КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

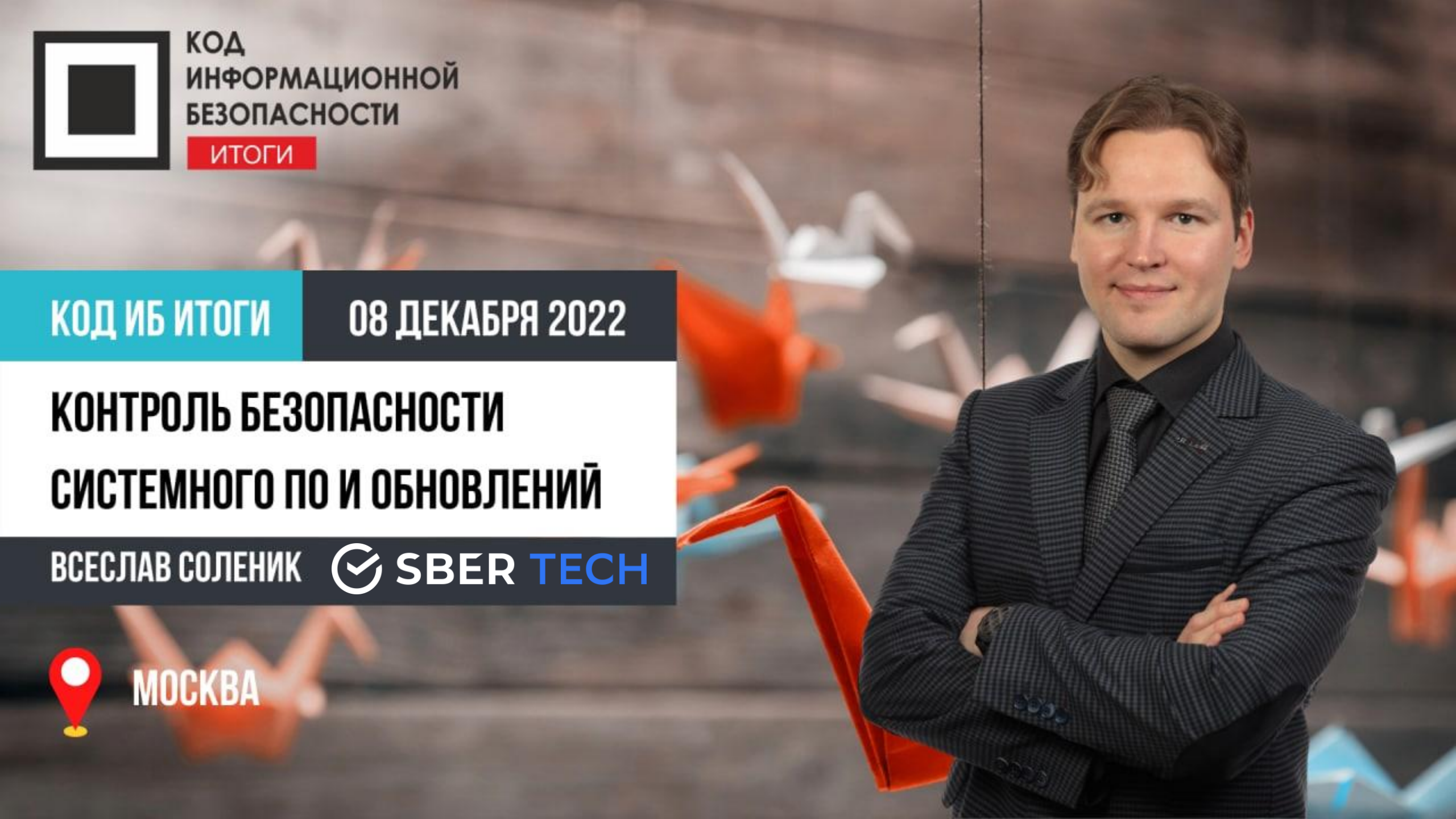
ИТОГИ

КОД ИБ ИТОГИ | 08 ДЕКАБРЯ 2022

КОНТРОЛЬ БЕЗОПАСНОСТИ СИСТЕМНОГО ПО И ОБНОВЛЕНИЙ

ВСЕСЛАВ СОЛЕНИК SBER TECH

МОСКВА



Обновление ПО. Контекст

Было

- Доверие вендорам, установка обновлений без ограничений
- Проверка freeware и open source (FOSS) на угрозы

Стало

- Обновление = риск привнести НДВ → внедрения в ПРОМ по решению
- Проприетарное ПО стало нести риски ИБ
- Каналы поставки коммерческого ПО перестали быть надежными

Проблематика: отсутствует покрытие проверками на риски **всех** видов ПО

Задача: создать Лабораторию исследования ПО

Основные риски

- Утечка персональных данных пользователя
- Угроза утечек корпоративных данных
- Атака со стороны злоумышленников
- Угроза IT-структуре компании
- Корпоративные и репутационные риски
- Угроза комплектующим для корпоративных ПК и серверному оборудованию
- Распространение политизированного или запрещенного контента
- Атака по политическим или идеологическим причинам

Типы легитимного ПО, несущего потенциальную угрозу

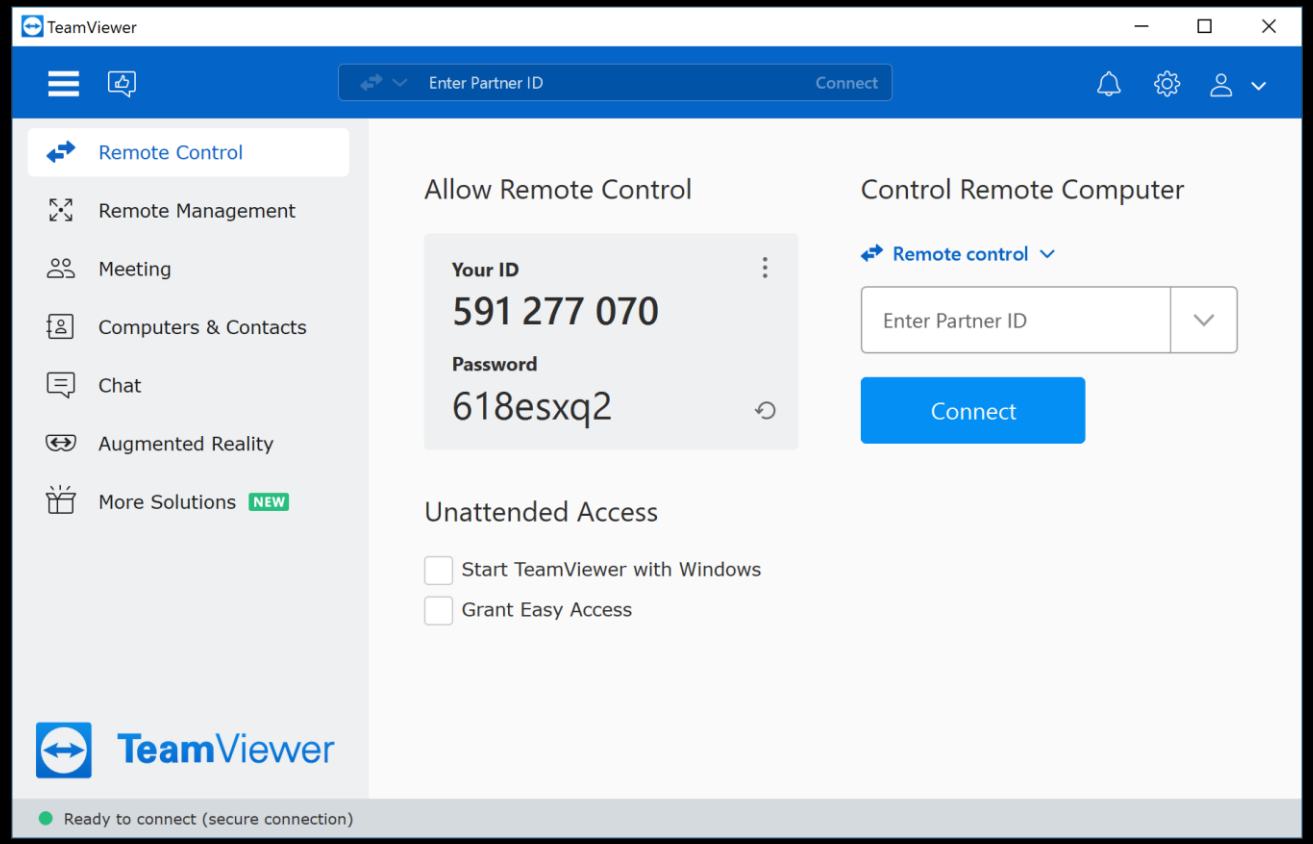
- Утилиты удаленного администрирования
- IRC-клиенты
- Программы автодозвона
- Загрузка файлов/Torrent-клиенты
- ПО мониторинга активности компьютера и комплектующих
- Менеджеры паролей
- FTP-клиенты
- VPN и Proxy
- Telnet

Вредоносное ПО

- Программы-вымогатели (Ransomware)
- Программы-шпионы (Spyware)
- Похищение данных пользователя (Infostealer, Keylogger, Fraudware)
- Интеграция злоумышленника в систему компании (Backdoor, Botnet, Miner)
- Помехи в работе пользователя (AdWare, Zip-бомба)

В любом загруженном из сети ПО могут содержаться элементы вредоносных программ, добавленные злоумышленниками в код оригинальной программы.

Пример: TeamViewer

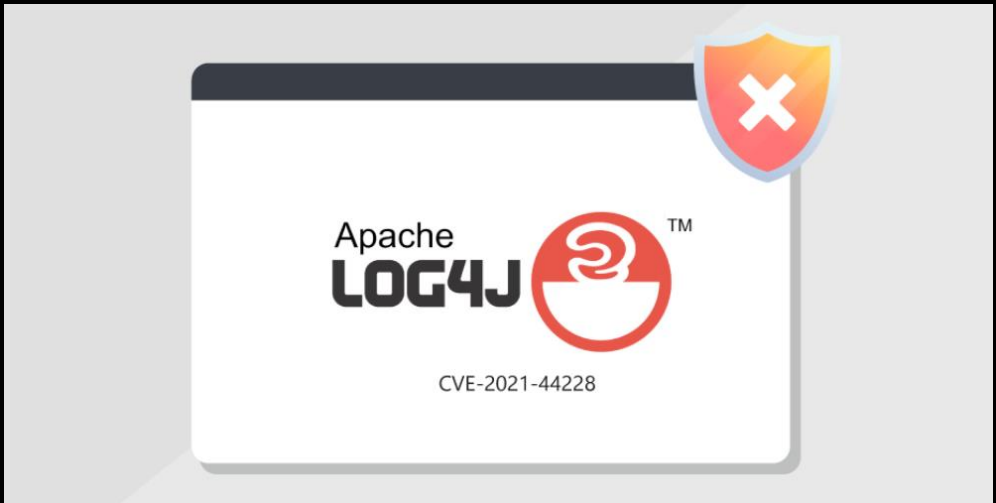


TeamViewer – программа для удаленного администрирования рабочего стола.

Может угрожать как отдельному пользователю, так и компании. Позволяет случайно или злонамеренно передать полный доступ к управлению персональным компьютером и всеми доступными ему функциями (доступ на серверы, доступ к базам данных, доступ к корпоративным файлам и документам, составляющих коммерческую тайну).

Помимо этого программа несет в себе ряд уязвимостей. Например, подмена msimg32.dll, которая приводит к скрытию факта работы TeamViewer от пользователя.

Log4j, CVE-2021-44228



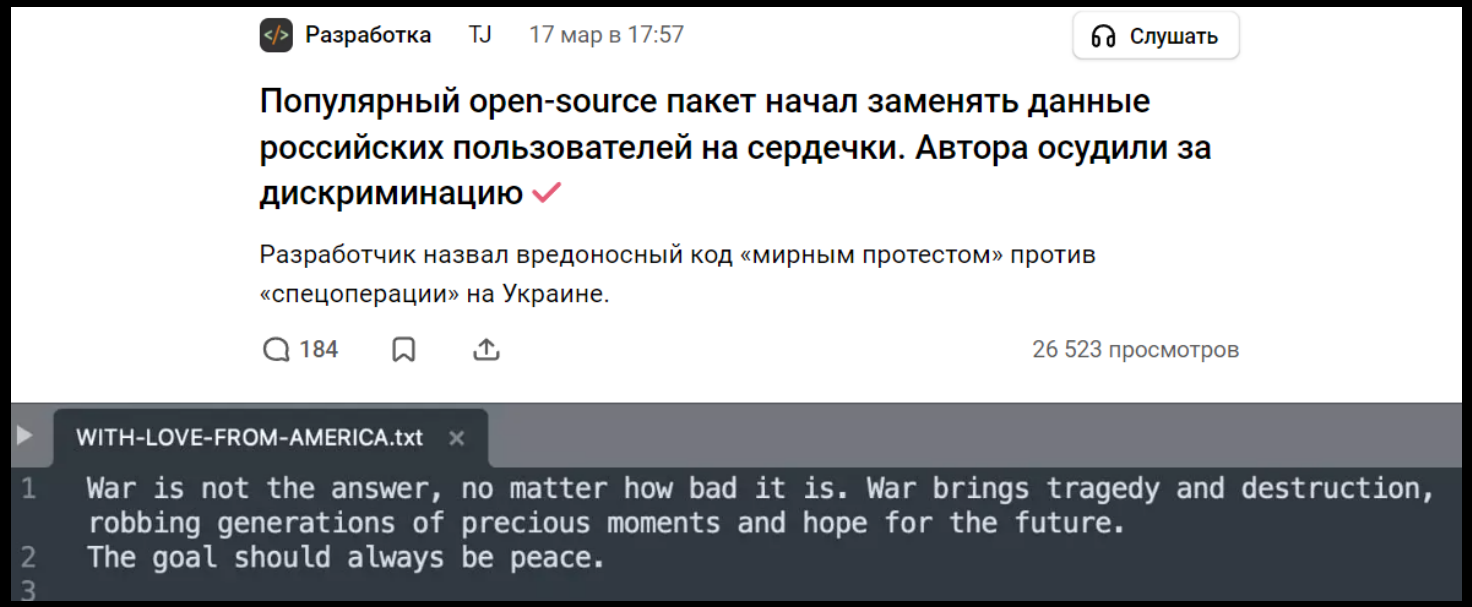
Apache Log4j – библиотека журналирования ошибок. Используется во многих Java-приложениях.

В 2021 году для Apache Log4j было обнаружено множество уязвимостей нулевого дня.

Самая известная – CVE-2021-44228 или Log4Shell. Это уязвимость типа RCE (Remote Code Execution или удаленное выполнение кода), которой присвоен 10-й уровень опасности из 10 по CVSS-стандарту.

Проверка на наличие этой уязвимости в серверном ПО – критически важная задача для любой крупной компании.

Угрозы после 24 февраля

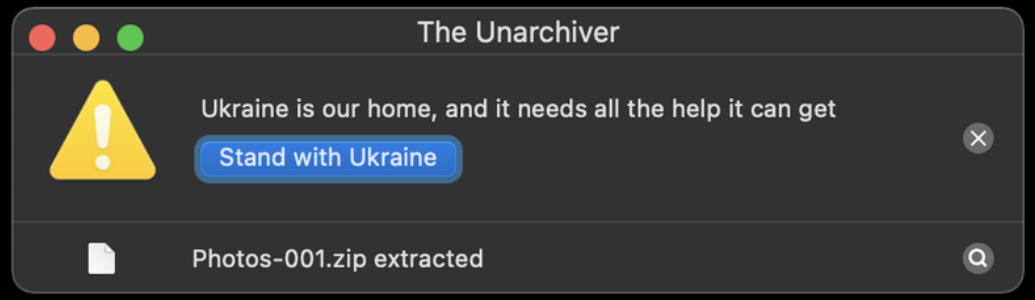


Сделать легитимное ПО опасным могут сами разработчики по политическим или идеологическим причинам.

После 24 февраля в код некоторых приложений были встроены политические лозунги, высказывания и пропагандистские баннеры. Их показывали только пользователям из России.

Другой пример — атаки WITH-LOVE-FROM-AMERICA. Разработчик пакета популярных open source библиотек встроил в свое ПО аналог Ransomware. Он шифровал и уничтожал все файлы на системе и запускался только на машинах с российскими IP-адресами.

The Unarchiver



Одним из примеров политизированного ПО стал исследованный в нашей лаборатории “The Unarchiver” – разработанный компанией MacPaw распаковщик архивов.

В него был встроен функционал уведомлений, управляемых с серверов разработчиков. Этот функционал использовался для рассылки политических лозунгов и сообщений.

Подход к безопасности ПО

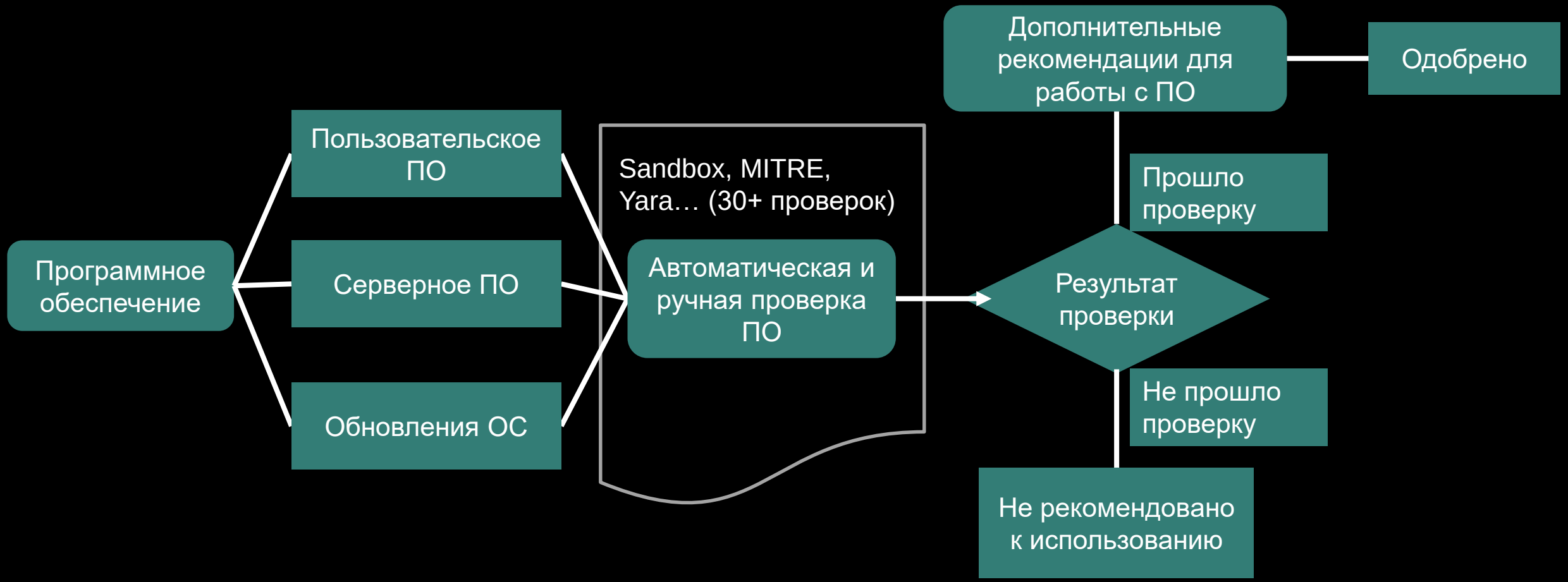
Сегодня каждая крупная компания должна проверять **ВСЕ** устанавливаемые программные продукты как для рабочих машин, так и для серверного оборудования.

На какие уязвимости обращать внимание:

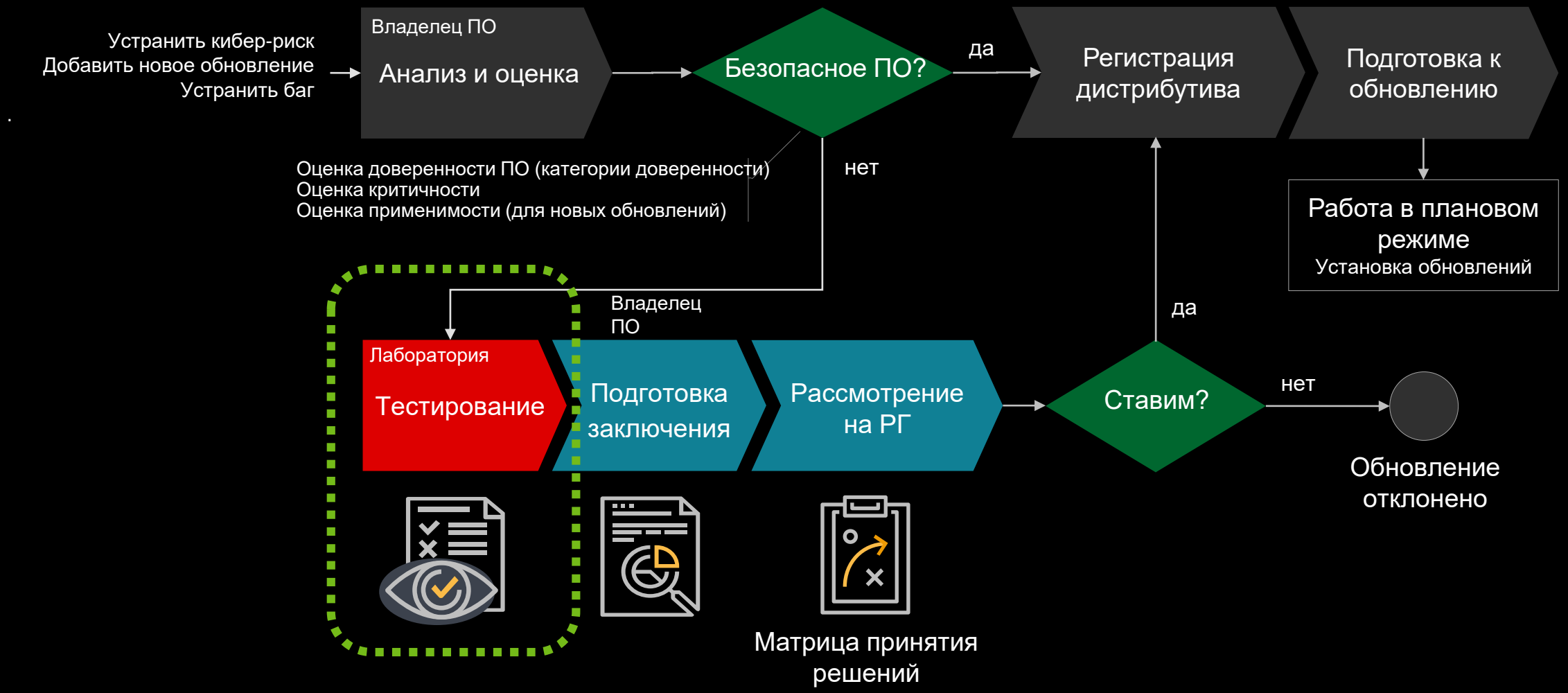
- Общие уязвимости класса исследуемого ПО
- Известные CVE или CWE для исследуемого ПО
- Специфичные для компании уязвимости
- Политические или идеологические угрозы
- Наличие APT(advanced persistent threat – постоянной серьезной угрозы) для компании или индустрии в целом

Наша лаборатория проводит подобные исследования, формирует отчет об угрозе для ПО и общие рекомендации для работы.

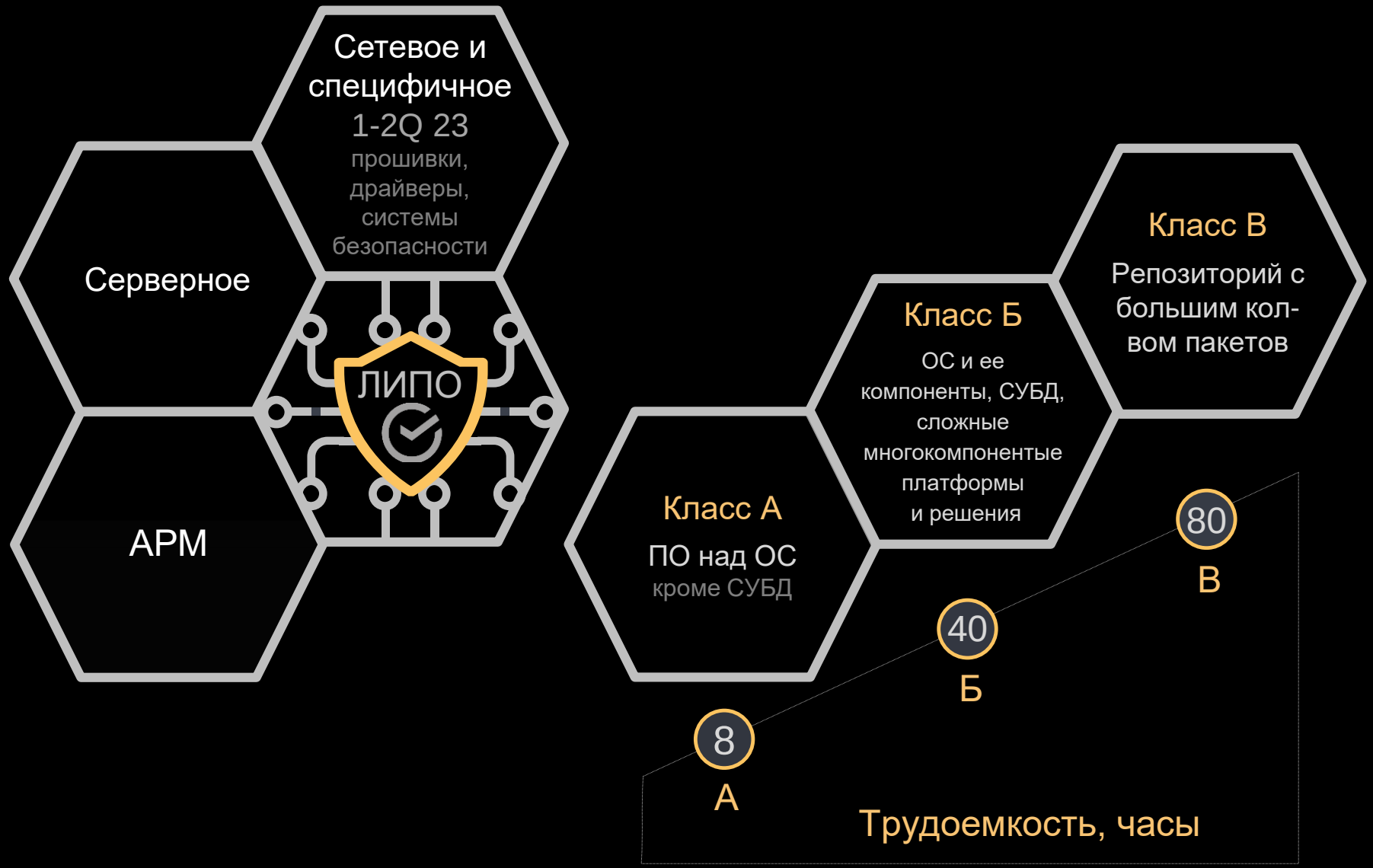
Этапы проверки



Процесс исследования ПО/СПО



Подходы к исследованию ПО



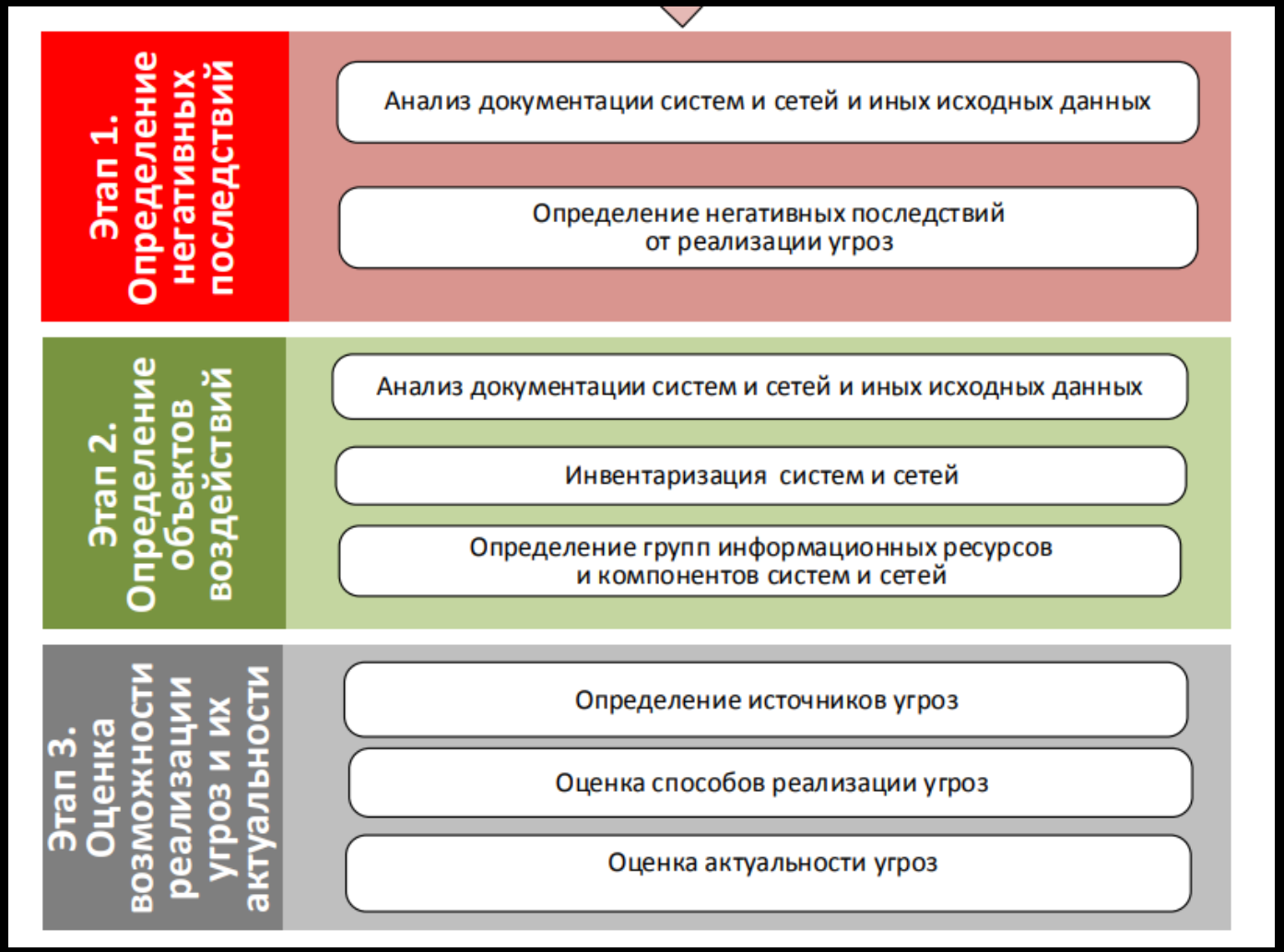
Типы дистрибутивов для исследования

<table>
<tr><th>Класс А
ПО над ОС
кроме СУБД</th><th>Класс Б
ОС и ее компоненты, СУБД, сложные многокомпонентные платформы и решения</th><th>Класс В
Репозиторий с большим кол-вом пакетов</th></tr>
<tr><td colspan="2">Динамическое исследование дистрибутива*:
1. Фиксация и анализ трафика, генерируемого в процессе инсталляции.
2. Фиксация и анализ изменений, вносимых в процессе инсталляции.
3. Запуск ПО, снятие метрик в процессе работы, фиксация и анализ трафика в процессе запуска и работы ПО.
4. Проверка работы ОС и ПО при изменении системного времени и даты.
5. Поиск и анализ НДВ и декларированного потенциально опасного функционала.</td><td></td></tr>
<tr><td colspan="2">Статическое исследование дистрибутива:
1. Сканирование на CVE** и анализ общедоступной информации по уязвимостям и их эксплуатации.
2. Сканирование на наличие ВПО.
3. Анализ зависимостей (OSS, при доступности информации) и уязвимостей в них**.
4. Анализ информации из открытых источников о дистрибутиве, наличии в дистрибутиве ошибок и уязвимостей, НДВ и функционала, противоречащего требованиям ИБ.
5. Анализ репутации производителя дистрибутива, анализ негативной истории разработки производителя.</td><td></td></tr>
<tr><td></td><td></td><td>Статическое исследование репозитория:
1. Сканирование на CVE** и анализ информации по уязвимостям и их эксплуатации.
2. Сканирование на наличие ВПО.
3. Фиксация и анализ изменений в файловой системе при массовой установке пакетов.</td></tr>
</table>

*динамическое исследование дистрибутивов только для платформы Intel x86. для RISC платформ (IBM DB2, AIX, Solaris) только статическое исследование

**не проводится поиск и анализ уязвимостей нулевого дня

Требование и методология ФСТЭК (от 28.10.2022г.)



Лаборатория исследования ПО: преимущества

1. Митигация рисков ИБ

Программная инфраструктура становится более контролируемой средой, любое стороннее ПО проверяется перед публикацией

3. Рост доверия к обновлениям

Для конечного потребителя обновления должны снова стать источником надежности

2. Анализ каналов поставки

Необходимо отсечь ненадежные и скомпрометированные каналы поставки ПО

Результаты нашей работы в 2022 году

Всего за 2022 год лаборатория провела почти 4000 проверок различного ПО и их обновлений.

Из них:

- ✓ 2500+ – пользовательского
- ✓ 1000+ – серверного
- ✓ 300+ – обновления ОС

Было отклонено 4 дистрибутива по причинам политизированности вендора, либо умышленной компрометации дистрибутивов ПО.
Более 350 дистрибутивов были отклонены как содержащие в себе критические уязвимости.