

Обзор презентационных материалов по информационной безопасности и цифровым проектам

Редакция от 18 октября 2026 года

Краткое резюме

Отчёт сводит шесть локально доступных PDF-материалов: четыре презентации из исходного каталога и два доклада Black Hat. Визуально просмотрены контактные листы всех 193 PDF-страниц. Глубина текстового разбора неодинакова: «Сырьё решает» имеет структурированное текстовое извлечение; Safari и Bytecode разобраны по тексту презентаций; у NEMESIS, «Атласа» и «ИБ · 2025—2026» мелкие подписи и часть содержания ещё требуют полноразмерного увеличения/извлечения. Визуальные наблюдения отделены от выводов о содержании; контакт-листы дают общее представление о дизайне, но не позволяют подтвердить каждую мелкую подпись или читаемость в аудитории.

Главный редакционный вывод: заявленные в презентациях метрики следует приписывать авторам и сопровождать методикой, выборкой и условиями эксперимента. Исторические кейсы Safari не описывают актуальное состояние исправленных систем. Недоступные части не следует заполнять предположениями.

1. Объём и метод

В корпус включены: **Сырьё.pdf**, **nemesis.pdf**, **rework_atlas.pdf**, **иб-2025-2026.pdf**, **safari_sandbox_escape.pdf** и **Bytecode-Jiu-Jitsu-Black-Hat-USA-2024.pdf**. Первые четыре — материалы каталога; последние два добавлены отдельно и имеют собственные разборы.

Метод: анализ локальных текстовых извлечений, рендер всех страниц в контакт-листы и визуальная проверка композиции/палитры/типов графики; фиксация статуса доступности для каждого файла. Это редакционный обзор, а не независимый аудит заявленных результатов, тестирование продуктов или попиксельная проверка каждого слайда в полноразмерном режиме. Мелкие подписи, таблицы, код и экранные тексты в контакт-листах не всегда читаются; для них нужны отдельные увеличенные рендеры и, при необходимости, OCR.

2. Карточки материалов

2.1 «Сырьё решает. Планируй СЕЙЧАС»

Файл: **Сырьё.pdf**. Статус: текстовая структура извлечена; визуально просмотрены контакт-листы всех 18 PDF-страниц. Извлечённая структура содержит 17 содержательных частей: обложка, контекст и проблема, цель и задачи, аналоги, путь пользователя, сравнение моделей, тестирование, инструменты, ход работы, интерфейс, результаты, затраты/рынок, планы, команда и источники. Внутренняя нумерация отдельных страниц, похоже, сбита: после страницы «10 / ход работы» следует слайд с подписью «09»; здесь номера ссылок ниже указаны по PDF.

Презентация ведёт от проблемы планирования сырья в химическом производстве к концепции цифровой поддержки технолога на базе LLM и вызова инструментов, затем к тестированию, результатам и дальнейшему развитию. В тексте названы BFSL, τ^2 -bench, Task Success Rate и Tool Selection Accuracy; авторы указывают, среди прочего, 97,12% Tool Selection Accuracy, 87,36% Task Success Rate и задержку 5,67 секунды. В разных локальных пересказах значение точности маршрутизации расходится; без сверки исходного слайда его не приводим. Цифры не проверялись независимо и требуют раскрытия методики, выборки и условий теста.

В извлечённом тексте заметны опечатки, неоднородные англоязычные термины и обрывки таблиц. Геометрию графиков, подписи, читаемость, шрифты и палитру нельзя надёжно оценить по одному текстовому слою.

Кратко для сайта: проект о цифровой поддержке планирования сырья для химического производства. Материал описывает производственную задачу, путь технолога, использование LLM и инструментов, тестирование и возможное масштабирование. Показатели представлены как заявления авторов и требуют проверки по методике и первичным данным.

2.2 NEMESIS — Red Team Operations Platform

Файл: **nemesis.pdf**, 9 PDF-страниц. Контакт-листы всех 9 страниц просмотрены; текстовый/содержательный разбор остаётся ограниченным, поэтому функциональность и результаты платформы не выводятся из мелких надписей.

По всей деке наблюдаются ярко-жёлтый фон, чёрные геометрические блоки и красно-оранжевые акценты. После обложки идут метрики, роли, таблица, карточки задач и архитектурные схемы (PDF 2–7); страницы 8–9 выглядят более абстрактными/иллюстративными. Контрастные цветовые решения сильны, но фоновая кодовая текстура и мелкие подписи могут мешать чтению (особенно 3–7). Подробная визуальная фиксация — в **visual_review_20261018.md**.

Кратко для сайта: визуальный стиль NEMESIS заметен по жёлто-чёрной палитре и геометрическим блокам. Точное содержание мелкого текста и заявления об эффективности требуют проверки на полноразмерных страницах.

2.3 «Атлас. Профессии системы безопасности»

Файл: **rework_atlas.pdf**, 14 PDF-страниц. Контакт-листы всех страниц просмотрены; содержательные детали остаются ограничены мелким текстом.

Визуальная система — белый фон, чёрно-серый текст, много свободного пространства и приглушённые цветные блок-схемы/таблицы. В середине чередуются воронка и сравнения, дорожки задач, схемы/таблицы характеристик, а затем тёмные скриншоты интерфейса (PDF 2–13); обложка и финал повторяют образ стопки документов (1, 14). Сетка спокойная, но таблицы и подписи на страницах 6, 8–9, 12–13 малы; скриншоты 10–11 плохо читаются на миниатюрах. Подробности — в **visual_review_20261018.md**.

Кратко для сайта: «Атлас» использует сдержанный редакционный стиль с большим количеством воздуха и визуально чередует схемы и интерфейсные экраны. Мелкие подписи не расшифровывались.

2.4 «ИБ · 2025—2026»

Файл: **иб-2025-2026.pdf**, 13 PDF-страниц. Текстовое чтение прежним инструментом ограничено размером файла (52 466 004 байта); визуальный контакт-лист отрендерен и просмотрен целиком.

Виден повторяющийся серо-оливковый фон и звёздно-месячный графический мотив. Структура идёт от метрик/цели к дорожной карте, стеку и схеме алгоритма, затем к тёмным интерфейсным скриншотам и ресурсам (PDF 2–12); страница 13 собрана преимущественно из логотипов. Контакт-лист не позволяет точно прочесть таблицу 4, метрики, подписи схем и UI-текст на 8–10. Подробности — в **visual_review_20261018.md**.

Кратко для сайта: визуально презентация посвящена проекту ECLIPSE и сочетает схемы, метрики, таблицы и экранные макеты. Утверждения и мелкие детали пока не пересказываются без полноразмерной проверки.

2.5 Cross-Site Escape: Pwning macOS Safari Sandbox the Unusual Way

Файл: **safari_sandbox_escape.pdf**. Доклад Zhi Zhou, Black Hat Europe 2020; локальная копия скачана со страницы Speaker Deck. Статус: текстовый разбор и визуальный просмотр контакт-листов всех 62 страниц выполнены. Это исторические кейсы старых версий OS X/macOS, вплоть до Catalina 10.15.2, а не характеристика современных исправленных систем.

Визуально дек преимущественно чёрный, с белыми заголовками и оранжево-жёлто-голубыми акцентами. Разделительные тезисы чередуются с кодом, схемами IPC/URL и скриншотами; цепочка Dictionary раскрывается по последовательным состояниям (PDF 49–58). Пошаговое наращивание схемы помогает вести сложную историю, но мелкий код/серые подписи и разреженные промежуточные кадры могут мешать самостоятельному чтению. Подробные номера и оговорки см. **visual_review_20261018.md**.

Доклад рассматривает переход от JavaScript в Safari/WebContent к более привилегированным компонентам посредством IPC, URL-схем и legacy WebView. Среди разобранных примеров — раннее обращение к CFPreferences до включения sandbox и связанная с ним проблема порядка/кэширования; сценарий Dashboard и IPC к Dock; доверенная схема HelpViewer; подмена словарного ресурса с участием MobileAssets и Dictionary. В одном из описанных сценариев содержимое загружалось в legacy WebView, а делегат открывал ссылку на локальное приложение через системный механизм запуска. Отдельно важно, что выход из sandbox и выполнение native code — не одно и то же: некоторые этапы требовали дополнительной уязвимости, а кейс HelpViewer был частичным.

Выводы докладчика: проверять границы доверия между процессами, XPC/MIG и WebKit IPC, URL-обработчики, делегаты WebView, ранние обращения до sandbox lockdown и устаревшие компоненты — не только ошибки управления памятью. Эти наблюдения не доказывают наличие тех же уязвимостей в текущей macOS.

Кратко для сайта: исторический доклад о цепочках взаимодействия Safari, IPC и legacy-компонентов macOS, показывающий, как ошибки доверия и обработки ресурсов могут дополнять уязвимость renderer. Не переносить описанные кейсы на актуальные исправленные версии.

2.6 Bytecode Jiu-Jitsu: Choking Interpreters to Force Execution of Malicious Bytecode

Файл: **Bytecode-Jiu-Jitsu-Black-Hat-USA-2024.pdf**, 77 страниц. Авторы: Toshinori Usui, Yuto Otsuki, Ryo Kubota, Yuhei Kawakoya, Makoto Iwamura и Kanta Matsuura. Статус: текстовый разбор и визуальный просмотр контакт-листов всех 77 страниц выполнены.

Визуально повторяется тёмная шапка Black Hat над белыми слайдами; охристо-оранжевые заголовки сочетаются с цветными блок-схемами и моноширинным кодом. Механизм объясняется последовательным наращиванием схем памяти (PDF 10–15, 34–55); чек-листы возвращаются с меняющимся выделением, а фотографии дзюдо разбирают технические разделы. Это помогает рассказывать сложный процесс устно, но без докладчика некоторые кадры выглядят повторными; код и подписи малы в миниатюрах. Полный список страниц — в **visual_review_20261018.md**.

Авторы описывают инъекцию вредоносного байткода в уже работающий процесс-интерпретатор. Идея использует среду исполнения интерпретатора, а не классическую инъекцию машинного кода с исполняемой страницей и новым потоком. Метод включает получение образца байткода и таблиц символов, автоматизированное исследование структур памяти, определение счётчика виртуальной программы (VPC), поиск связанных объектов и таблиц, запись подготовленных структур и перенаправление VPC на внедрённый байткод.

В презентации показаны эксперименты с Python, Lua и VBScript. Для оценки обнаружения сравнивались нагрузка с бесконечным циклом и загрузчик. По таблице авторов, антивирусы обнаружили оба варианта в 9 случаях из 72; sandbox/EDR не обнаружили вариант с циклом, но обнаружили загрузчик; применённые средства memory forensics не обнаружили ни один вариант. Эти цифры относятся к тестам авторов, конкретным инструментам, конфигурациям и образцам; это не независимое или универсальное сравнение защитных продуктов.

Авторы предлагают защитникам учитывать байткод, мониторить записи в память процессов-интерпретаторов, улучшать анализаторы и ограничивать права записи. Кратко для сайта: доклад показывает исследовательский способ направить работающий интерпретатор на внедрённый байткод и обсуждает ограничения сигнатурного обнаружения; метрики обнаружения атрибутированы авторам.

3. Сопоставимые наблюдения

1. Ясное обещание на титуле: NEMESIS сразу поясняет назначение подзаголовком, а «Сырьё решает» — слоганом «Планируй СЕЙЧАС». Это наблюдение касается только доступных титулов.
2. Сюжет «проблема → решение → проверка → следующий шаг» наиболее ясно подтверждён в текстовой структуре «Сырьё решает», но не должен автоматически приписываться всему корпусу.
3. Для технических докладов полезно показывать цепочку по шагам и отдельно обозначать предпосылки, границы доверия, достигнутый эффект и дополнительные условия. Обзор Safari иллюстрирует важность различать выход из sandbox и native code execution.
4. Числа следует сопровождать определением метрики, методикой, объёмом и составом выборки, версиями и конфигурациями инструментов. Если проверки не было, писать «по данным авторов».
5. По контакт-листам видны заметно разные визуальные системы: жёлто-чёрные геометрические блоки NEMESIS, сдержанная бело-серая верстка «Атласа», серо-оливковая палитра ECLIPSE и чёрный контрастный стиль Safari; подробности привязаны к PDF-страницам в отдельном визуальном обзоре. Контакт-листы позволяют сравнить композицию и плотность, но не проверить чтение мелкого текста.

4. Практические выводы для подготовки презентаций и обзоров

- Строить повествование от конкретной задачи к предлагаемому решению, затем к воспроизводимой проверке и ограничениям.
- На каждом графике и в каждой метрике давать единицы измерения, базовую линию, размер выборки, методику и ссылку на первичные данные.
- Разделять демонстрацию технической цепочки и выводы о её применимости: явно указывать версии, конфигурации, предпосылки и необходимые дополнительные уязвимости.
- При редакционном обзоре разделять наблюдаемый факт, заявление авторов и собственную рекомендацию.
- Маркировать неполно прочитанные источники и не придумывать описание отсутствующих страниц.

5. Ограничения и пробелы

Визуально просмотрены контакт-листы всех 193 PDF-страниц, но это обзор общего строя, а не проверка каждой страницы в масштабе чтения. Мелкие подписи, метрики, таблицы, код и тексты внутри интерфейсных скриншотов могут быть неразборчивы; для спорных мест нужны увеличенные рендеры и/или OCR. Для трёх коротких презентаций текстовый разбор остаётся ограниченным, даже несмотря на полный визуальный охват. Результаты Safari и Bytecode атрибутированы авторам и не перепроверены независимым тестированием. Полный перечень визуальных наблюдений по PDF-страницам вынесен в **visual_review_20261018.md**.

6. Реестр исходников и источников

Локальный файл	Статус разбора	Оговорка
Сырьё.pdf	Текстовая структура и визуальный обзор 18 страниц	Метрики — заявления авторов; мелкие детали не проверялись полноразмерно
nemesis.pdf	Визуальный обзор 9 страниц; текстовый разбор ограничен	Функции/результаты не выводятся из мелких надписей
rework_atlas.pdf	Визуальный обзор 14 страниц; текстовый разбор ограничен	Схемы/таблицы видны, мелкие подписи не расшифрованы

Локальный файл	Статус разбора	Оговорка
иб-2025-2026.pdf	Визуальный обзор 13 страниц; текстовое извлечение ограничено	Метрики и подписи требуют полноразмерной проверки
safari_sandbox_escape.pdf	Текстовый разбор и визуальный обзор 62 страниц	Исторические кейсы; не описание актуального состояния macOS
Bytecode-Jiu-Jitsu-Black-Hat-USA-2024.pdf	Текстовый разбор и визуальный обзор 77 страниц	Экспериментальные результаты — по данным авторов

Связанные локальные разборы: **presentation_analysis.md**, **safari_sandbox_escape_analysis.md**, **bytecode_jiu_jitsu_analysis.md**, а также редакционная основа **report_structure.md**.

Источники дополнительных докладов:

- Cross-Site Escape, Speaker Deck: <https://speakerdeck.com/chichou/cross-site-escape-pwning-macos-safari-sandbox-the-unusual-way>
- Прямая копия PDF Safari: <https://files.speakerdeck.com/presentations/8d3d8e156509429599234b772579d698/eu-20-Zhou-Cross-Site-Escape-Pwning-MacOS-Safari-Sandbox-The-Unusual-Way.pdf>
- Bytecode Jiu-Jitsu, PDF: https://paper.vulsee.com/Black%20Hat%20USA%202024%20slides/Toshinori%20Usui%20%26%20Yuto%20Otsuki%20%26%20Ryo%20Kubota%20%26%20Yuhei%20Kawakoya%20%26%20Makoto%20Iwamura%20%26%20Kanta%20Matsuura_Bytecode%20Jiu-Jitsu%20Choking%20Interpreters%20to%20Force%20Execution%20of%20Malicious%20Bytecode.pdf
- NTT, описание исследования: <https://group.ntt/en/topics/2024/10/16/cyberattack.html>
- Black Hat USA 2024, запись выступления: <https://www.youtube.com/watch?v=5fs9ntKOYW0>

Редакционная основа подготовлена 18 октября 2026 года на основе материалов, находившихся в проектной папке на эту дату.