств – пять подписей под каждым блоком;
4. б) криптовалюта – продавец, покупатель и майнер - три подписи;
5. в) при голосовании -две подписи- голосующий и оператор

6. Неизменность базируется на надежности хранения и применения закрытого ключа ЭП
7. Доступность обеспечивается множеством мест хранения контрактов в сети т.е. доступностью сети

Безопасный блок-чейн 2

1. Доступность эквивалентна возможности применения элементов сети
2. Надежность хранения ключа зависит от множества факторов, обеспечить которые можно в корпоративной сети и только на самом низком уровне безопасности в массовом применении
3. Проблемы: ОС с интегрированным криптопровайдером, доверенное аппаратное обеспечение и представление информации пользователю
4. Авторизация идентифицирует только сертификат ключа, а не само лицо. Удаленная биометрия- фикция в условиях развития нейросетевых технологий подделки, отпечатков пальцев, портретов и их оживления в режиме реального времени
5. Безопасность блок-чейна должна быть увязана с ограничениями для прикладного ПО и базироваться на сертифицированном криптопровайдере с доверенным оператором системы, что нереализуемо у массового пользователя

Рутина в искусственном интеллекте – лингвистические модели

1. Искусственный интеллект это не что иное, как экспертные системы (ЭС), известные с семидесятых годов прошлого столетия
2. ЭС состоит из следующих подсистем:
   а) форматирование и структуризация вводимых разнородных данных
   б) описание моделей систем, рассматриваемых данной ЭС и их соотношений с вводимыми данными и условиями
   в) формальное представление задач в направлении создания ЭС
   г) разбиение общих задач на элементарные подзадачи (ЭПЗ) и разработка параметров стыковки результатов решения ЭПЗ
   д) правила стыковки ЭПЗ и перебора вариантов цепочек ЭПЗ
   е) правила решения ЭПЗ – знания. Методы представления знаний
   ж) представление итогового результата из формализованных данных в воспринимаемые человеком виде
3. Для решения ЭПЗ могут использоваться различные инструменты, включая нейронные сети, квантовые компьютеры и модели языка

Исторические промахи в развитии искусственного интеллекта

1. Система IBM – Ватсон. Известные направления применения: медицина по классам заболеваний, финансовые задачи анализа и прогноза и т.д.
2. Крупные продвижения: а) система введения и формализации различных данных их структуризация и рубрикация в Хранилище;
   б) система накопления знаний, т.е. методов структуризации Задачи и ее разбиение на ЭПЗ с помощью обучения ЭС узкими, профильными специалистами
3. Результат: «быстрое» обучения ЭС за счёт «облегчения» обучения профессиональных специалистов
4. Все данные и «знания» располагаются на территории USA. Ответ может быть представлен по Интернету. Применение в медицине неуд. В Москве отказались от применения ИИ при диагностике заболеваний На разработку системы было потрачено более 3 млрд. $, а продается сейчас за 1.5.
5. Главное противоречие: ИИ обрабатывает конечную ситуацию, ему недоступна простая действительная прямая- континиум. Трамвай с КИ наехал на 3 человек, стоящих на рельсах - не предсказуемая ситуация

Нейронная сеть и задачи ИБ

1. Однослойная нейронная сеть – это перцептрон, т.е. обычный линейный фильтр, имеющий n – входов и n - весовых коэффициентов с дискриминирующей функцией суммы выходов. Апроксимирует функцию
2. Обучение – это формирование (вычисление) значений весовых коэффициентов. Теоретического обоснования работоспособности даже двуслойных НС не существует, только эксперементальные
3. Адаптивные НС – перестраиваемые в ходе работы линейные фильтры, по заранее выработанному правилу достижения наибольшей пользы
4. НС применяется для фильтрации сигналов от помех в фазированных, многоканальных решетках и задачах распознавания образов и анализа сцен т.е. для оценки опасности ПЭМИН и др., а так же для аутентификации при распознавании биометрических данных
5. Сложность вычислений зависит от n и как правило реализуется на видеокартах - ускорителях. Пригодна для решения некоторых ЭПЗ

ИБ «больших» данных (БоД)

1. БоД - обработка массивных данных больших объемов и разнообразных источников аналитическими методами
2. Суть в концентрация информации, ее извлечение и сопоставление при получении из разрозненных источников. Выявление ложных включений и вранья
3. Составляющие систем БоД :
   - высокоскоростной доверенный транспорт и системы взаимодействия с массовым пользователем;
   - большие хранилища; - -
   - аналитические системы.

   Соответственно К,Ц,Д- три задачи ИБ относятся ко всем подсистемам.
   Импортозамещение по различным подсистемам имеет различные уровни успеха
4. Хуже всего с большими хранилищами предназначенными для решения сложных аналитических и многократных транзакционных задач
5. Проблема с обеспечением гарантий доступности на импортном телекоммуникационном оборудовании. Нет собственных или аттестованных телекоммуникационных чипов типа Марвеловских

Квантовый компьютинг (КК) и Квантовые вычисления

1. КК - специальным образом организованные вычисления подобно аналоговым ЭВМ с использованием системы случайных величин
2. Основа универсального КК - конкретное множество физических объектов, допускающих определенные связи между объектами
3. Кубит - физическая сущность, моделируемая комплексной случайной величиной, которая при реализации (наблюдении) принимает одно из двух значений О или 1
4. Множество кубитов моделируется множеством коррелированных случайных величин(например, спутанные состояния)
5. Сеть и вид корреляций определяется конкретной решаемой задачей
6. В общем случае надо задать 2^n параметров для задачи решения системы булевых уравнений с n неизвестными. Квантовый акселератор частной задачи может иметь фиксированную сеть, что технически существенно проще реализовать. Перспектива - квантовые частные акселераторы

«Достижения» реализации КК

1. Предложен КК в 1980 году, т.е. 44 года назад. Сейчас реализован на 10 кубитах (за 6 лет с 2018года добавилось 2 кубита)
2. Для некоторого класса задач реализован n=100 кубитный компьютер, но не для наиболее актуальных направлений, а как акселератор именно для этих задач в виде сложнейшего физического прибора, похожего на грандиозный аналоговый компьютер(прибор)
3. По сути сейчас для каждой математической задачи нужен свой квантовый алгоритм вычислений и в настоящее время свой КК акселератор
4. Моделирование на традиционной ЭВМ возможно для 50 кубитов (системы 50 случайных величин)
5. В системе ЭП по ГОСТ сейчас n = 256 или 512 (600-1200 лет)
6. Постквантовая криптография оперирует еще большими величинами n с произвольными конфигурациями, следовательно, она фантазийна

Выводы по перспективам ожиданий

- Блокчейн требует как системы ЭП со строгим контролем работы УЦ и оперативного контроля оператора криптобиржи
- ИИ - в ближайшем и отдаленном будущем - полезный помощник при четко определенных и оттестированных для него задач. Как бы не хотелось на него все возложить, но это подруливатель и ALARM
- Нейронная сеть - эффективный инструмент при решении в отдельных фиксированных конечных моделях ситуаций конкретных проблем
- БоД - концентрация информации для прояснения тенденций и принятия решений с возможностью выявления дезинформации. Требует обеспечения целостности и доступности системы
- КК - в настоящее время и в ближайшее время акселератор решения отдельных задач, в том числе криптографических
- Сегмент обеспечения ИБ массового пользователя ждет эффективных, удобных для применения и недорогих решений