Антифишинг
www.antiphish.ru

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ОНЛАЙН

От «осведомленности» и «рассылок» — к управлению навыками по безопасности.

Пять неудобных вопросов

Сергей Волдохин sv@antiphish.ru

1. Вы точно знаете, как работают цифровые атаки на людей?

СБЕРБАНК
Всегда рядом

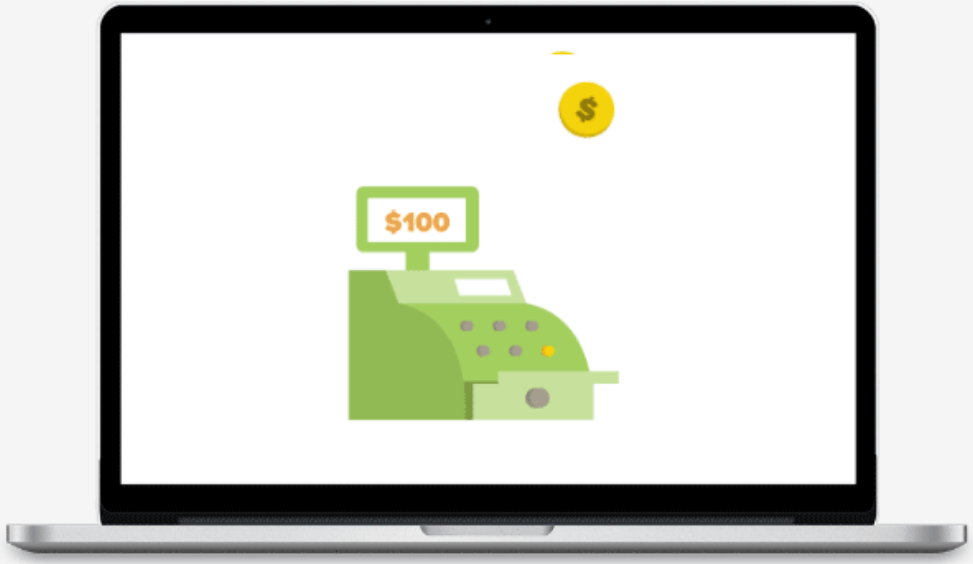
ЕЖЕМЕСЯЧНЫЙ МОТИВИРОВАННЫЙ ОПРОС ГРАЖДАН О ПЛАТЕЖНОЙ СИСТЕМЕ ПАО СБЕРБАНК РОССИИ.

ОСТАВЬТЕ СВОЕ МНЕНИЕ И ПОЛУЧИТЕ ВОЗНАГРАЖДЕНИЕ ДО 600 000 РУБ

Денежных бонусов осталось: 75

Выплачено бонусов за месяц: 34763841 руб

ПОМОГИТЕ КОМПАНИИ ПАО СБЕРБАНК УЛУЧШИТЬ КАЧЕСТВО СЕРВИСА, ОТВЕТИВ НА НЕСКОЛЬКО ПРОСТЫХ ВОПРОСОВ И ПОЛУЧИТЕ ДО 600 000 РУБЛЕЙ!



Личная

Авторитет

Жадность

Личная

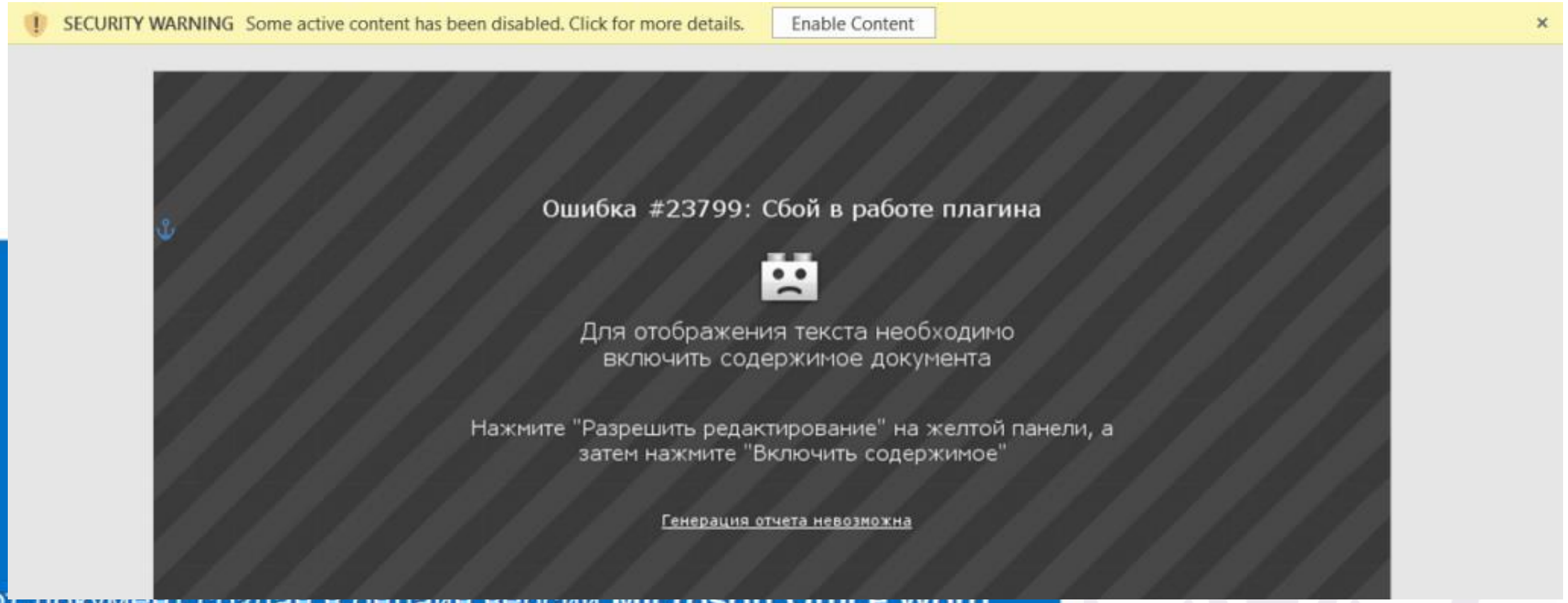
Срочность

Жадность

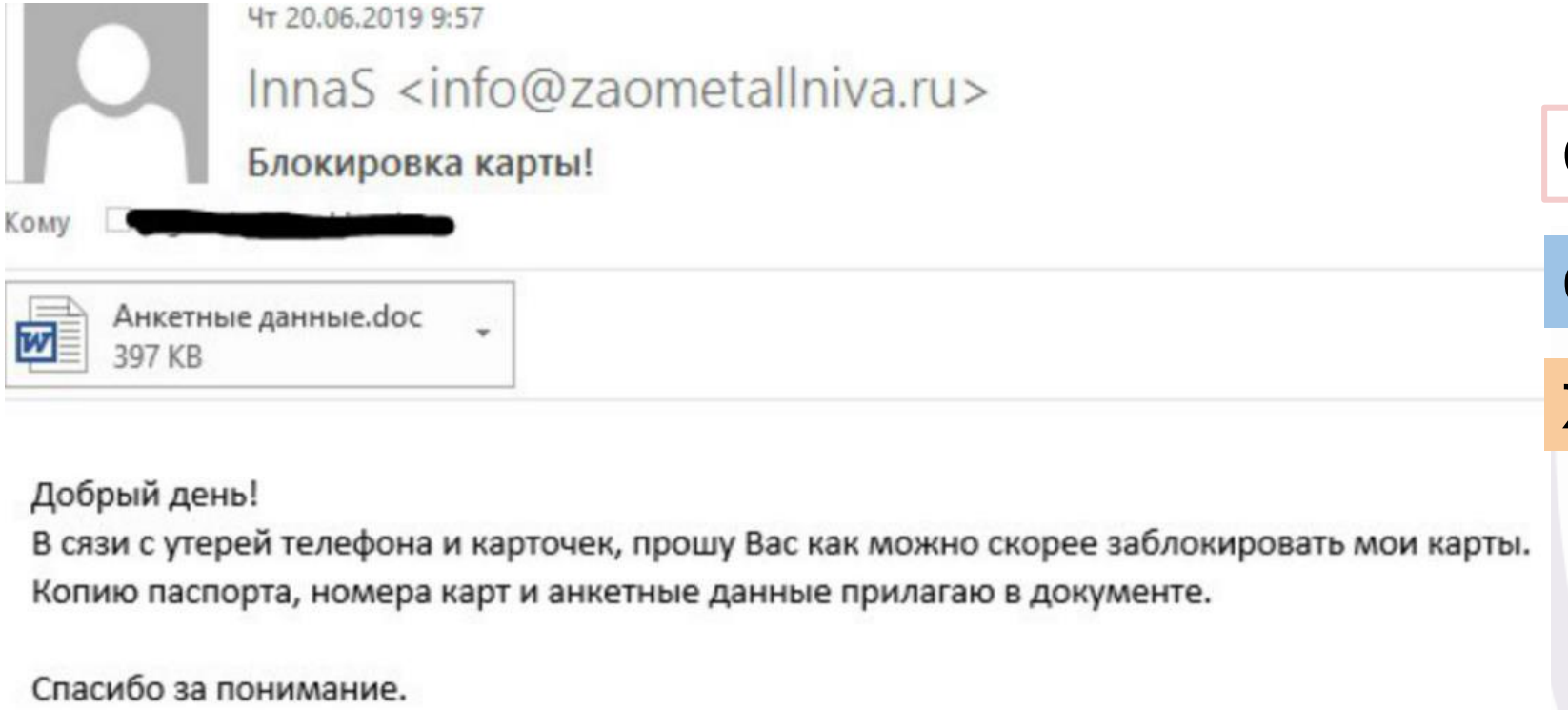
Личная

Срочность

Социальное одобрение


SECURITY WARNING Some active content has been disabled. Click for more details.
Enable Content
Ошибка #23799: Сбой в работе плагина
Для отображения текста необходимо
включить содержимое документа
Нажмите "Разрешить редактирование" на желтой панели, а
затем нажмите "Включить содержимое"
Генерация отчета невозможна
Этот документ создан в онлайн версии Microsoft Office Word
Для просмотра или редактирования данного документа, необходимо
разрешить редактирование и включить содержимое онлайн контента

Внешняя



Срочность

Страх

Желание помочь

Квартира в новостройке

5,75% ставка по ипотеке

1–30 лет срок кредитования

26 млн. ₽ максимальная сумма

Все подробности и специальные условия для сотрудников [redacted] описаны по ссылке.

Ведущий кредитный менеджер

[redacted] Людмила Александровна

Отделение «Москва-Сити»
г. Москва, ул. [redacted] 10

[redacted] БАНК

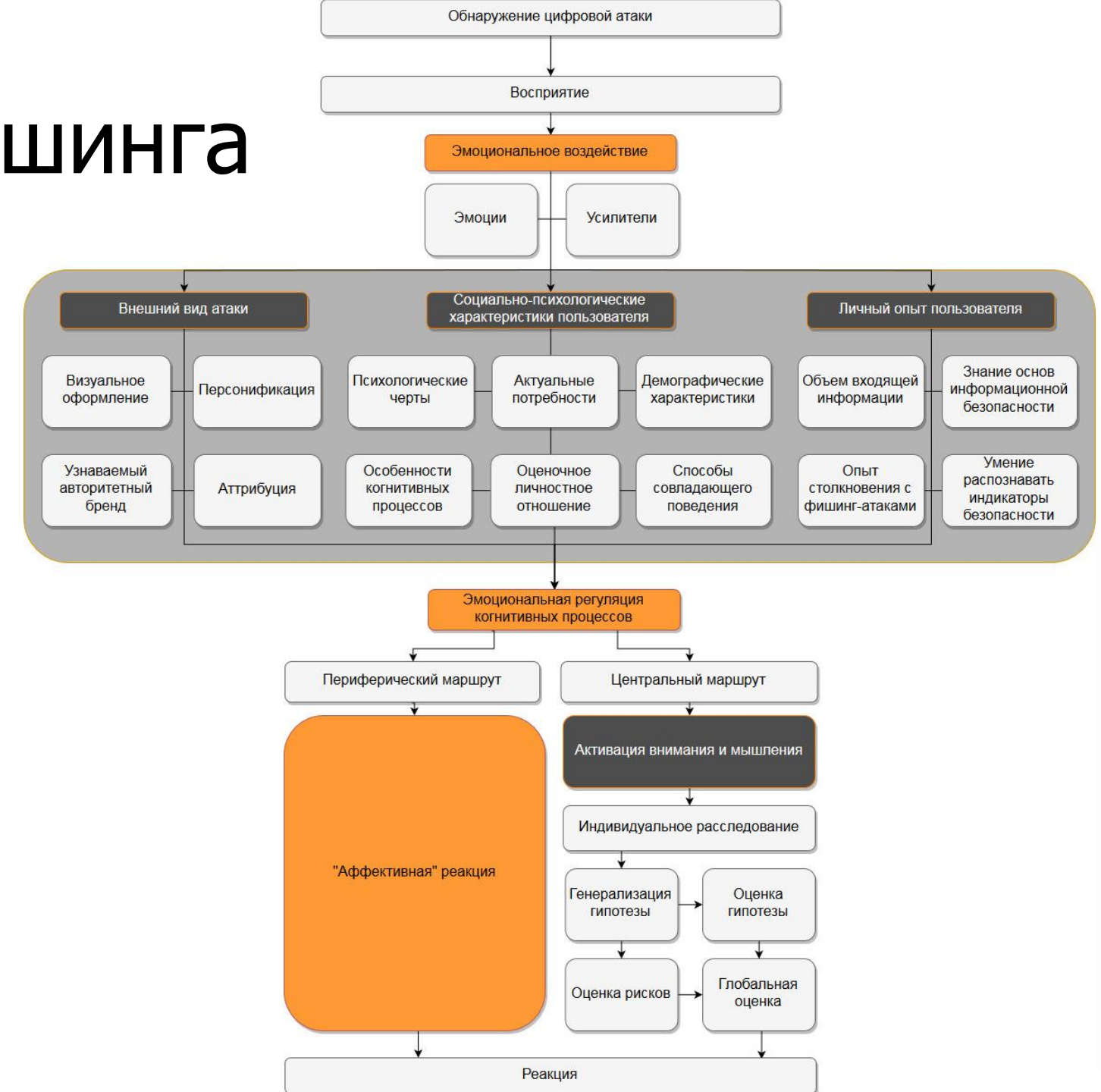
Корпоративная

Жадность

Любопытство

Проверка навыков

Модель Антифишинга



antiphish.ru/classification

Outline

Психологические векторы атаки

Страх

«Ваш компьютер заражен и заблокирован. Кликните здесь»

Раздражение

«Чтобы отписаться, перейдите по ссылке»

Невнимательность

«www.sbernbank.ru», «www.gmall.com»

Любопытство

«Смотри, как ты отжигаешь на видео»

Жадность

«Скидка 50% при оплате прямо сейчас»

Желание помочь

«Кажется, ваш коллега потерял свои вещи. Дайте мне его номер»

2. Что будете с этим делать?

«Повышать осведомленность»?

Будьте внимательны!!!!1111ОДИННАДЦАТЬ

Не переходите по неизвестным ссылкам

Не открывайте подозрительные вложения

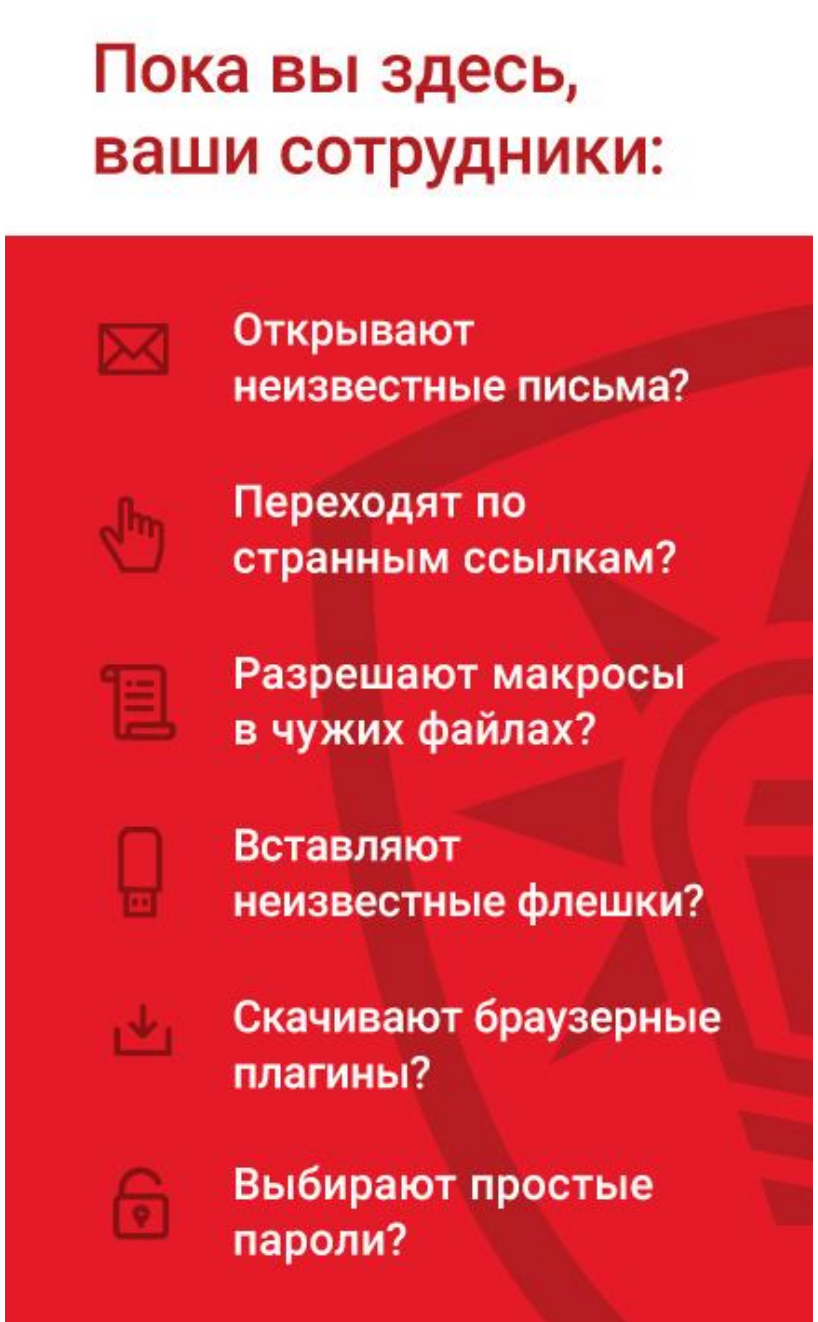
Не вводите пароли на подозрительных сайтах

Не устанавливайте программы из недоверенных источников ….

Капитан Очевидность

— Дядь Степан, ихний кучер на меня в лорнет посмотрел, чего это он?
— Чего… Зрение слабое.

к/ф «Формула любви»



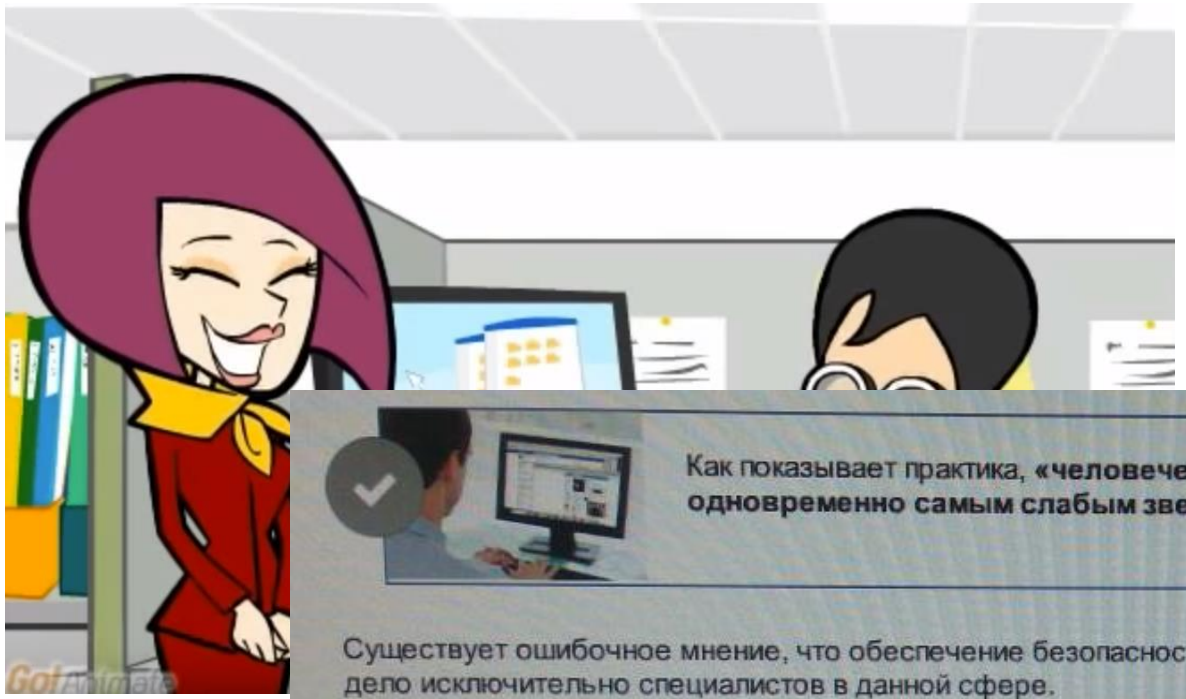
Что должны знать ваши сотрудники?

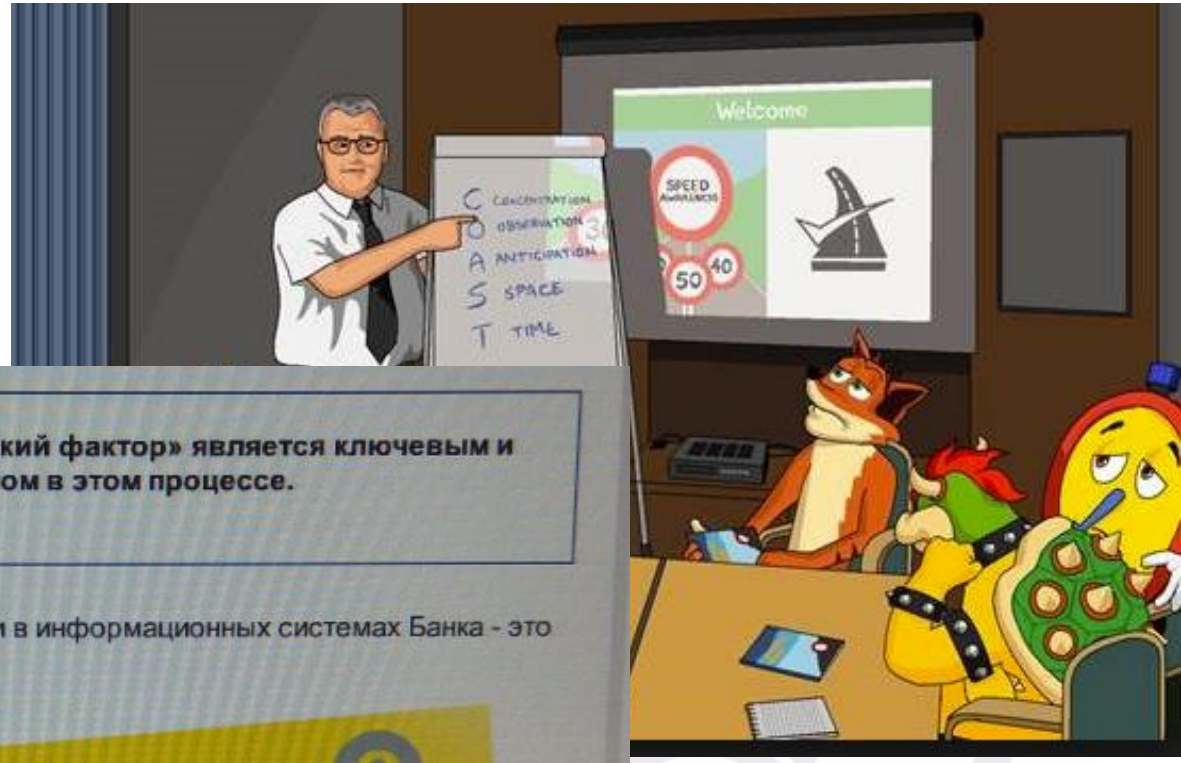
Что они должны уметь? Какие навыки влияют на безопасность?

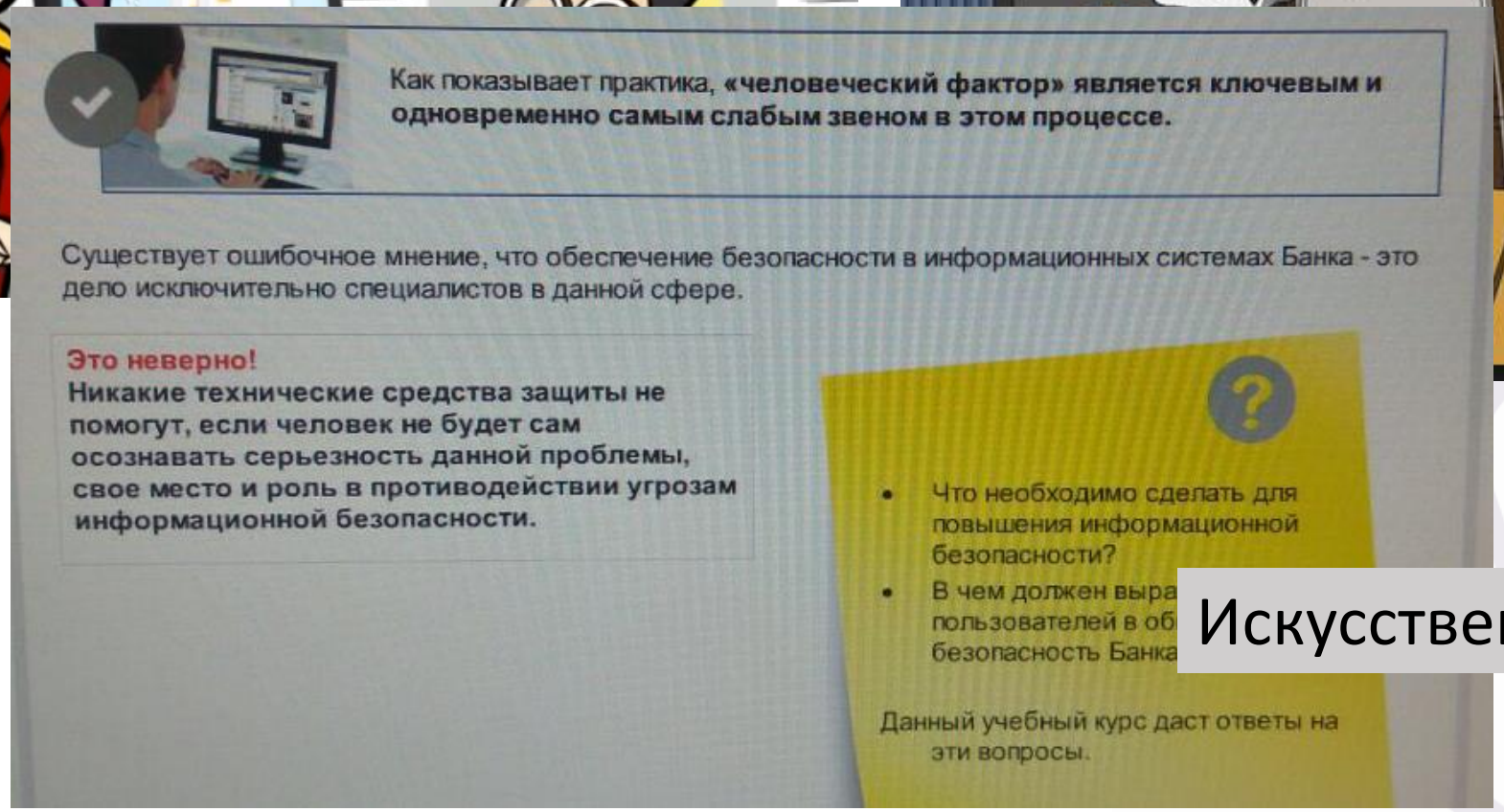
(Знания + Навыки) x Измерение

Тренируйте и измеряйте эти навыки

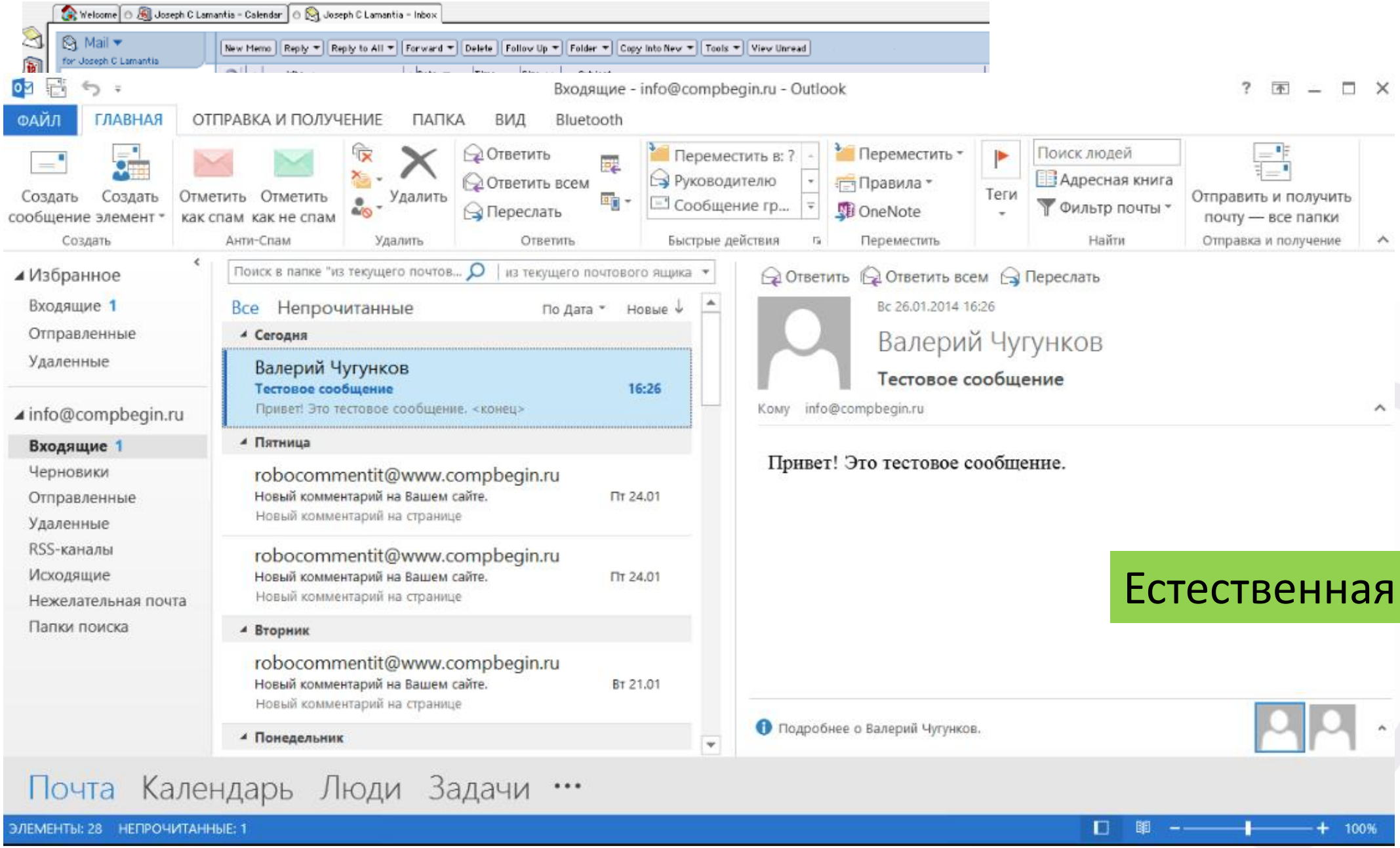
3. Как будете обучать сотрудников?







Искусственная среда



Естественная среда

4. Как тренировать и проверять навыки?

«Провокационные рассылки»?

Спам

Госуслуги

Одноклассники

Рассылка

Фишинг

Кликнули

antiphish.ru/template

Ид	Сценарий	Вектора атаки	Технологии
1	Руководитель HR-отдела обращается к сотруднику по имени и сообщает, что заключен договор с новой компанией ДМС. Обещают бесплатную стоматологию и полный чек-ап в известном медицинском центре. Полный список услуг во вложении. ...исы в этом месяце получат только те, ...рейдет по ссылке.	Корпоративная Персональная Жадность Любопытство Срочность	Эл. письмо Вложение MS Word Ссылка

Проверка навыков

Атаки на сотрудников

Электронная почта | Съемные устройства | Создать атаку

Атака на бухгалтерию 127 целей

Страх × | Раздражение × | корпоративная

отчеты за 20 марта 12:09

Атака на все отделы 2 390 целей

Любопытство × | Жадность × | Желание помочь × | внешняя

Невнимательность × | Срочность × | Авторитет ×

отчеты за 13 марта

Тестовая атака Секретари

Жадность × | Авторитет × | личная

отчеты за 7 марта

Как люди открывают письма

Переходят по ссылкам

Открывают вложенные файлы

Вводят данные в формы

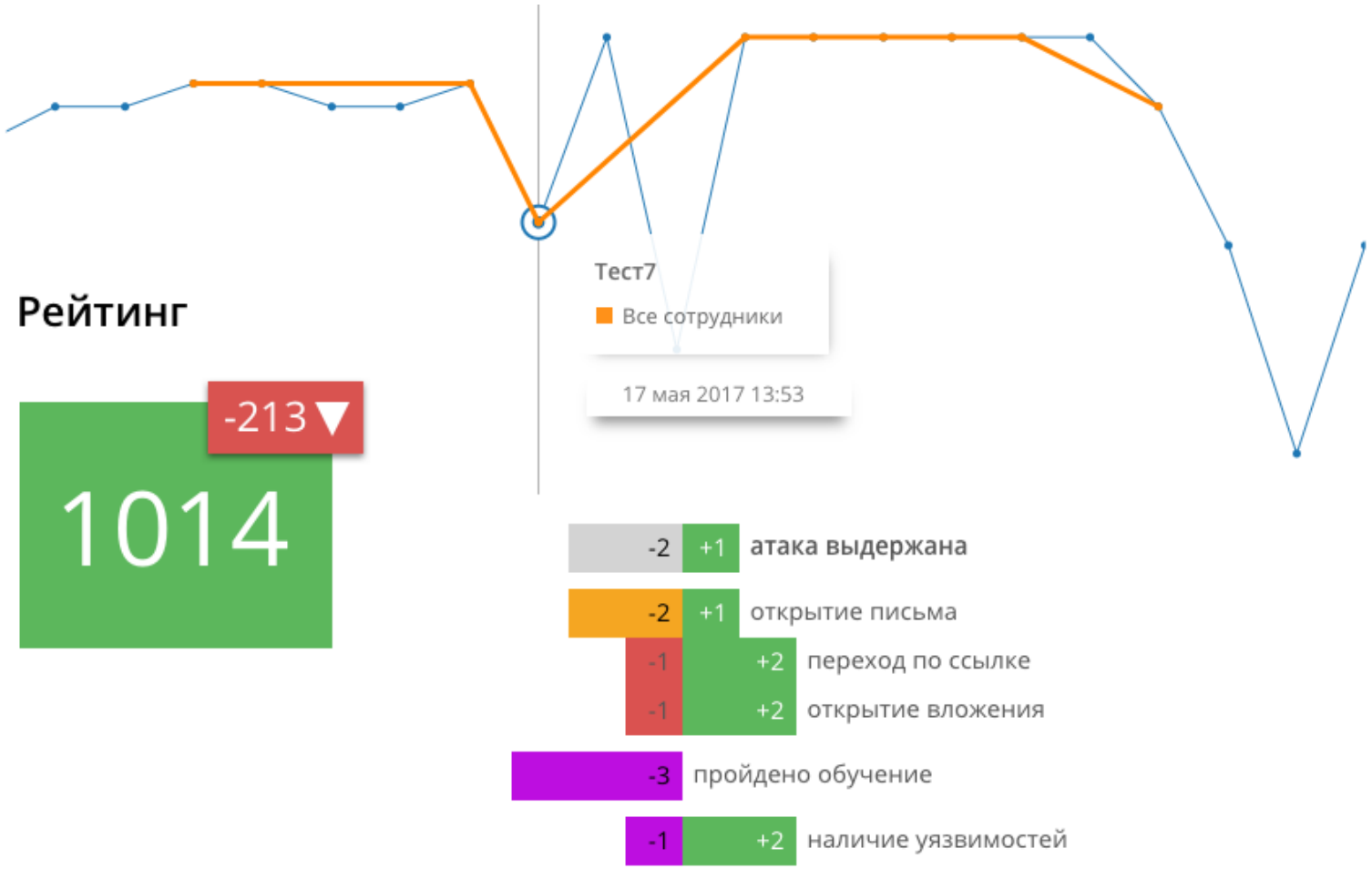
Подключают съемные устройства

...

Все психологические векторы покрыты?

Организационные векторы?

Как меняется поведение людей?



5. Как выбирать приоритеты?

Самые опасные вектора

Внешняя

Персональная

Страх

Анонимная

Желание помочь

Корпоративная

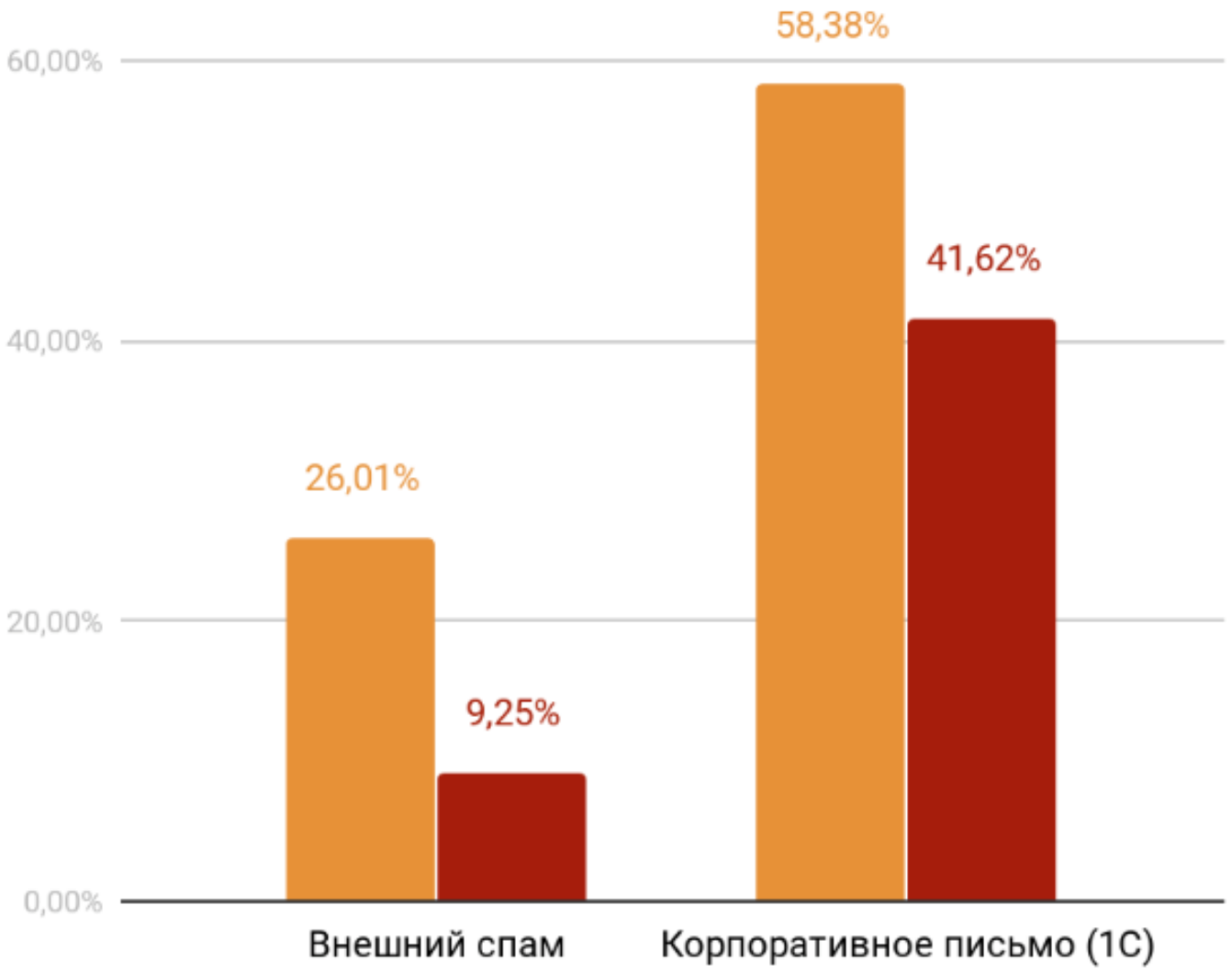
Персональная

Жадность

Желание помочь

antiphish.ru/classification

Самая опасная атрибуция



Значимые личностные черты

- Экстраверсия – Интроверсия.
- Эмоциональная устойчивость – Эмоциональная неустойчивость.
- Доброжелательность - Обособленность.
- Добросовестность – Импульсивность.
- Открытость опыту – Практичность.

Категории сотрудников,
которых важнее обучать и тренировать.


Эффективность фишинг-атак по ФО России
3
2,5
2
1,5
1
0,5
0
50р.
40р.
30р.
20р.
10р.
0р.
44
39
39
39
25
30
25
1
1
1
1,1
1,3
1,4
1,5
Центральный
Северо-Западный
Дальневосточный
Уральский
Южный
Сибирский
Приволжский
Эффективность атак
Средняя зарплата за 2017 год, Росстат

5*. Как организовать системный процесс?

Тем временем, в ТЗ:

Техническое задание

на разработку электронного обучающего курса по теме
«Информационная безопасность. Корпоративные алгоритмы работы»

Программы для ЭВМ позволят решить следующие задачи:

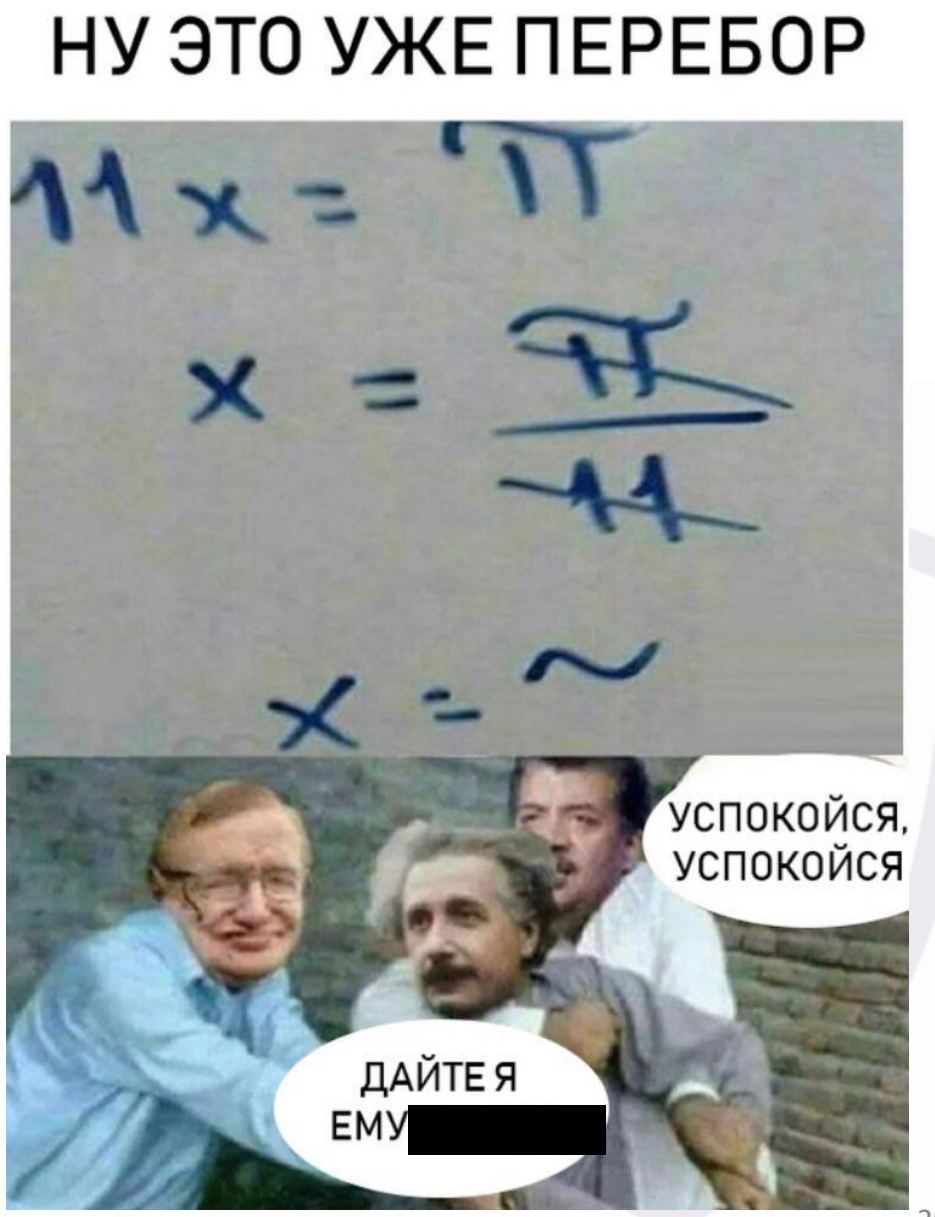
- повысить осведомленность работников в вопросах информационной безопасности;
- сформировать навыки и умения безопасного и целесообразного поведения при работе с компьютерными ресурсами, умения соблюдать нормы информационной этики и права;
- выработать навыки использования средств информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных корпоративных задач с соблюдением требований эргономики, техники безопасности, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

Целевая аудитория:

- менеджеры и специалисты

Система обучения работников преследует следующие цели:

- Сформировать комплекс необходимых навыков безопасной работы с информационными ресурсами.



Тем временем, в бюджетах ИБ:

Juniper				
Cisco			2 394,00 €	
Firewalls				
Checkpoint				
Juniper				35 000,00 €
Cisco				
Web Filtering				
Squidguard (URL Blacklist)				
or Other Solution			64 102,56 €	
Advanced Web-Filter			- €	
Vulnerability Management				
Nessus Security Center	3000	500	10 500,00 €	
Backup / Backup Encryption				
Symantec				
HP Data Protector				
Other Solution				
File/Folder Encryption				
Vormetric Server Agents	13		4 290,00 €	- €
Centralized Log Management - Splunk				

Обзор от Anti-Malware

Обзора рынка сервисов повышения осведомленности по ИБ (Security Awareness) от Аналитического центра Anti-Malware.ru

Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness)

Сергей Горюнов
Обозреватель Anti-Malware.ru

Проголосовало: 63

Требования и критерии

Таблица 1. Сравнительный анализ систем и сервисов повышения осведомленности по ИБ (Security Awareness)

№	Требования к вендору Security Awareness	Тип требования	Phishman Awareness Center	Kaspersky Security Awareness	Антифишинг	UBS Security Awareness Platform	Syssoft Security Awareness	Detea
ТРЕБОВАНИЯ К ВЕНДОРУ								
1	Наличие представительства вендора на территории России	обязательное	+	+	+	н/д	+	н/д
2	Наличие технической поддержки в рабочие дни на русском языке	обязательное	+	+	+	н/д	+	н/д
ТРЕБОВАНИЯ К ОПЫТУ ВНЕДРЕНИЯ И МАСШАБИРОВАНИЯ								
3	Возможность предоставления сервиса через Интернет, а также локальной инсталляции системы в инфраструктуру заказчика: платформа должна функционировать в полном объеме без доступа в Интернет	обязательное	+	-	+	-		
4	Наличие действующей инсталляции с числом лицензий не менее чем на 15 000 сотрудников.	обязательное	н/д	н/д	+	-		
5	Наличие компонентной схемы системы и руководства по масштабированию сервиса не менее чем на 300 000 сотрудников.	обязательное	-	-	+	-		
6	Возможность первичной загрузки и последующей синхронизации (удаления, изменения) сотрудников заказчика из интерфейса администратора через LDAP, а также единый файл определенного формата.	обязательное	+	н/д	+	н/д		
7	Наличие REST API, который позволяет управлять всеми заявленными функциями системы и получать всю статистику по работе	обязательное	-	-	+	-	-	-

Базовая функциональность

Собственные исследования

Обучающие курсы [адаптация + обновления]

Новые и актуальные для вас атаки

Управление навыками

On-premise и масштабируемость

API и интеграция с IRP/SOC/etc.

blog.antiphish.ru

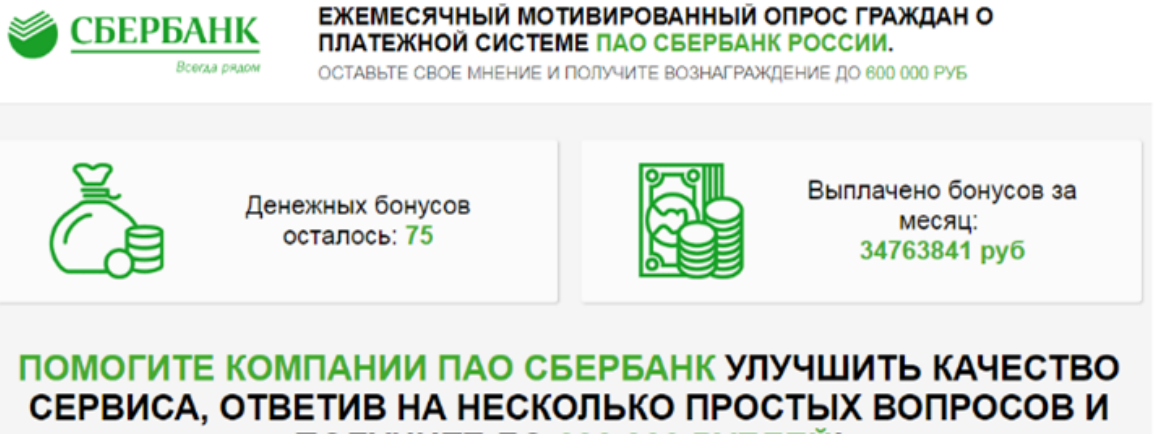
Антифишинг-дайджест №106 с 8 по 14 февраля 2019 года

Представляем новости об актуальных технологиях фишинга и других атаках на человека с 8 по 14 февраля 2019 года.

Сайты, почта и мессенджеры

Злоумышленники используют рекламные объявления Google для продвижения вредоносных сайтов.

Маскируясь под крупные банки, они предлагают пройти опрос и получить вознаграждение:



Андрей Жаркевич
редактор, ИТ-руководитель

Артемий Богданов
технический директор

Сергей Волдохин
выпускающий редактор

Присоединяйтесь к исследованиям

psy@antiphish.ru

Имитированные атаки +
тесты для сотрудников

Грамотные сотрудники и клиенты – лучшая защита.

Обучайте и тренируйте своих людей.

Антифишинг
www.antiphish.ru

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОНЛАЙН