

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

0x17E на практике

Александр Пушкин

Руководитель отдела ИИТ

компании «Перспективный мониторинг»



Что это за название презентации?

0x17E -> 382

№382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»



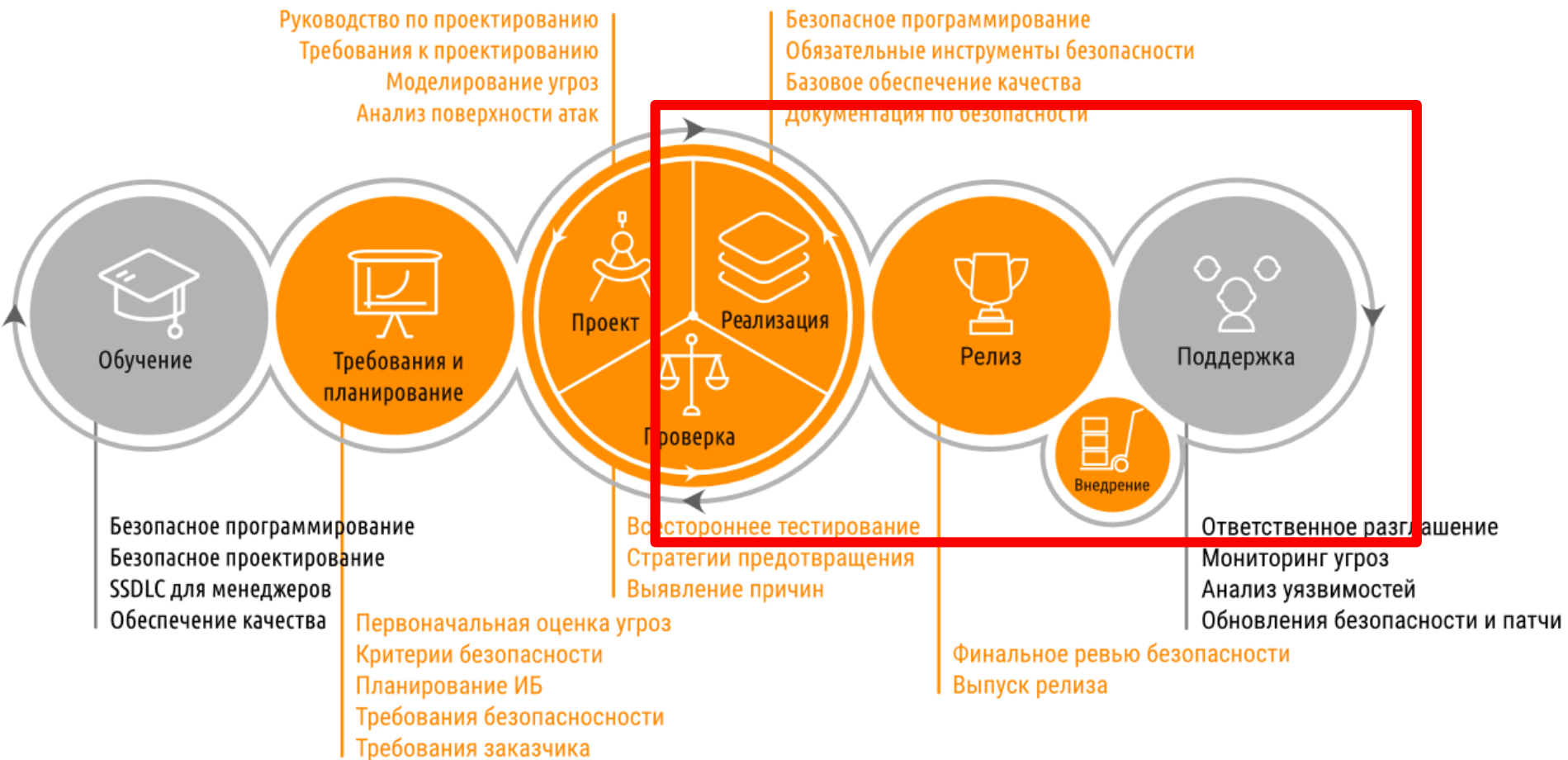
Что произошло 1 июля 2018 года?

Вступила в силу редакция 382-П (Указание 4793-У):

1. Уведомление об инцидентах ИБ
2. Безопасность прикладного ПО, используемое для перевода денежных средств
3. Разделение контуров у клиент-банка
4. **Проведение тестов на проникновение и анализ уязвимостей ИБ объектов информационной инфраструктуры**
5. Использование отечественной криптографии



Пентест, как неотъемлемый элемент цикла безопасной разработки



Пентест – как способ контроля процессов



Выведение ПО из
эксплуатации

Обработка инцидентов

Проверка
осведомленности (пункт
2.12 положения 382-П)

Потребности игроков финансового рынка или как была понята трактовка по проведению тестов на проникновение



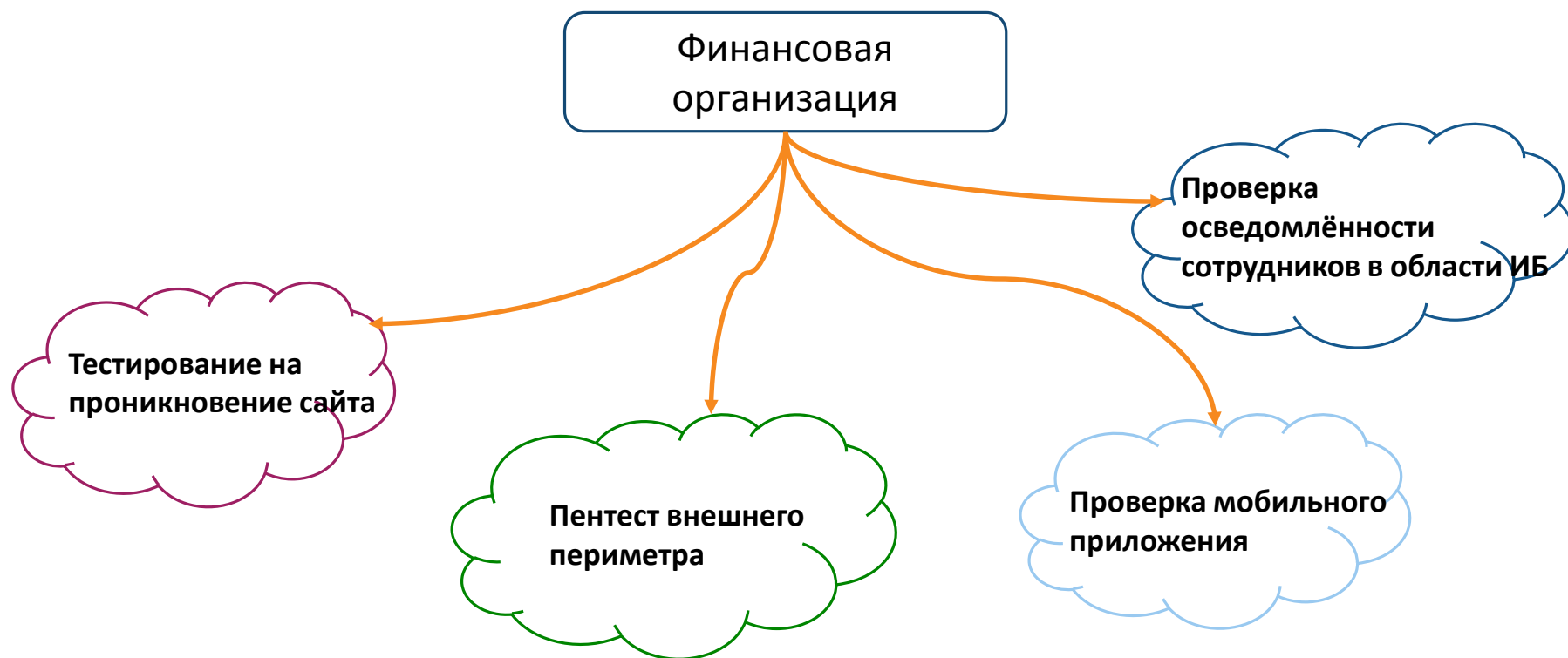
Указание 4793-У:

2014) (далее – ГОСТ Р ИСО/МЭК 15408-3-2013);

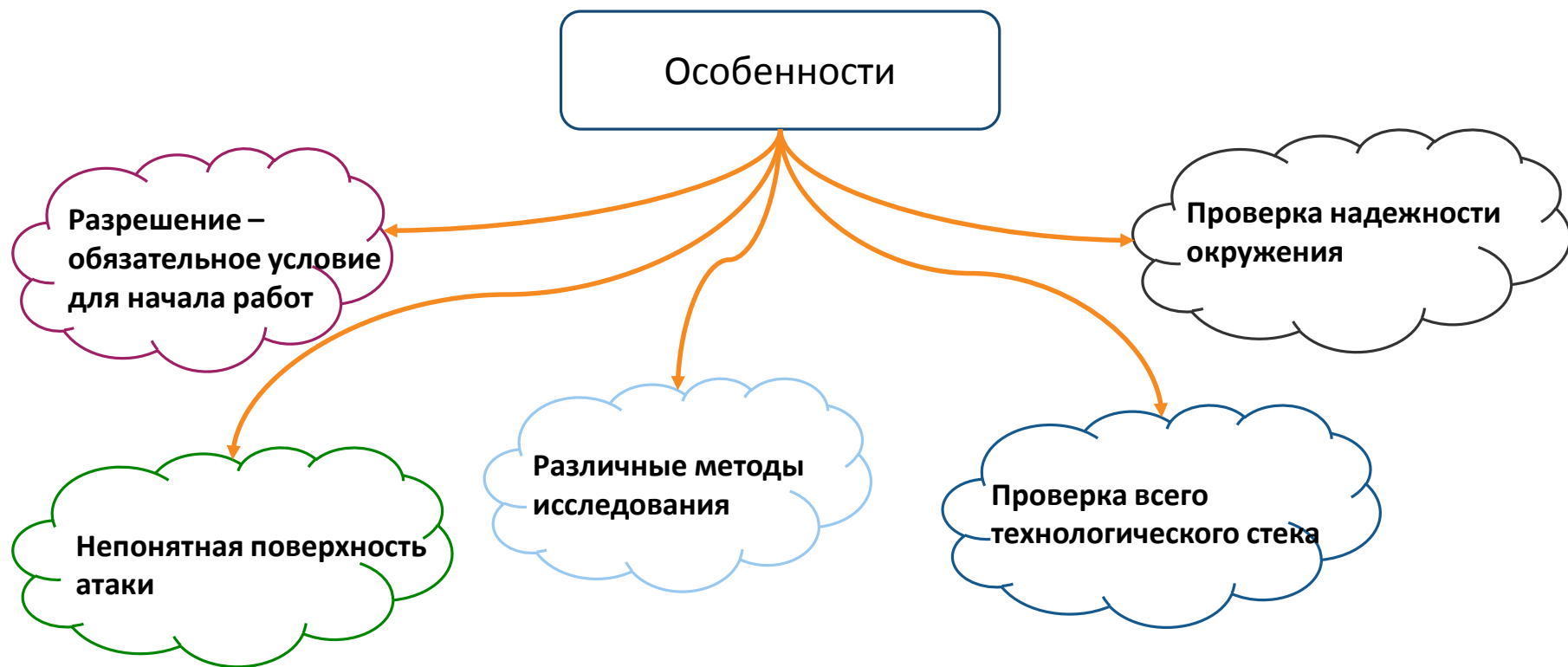
ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

Для проведения анализа уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений оператору по

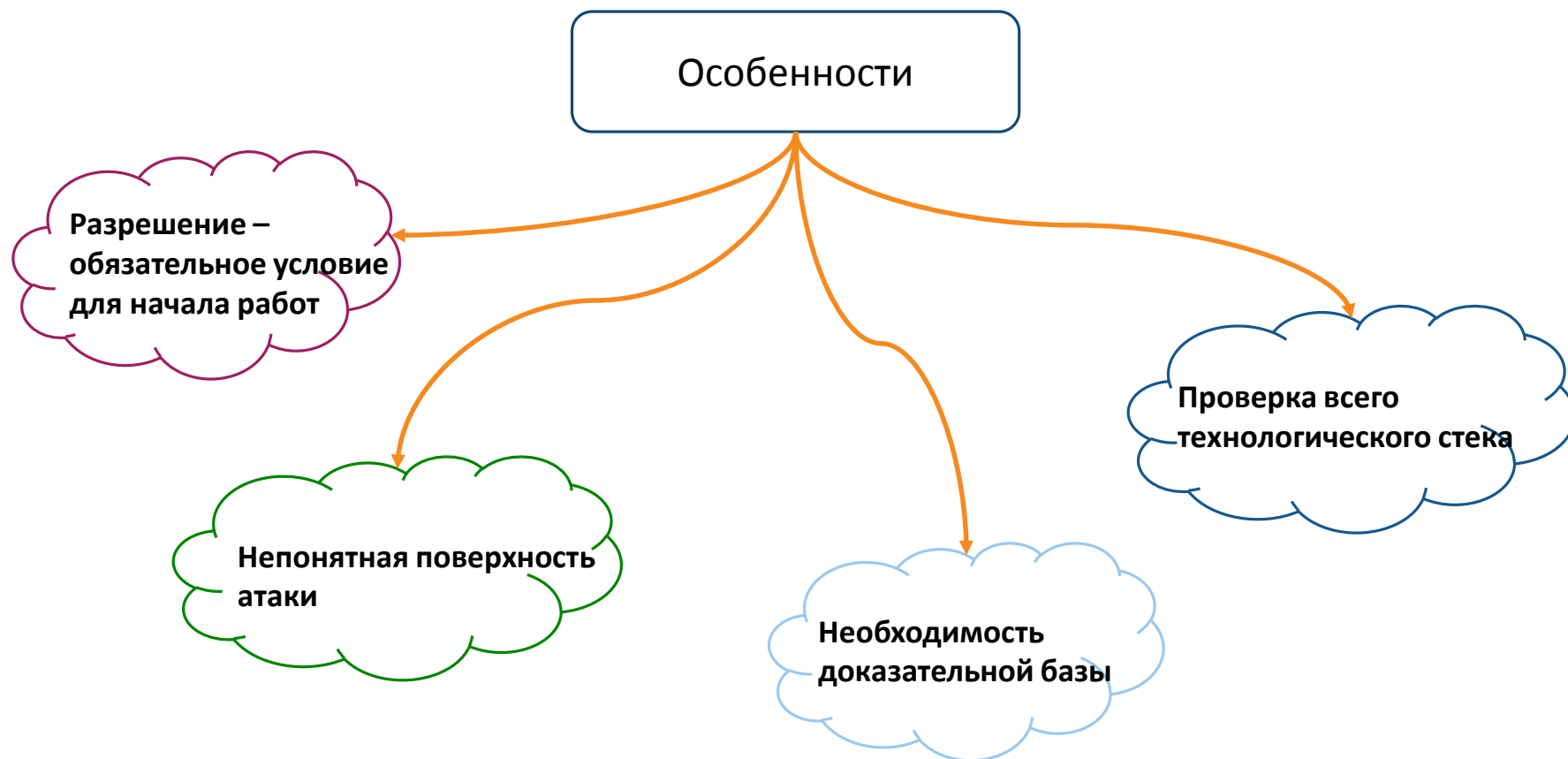
Потребности игроков финансового рынка или как была понята трактовка по проведению тестов на проникновение и анализу уязвимостей



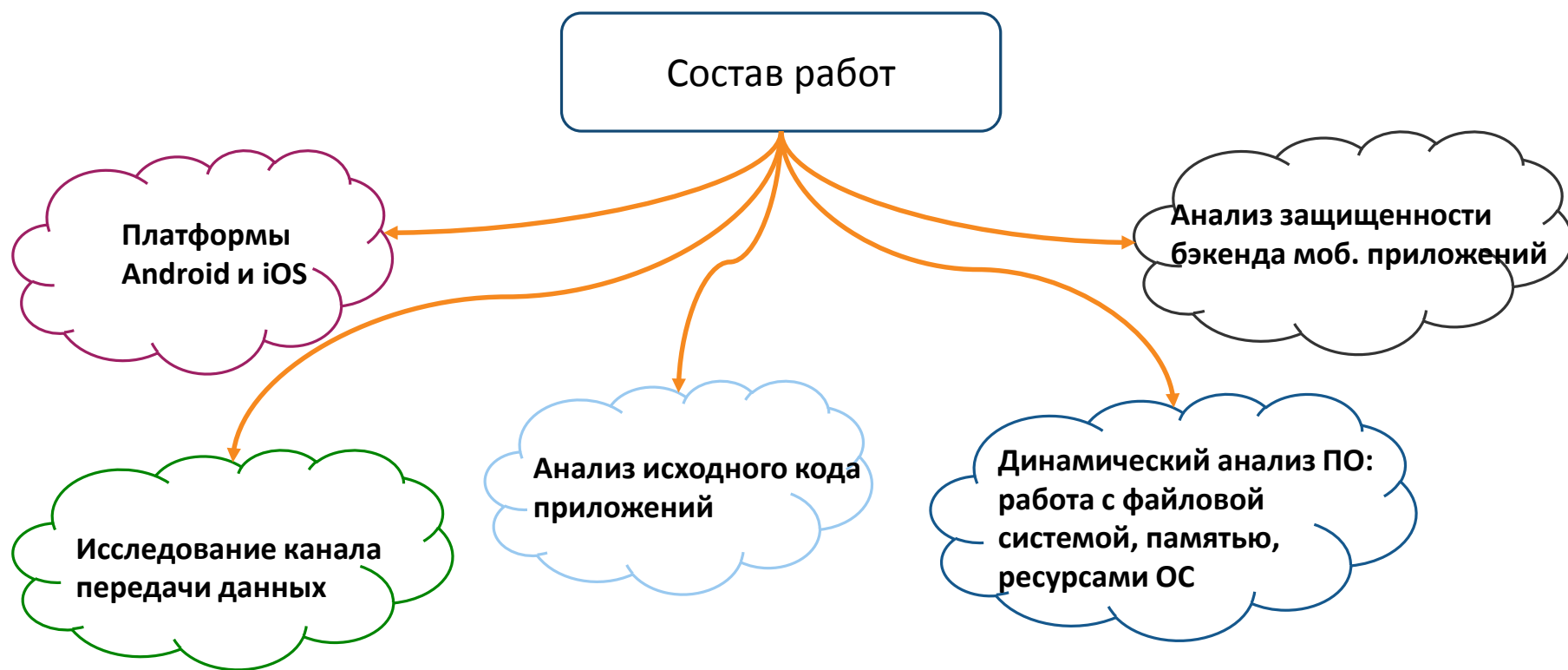
Тестирование на проникновение сайта финансовой организации



Пентест и анализ уязвимостей внешнего периметра

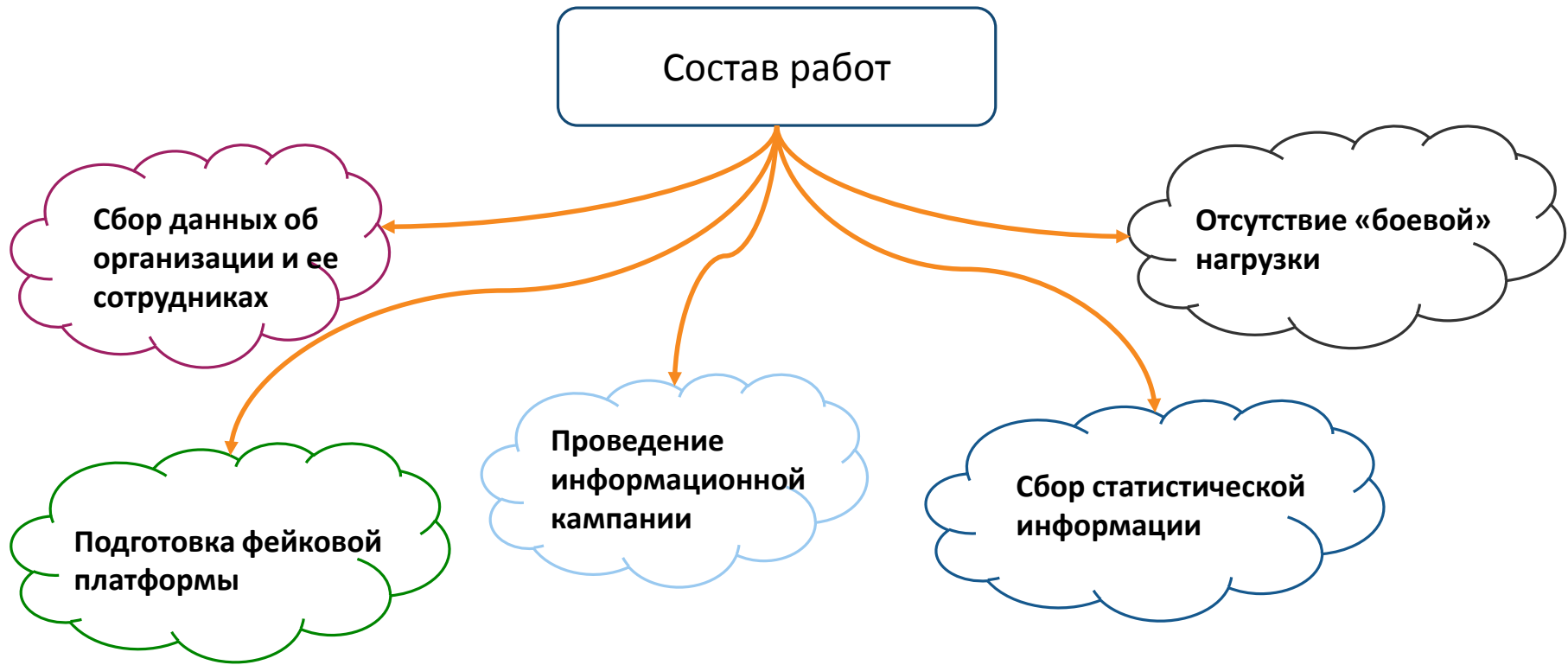


Проверка мобильного приложения





Проверка осведомлённости сотрудников в области информационной безопасности



Проверка осведомлённости сотрудников в области информационной безопасности



Подведение итогов 2018 года

Даты: 21–23 января, 2018 г.

Контакты:

* Required

ФИО *

Your answer

Адрес электронной почты *

Your answer

Что/Кого Вы в своей фирме цените? *

- Рабочий график
- Возможность карьерного роста
- Дружелюбная атмосфера

Проверка осведомлённости сотрудников в области информационной безопасности



Reply Reply All Forward



Чт 2018 11:05

web@ .ru

В компании принят новый документ

To

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Уважаемые коллеги!

В нашей компании утвержден новый распорядительный документ - распоряжение от
«Об утверждении и введении в действие правил использования социальных сетей/мессенджеров на рабочей станции для пользователей информационных систем»

Документ устанавливает общие правила по обеспечению безопасности информации при работе в информационных системах (ИС) компании.

С момента издания данного распоряжения признаются утратившими силу «Правила по обеспечению мер безопасности информации при работе в автоматизированных системах», утвержденные Приказом от « » № 01-3-

С уважением,
дирекция безопасности



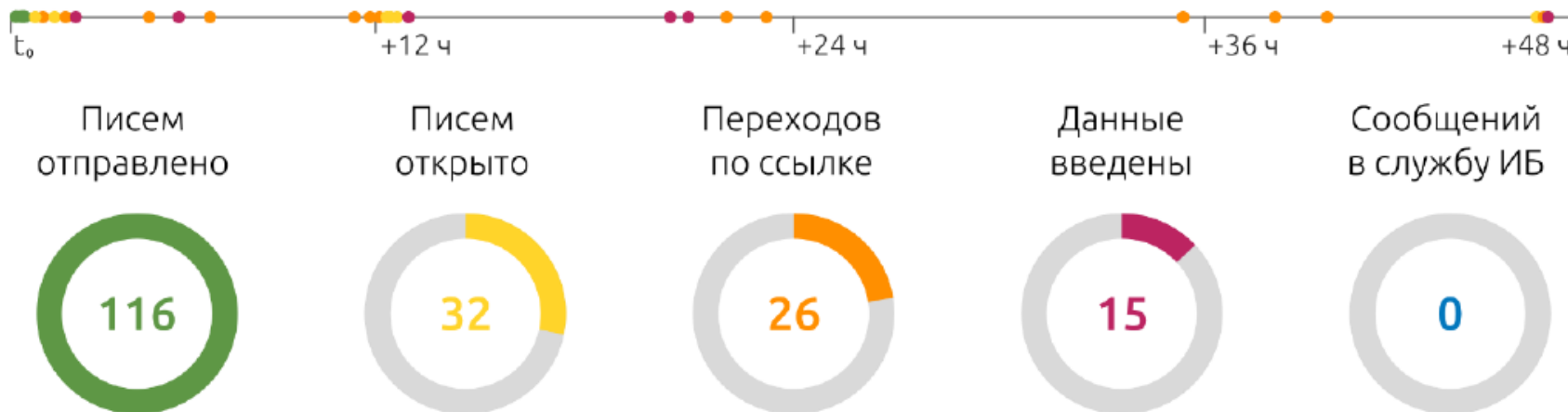
020

Правила...docx

Проверка осведомлённости сотрудников в области информационной безопасности



Таймлайн кампании



Подробности

Поиск:

Имя	Почта	Должность	Статус
Иоганн Тритемий	it@benediktiner.de	Аббат	Данные введены
Алан Тьюринг	bombe@cam.ac.uk	Тестирующий	Письмо отправлено
Уитфилд Диффи	publickey@icann.org	CISO	Письмо отправлено
Майкл Роджерс	bigboss@nsa.gov	Адмирал	Переход по ссылке

Расширение объектов информационной инфраструктуры для проведения тестов на проникновение

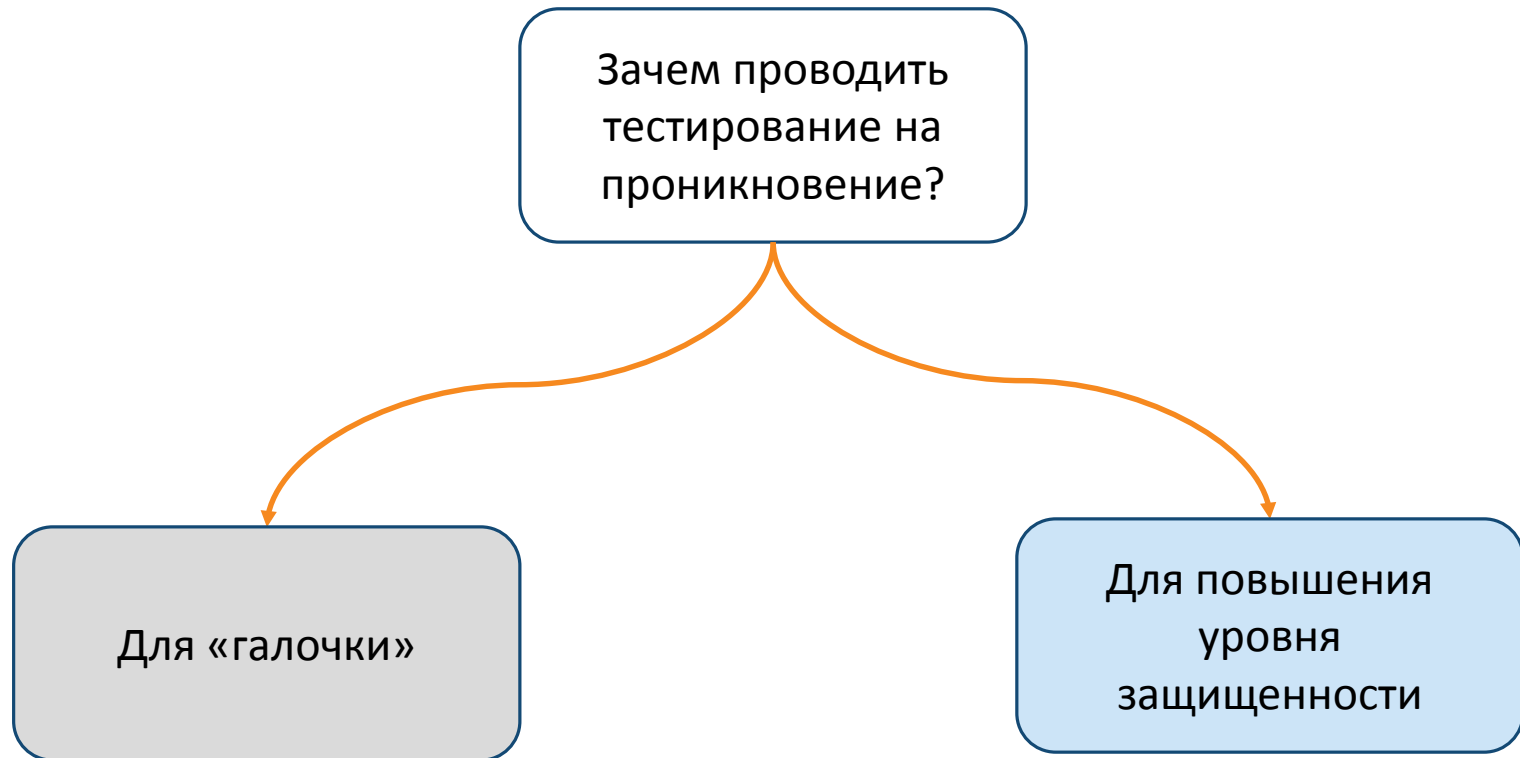


Внешний нарушитель

1. Сайты
2. Внешний периметр
3. Мобильные приложения
4. Проверка осведомленности

Внутренний нарушитель

1. Банковские информационные системы
2. Сервера баз данных
3. Типовые рабочие места
4. Сетевое оборудование





Спасибо за
внимание!

Александр Несергеевич Пушкин

Руководитель отдела ИИТ

компании «Перспективный мониторинг»

Aleksandr.Pushkin@amonitoring.ru