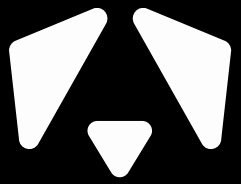


ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Практики безопасной разработки по РС БР ИББС-2.6-2014

Михаил Богатырев, руководитель направления

Доверие — состояние уверенности в том, что АБС соответствует установленным для нее требованиям к обеспечению ИБ.

Из РС БР ИББС-2.6-2014

Свидетельства доверия

- регламенты, используемые для организации деятельности по обеспечению ИБ на этапах жизненного цикла АБС

- документированные результаты выполнения деятельности по обеспечению ИБ на этапах жизненного цикла АБС

Из РС БР ИББС-2.6-2014

Стадии жизненного цикла

1) разработка технического задания (ТЗ);
2) проектирование;
3) создание и тестирование;
4) приемка и ввод в действие;
5) эксплуатация;
6) сопровождение и модернизация;
7) снятие с эксплуатации.

Из РС БР ИББС-2.6-2014

Работы независимого эксперта

- выполняются один раз и требуют нишевой экспертизы
- выполняемые раз в год, требующие особых инструментов и навыков
- которые *РС БР ИББС-2.6-2014* напрямую рекомендует с участием независимого эксперта

Разработка (ТЗ), проектирование

7.6. Функциональные требования ЧТЗ подсистемы ИБ АБС рекомендуется рассматривать в качестве основного документа, на соответствие которому оцениваются свидетельства доверия, формируемые на последующих стадиях жизненного цикла АБС.

Из РС БР ИББС-2.6-2014

Независимый эксперт

- Разрабатывает модели угроз и нарушителя.
- Анализирует ЧТЗ подсистемы ИБ АБС .

Свидетельство доверия № 1 – заключение о соответствии ЧТЗ подсистемы ИБ АБС требованиям и актуальным угрозам.

Создание и тестирование

8.11. В ходе предварительных испытаний АБС рекомендуется проведение независимого или совместного с разработчиком полного тестирования с целью проверки полноты и корректности реализации всех требований ЧТЗ на подсистему ИБ АСБ применительно ко всем компонентам АБС.

Из РС БР ИББС-2.6-2014

Независимый эксперт

- Проверяет защищенность среды разработки.
- Внедряет практики и инструменты анализа исходных кодов.
- Выполняет фаззинг.
- Тестирует безопасность АБС.

Свидетельство доверия № 2 – протоколы тестирования полноты и корректности требований ЧТЗ.

Приемка и ввод в действие

9.5. Дополнительно в рамках проведения опытной эксплуатации рекомендуется проведение комплексной оценки защищенности, включающей проведение:

— тестирования на проникновение;

— выявления известных уязвимостей компонентов АБС.

Из РС БР ИББС-2.6-2014

Независимый эксперт

- Проводит тестирование на проникновение.
- Выявляет известные уязвимости.

Свидетельство доверия № 3 – отчеты о тестировании на проникновение и выявлении уязвимостей.

Эксплуатация, сопровождение и модернизация

10.2. Периодичность проведения работ по оценке защищенности определяется решением организации БС РФ. Для АБС, используемых для реализации банковского платежного технологического процесса, рекомендуется проведение комплексной оценки защищенности не реже одного раза в год.

Из РС БР ИББС-2.6-2014

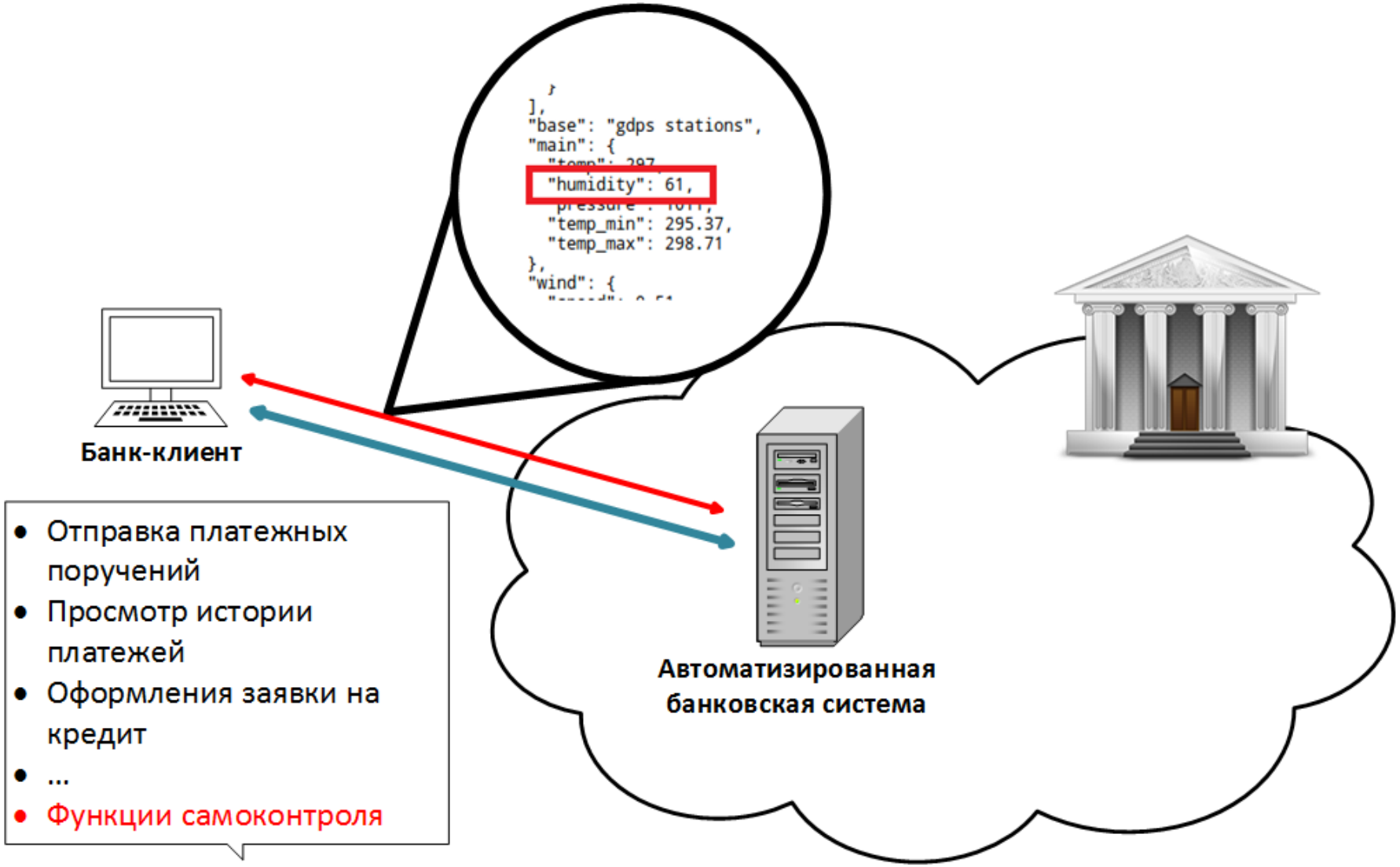
Независимый эксперт

- Проводит тестирование на проникновение.
- Выявляет известные уязвимости.
- Мониторит сообщения об уязвимостях АБС.

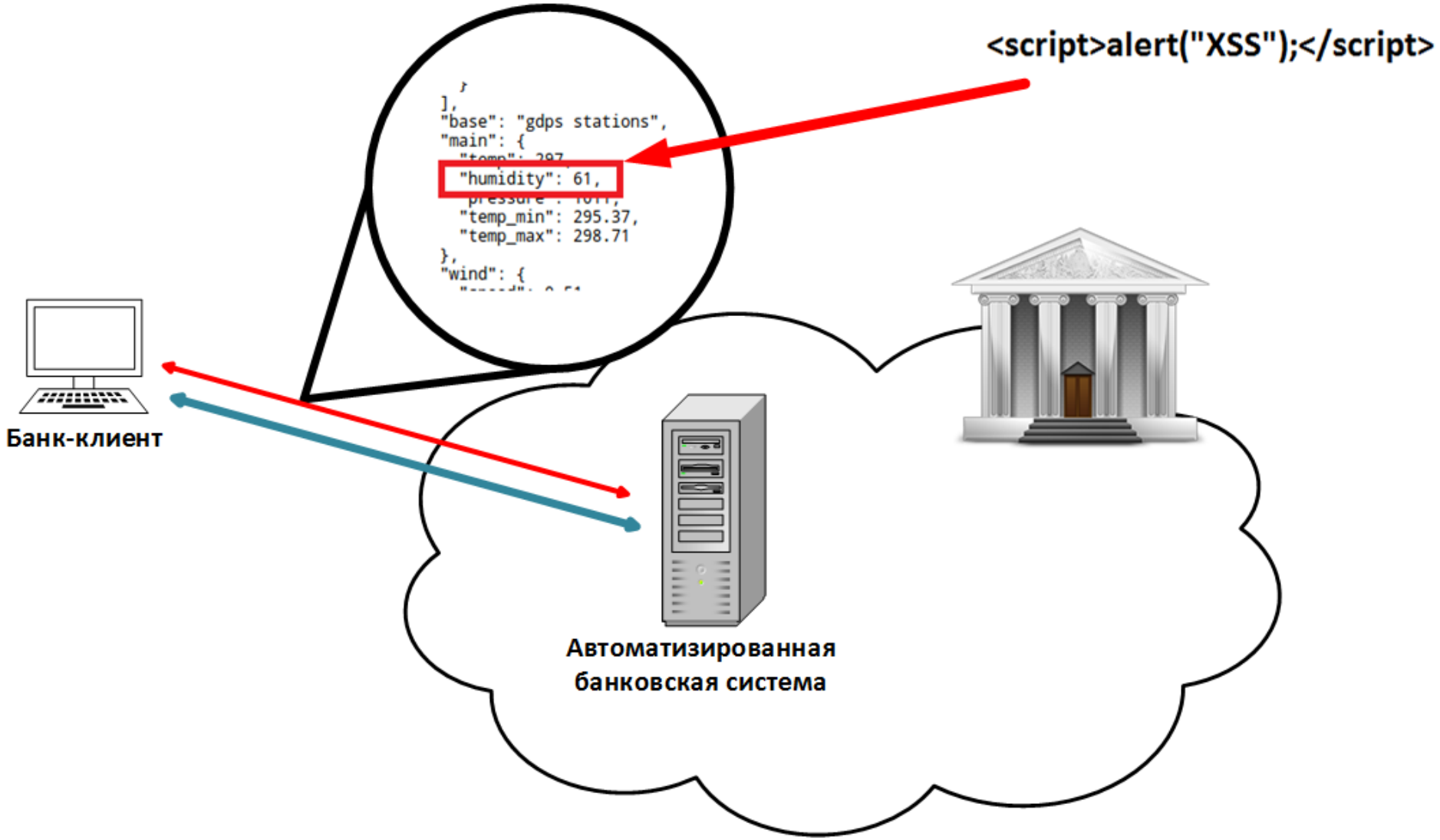
Свидетельство доверия № 4 – отчеты о тестировании на проникновение и выявлении уязвимостей.

Как мы нашли уязвимость

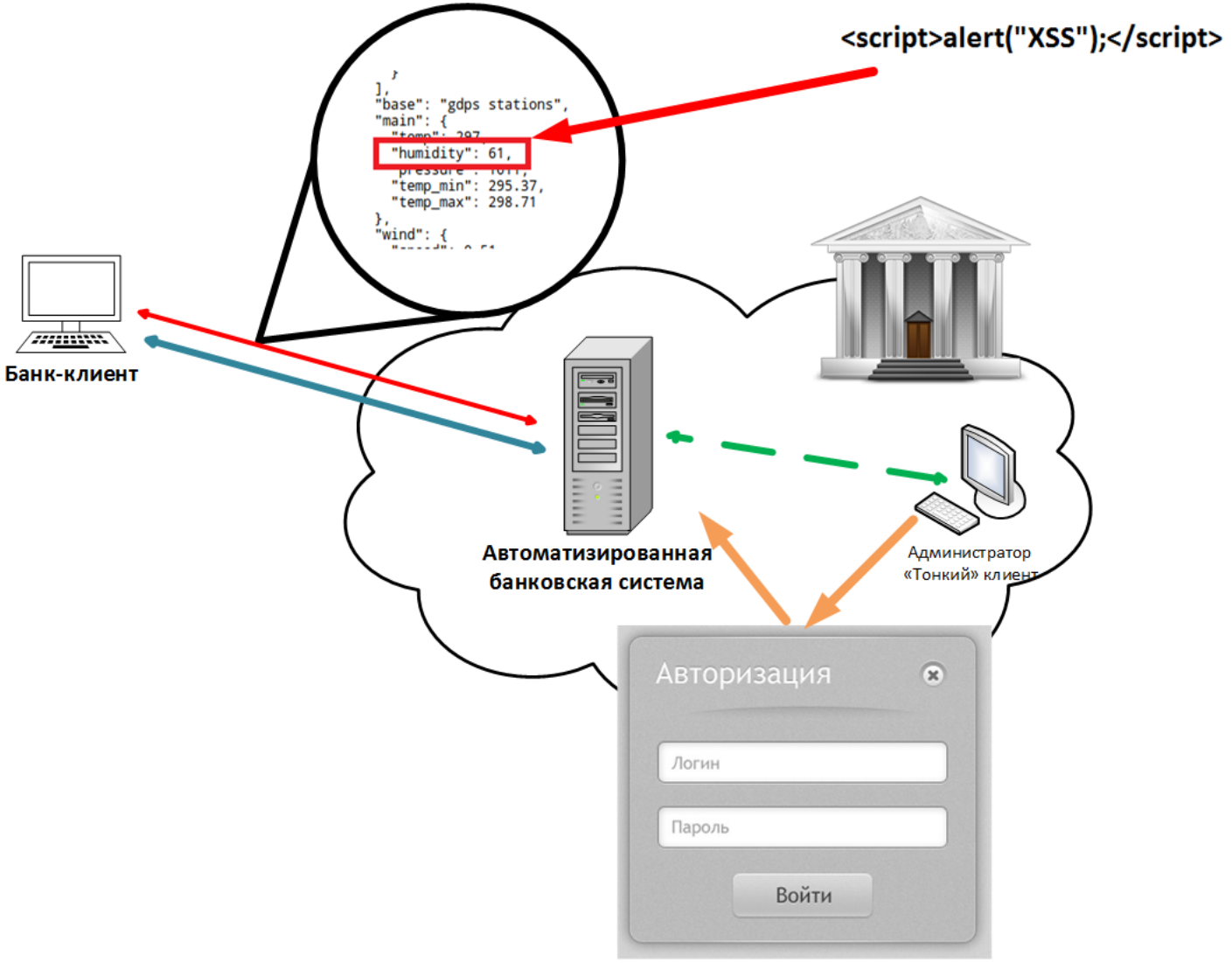
Пример из практики



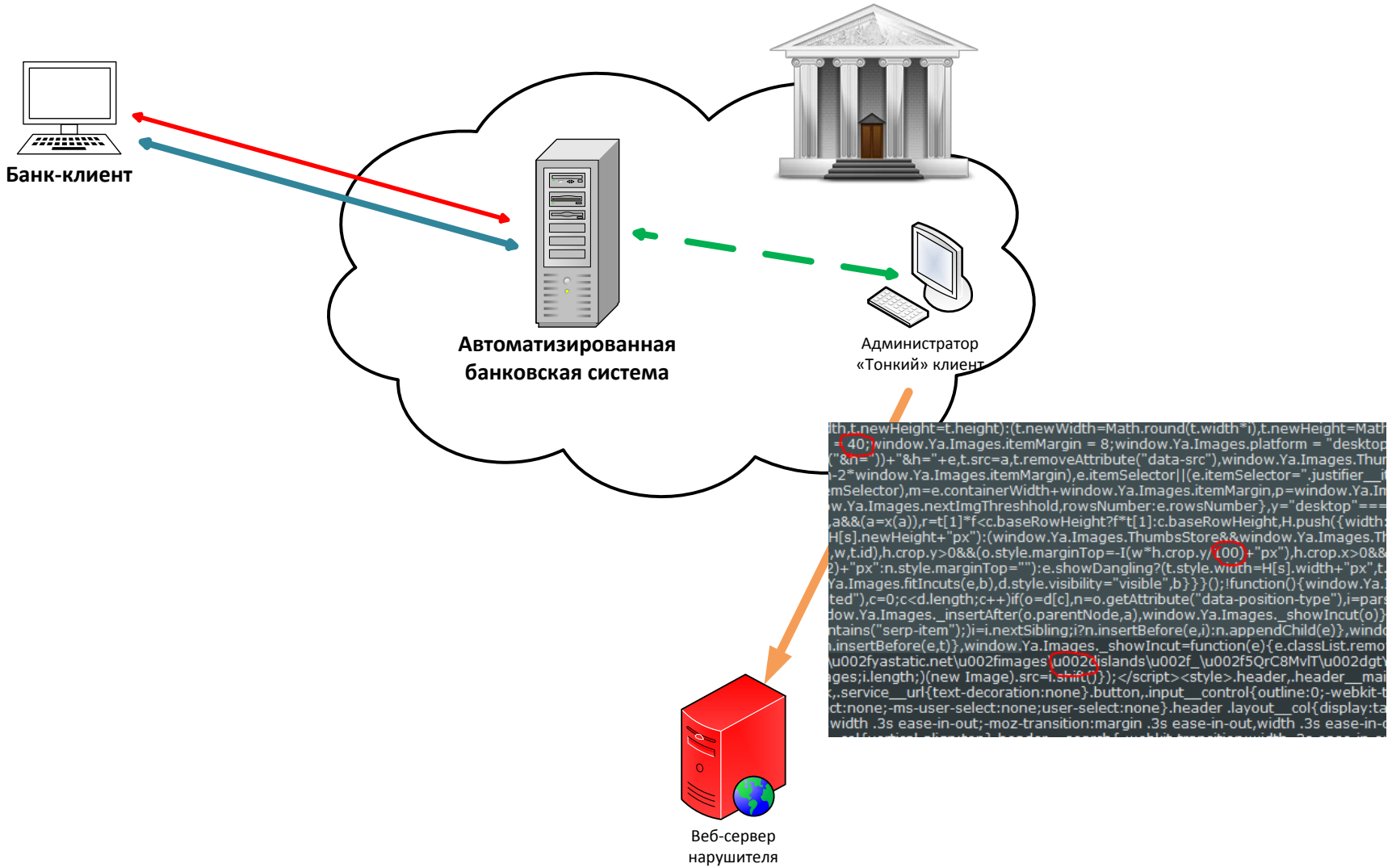
Базовый вектор



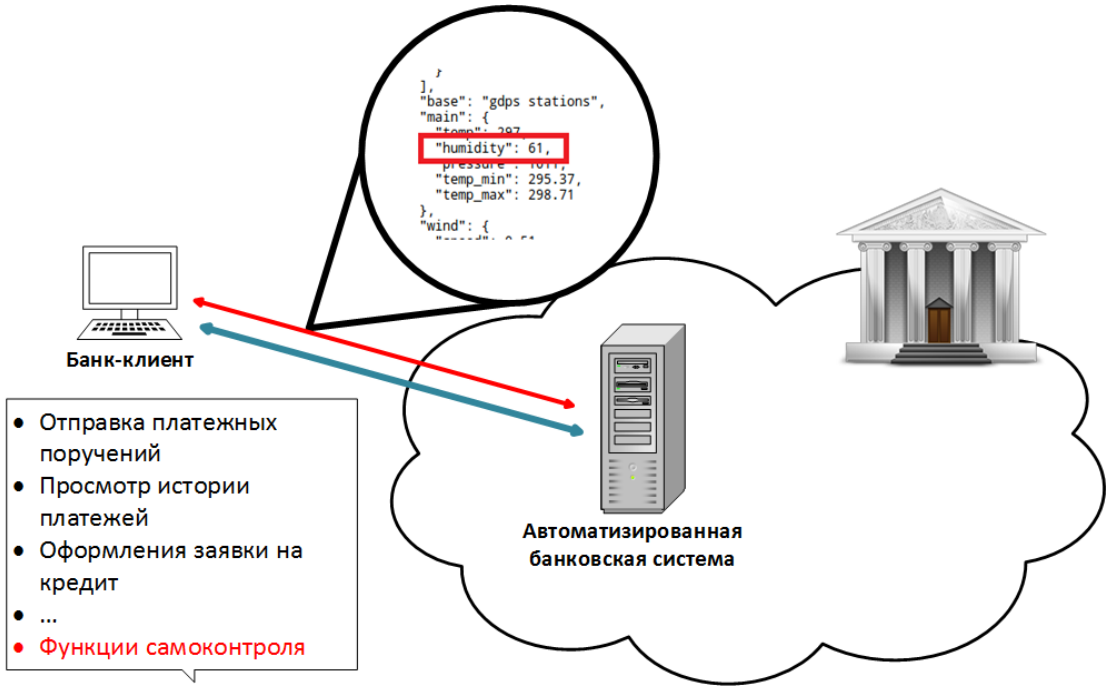
Фиктивная аутентификация



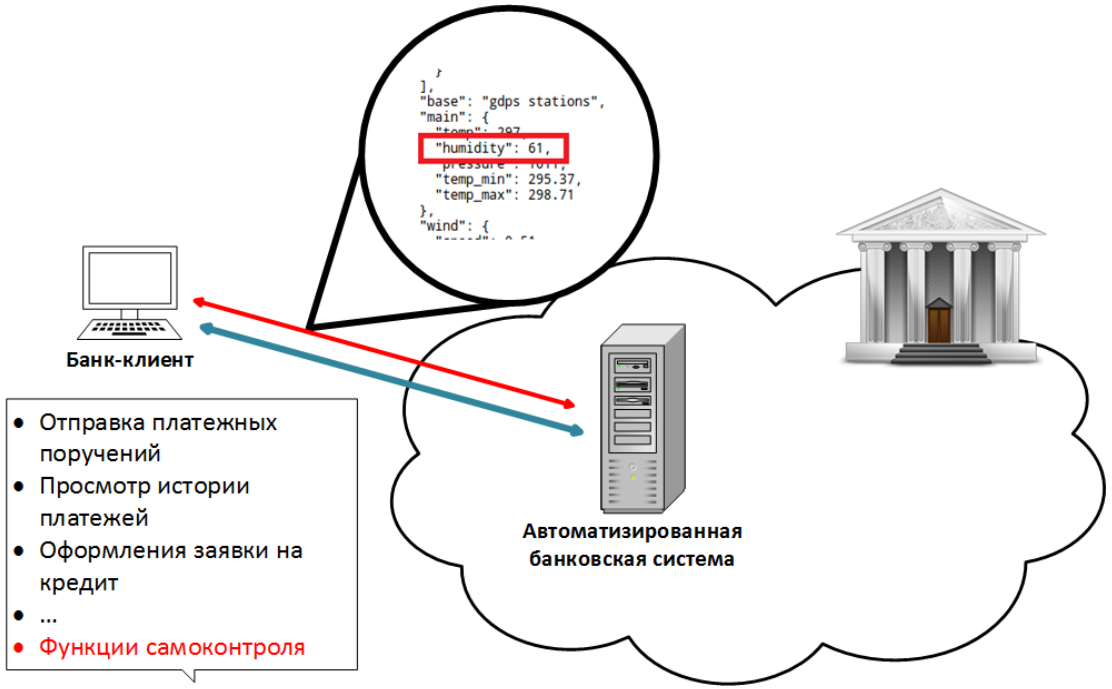
Отправка данных пользователей



Пример из практики



1) разработка технического задания (ТЗ);
2) проектирование;
3) создание и тестирование;
4) приемка и ввод в действие;
5) эксплуатация;
6) сопровождение и модернизация;
7) снятие с эксплуатации.

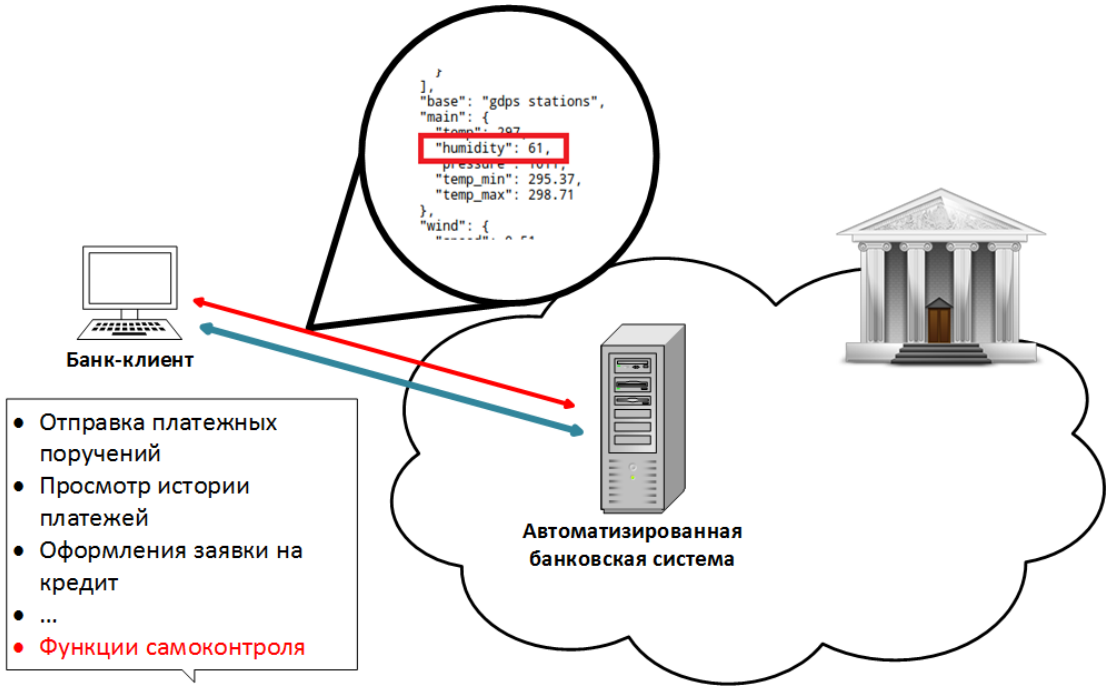


4) приемка и ввод в действие;

5) эксплуатация;

6) сопровождение и модернизация;

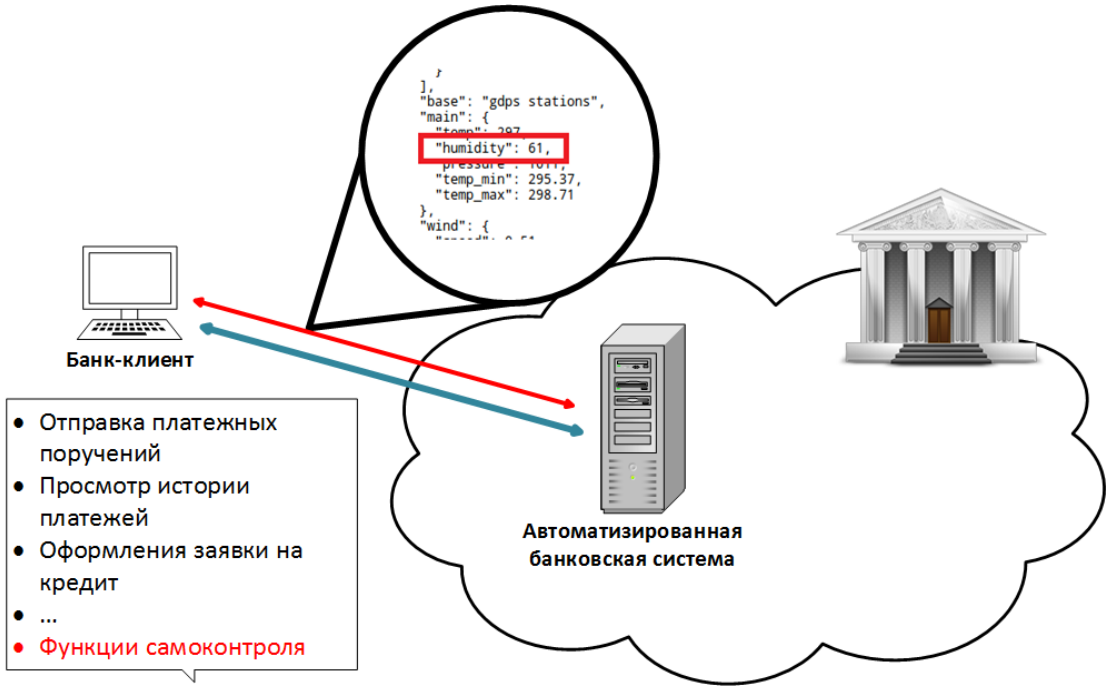
Выявление уязвимости при тестировании на проникновение.



3) создание и тестирование;

Выявление уязвимости при:

- ❑ анализе исходных кодов
- ❑ динамическом анализе кода
- ❑ тестировании на проникновение



1) разработка технического задания (ТЗ);
2) проектирование;

Предотвращение уязвимости при учете угрозы со стороны клиента

Спасибо за внимание!

Вопросы?

Михаил Богатырев

Руководитель направления

Компании «Перспективный мониторинг»

Mikhail.Bogatyrev@ amonitoring.ru