



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?

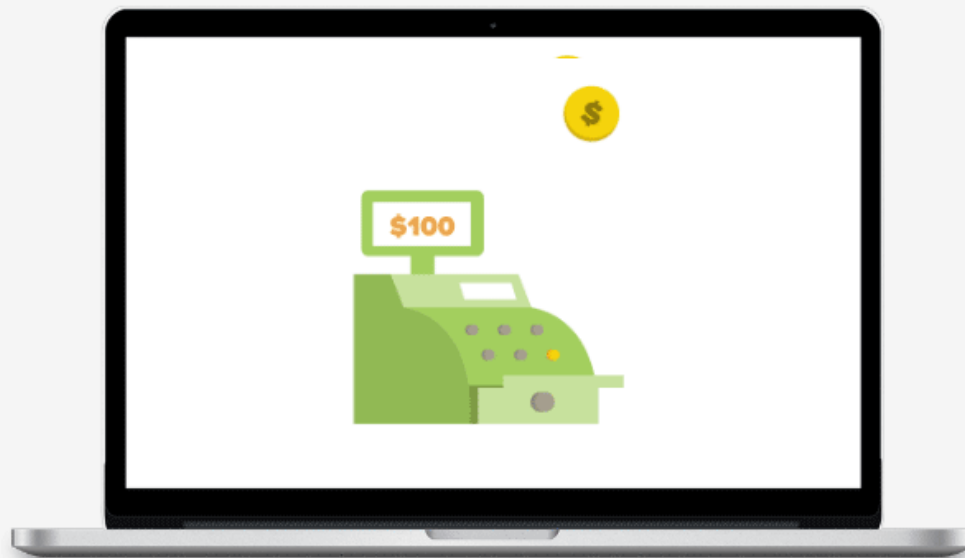


Денежных бонусов
осталось: **75**



Выплачено бонусов за
месяц:
34763841 руб

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



 Личная

Авторитет

Жадность

СРЕДСТВА УСПЕШНО ЗАЧИСЛЕНЫ НА ВНУТРЕННИЙ СЧЕТ!

СУММА ВОЗНАГРАЖДЕНИЯ, ГОТОВАЯ К ОТПРАВКЕ СОСТАВЛЯЕТ:

153 015 РУБЛЕЙ

В связи с лимитами платежных систем, перевод будет отправлен двумя равными частями **в течение 10 минут.**

Чтобы моментально и в полном размере получить выплату необходимо выполнить закрепительный платеж. С Вашей карты/кошелька будет списана сумма **150 руб.**

 Личная

Срочность

Жадность

ВЫПОЛНИТЬ ЗАКРЕПИТЕЛЬНЫЙ ПЛАТЕЖ (150 РУБ) И
ПОЛУЧИТЬ 153 015 РУБ.

ВЫПОЛНИТЬ ЗАКРЕПИТЕЛЬНЫЙ ПЛАТЕЖ И ПОЛУЧИТЬ ВЫПЛАТУ

*Если не получается оплатить банковской картой, воспользуйтесь электронным кошельком или воспользуйтесь другой банковской картой

BILLING EUROPE PAYMENT
secure payments on the Internet

КОММЕНТАРИИ УЧАСТНИКОВ **ПОТРЕБИТЕЛЬСКОГО РЕЙТИНГА**

ПОКАЗАНЫ ПОСЛЕДНИЕ 5 КОММЕНТАРИЕВ ИЗ 9005



Куликова Мария

 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



Чт 20.06.2019 9:57

InnaS <info@zaometallniva.ru>

Блокировка карты!

Кому 



Анкетные данные.doc
397 KB

Добрый день!

В связи с утерей телефона и карточек, прошу Вас как можно скорее заблокировать мои карты.
Копию паспорта, номера карт и анкетные данные прилагаю в документе.

Спасибо за понимание.

Срочность

Страх

Желание помочь



Квартира в новостройке

5,75%

ставка по ипотеке

1–30 лет

срок кредитования

26 млн. ₽

максимальная сумма



 Корпоративная

Жадность

Любопытство

Все подробности и [специальные условия для сотрудников](#)  описаны по ссылке.

Ведущий кредитный менеджер

 Людмила Александровна

Отделение «Москва-Сити»

г. Москва, ул.  10

 **БАНК**



Модель Антифишинга



antiphish.ru/classification

Outline ×

- Антифишинг — сервис об...
- Классификация цифровы...
- Технологические векторы циф...
- Электронная почта
- Сайты
- Социальные сети
- Мессенджеры
- Офис, рабочие помещения
- Дополнительные технологиче...
- Работа через устаревшие в...
- Разнообразие версий опера...
- Использование нелицензио...

Психологические векторы атаки

Страх

«Ваш компьютер заражен и заблокирован. Кликните здесь»

Раздражение

«Чтобы отписаться, перейдите по ссылке»

Невнимательность

«www.sberbank.ru», «www.gmail.com»

Любопытство

«Смотри, как ты отжигашь 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

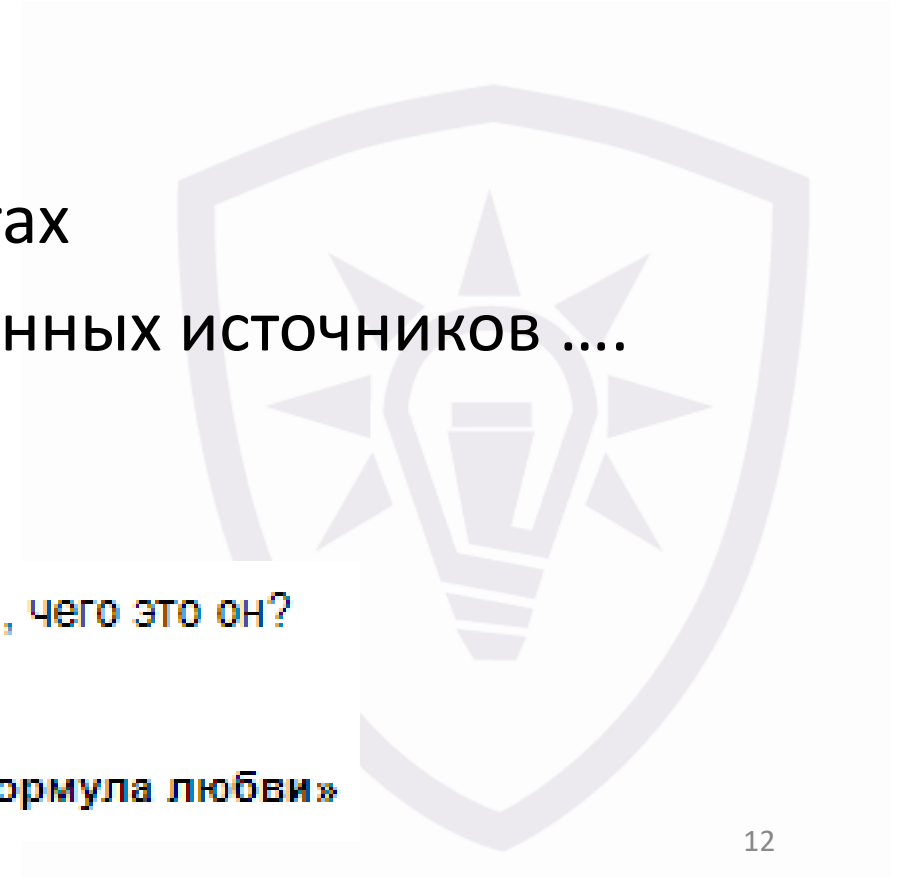
Не вводите пароли на подозрительных сайтах

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»



Пока вы здесь,
ваши сотрудники:



Открывают
неизвестные письма?



Переходят по
странным ссылкам?



Разрешают макросы
в чужих файлах?



Вставляют
неизвестные флешки?



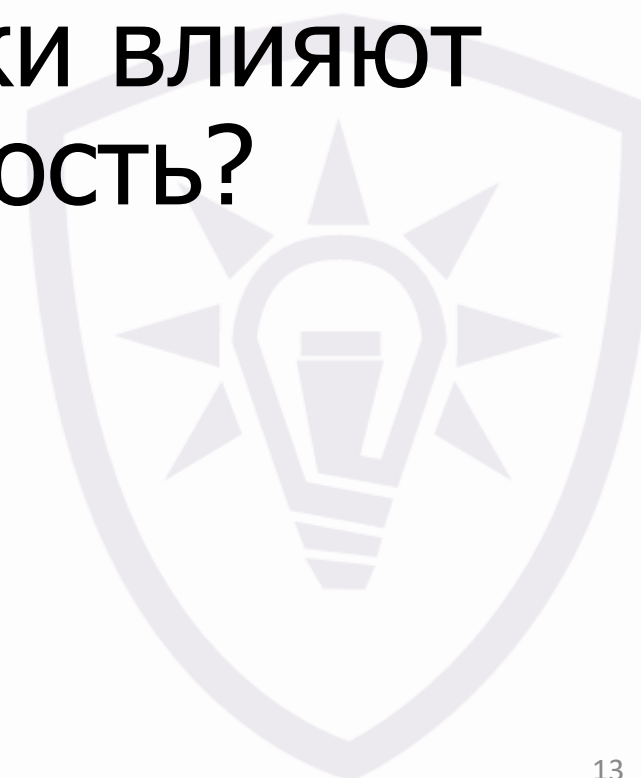
Скачивают браузерные
плагины?



Выбирают простые
пароли?

Что должны знать ваши сотрудники?

Что они должны уметь? Какие навыки влияют на безопасность?



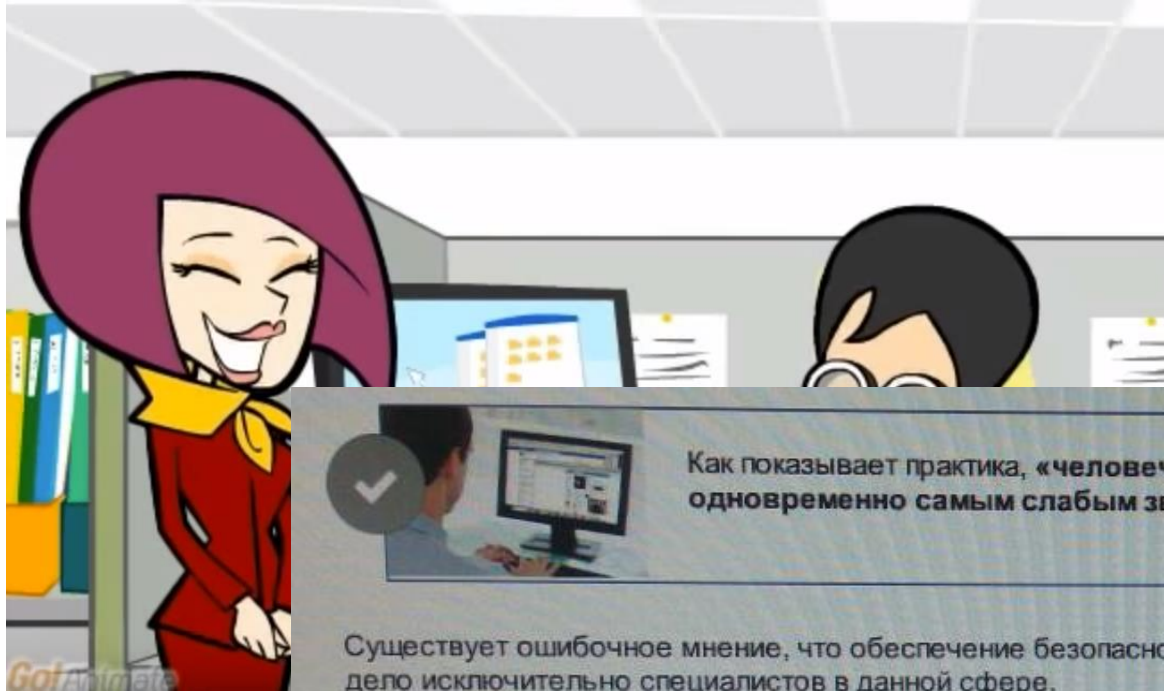
(Знания + Навыки) x Измерение



Тренируйте
и измеряйте
ЭТИ НАВЫКИ

3. Как будете
обучать сотрудников?





Как показывает практика, «человеческий фактор» является ключевым и одновременно самым слабым звеном в этом процессе.

Существует ошибочное мнение, что обеспечение безопасности в информационных системах Банка - это дело исключительно специалистов в данной сфере.

Это неверно!

Никакие технические средства защиты не помогут, если человек не будет сам осознавать серьезность данной проблемы, свое место и роль в противодействии угрозам информационной безопасности.



- Что необходимо сделать для повышения информационной безопасности?
- В чем должен выражаться уровень информированности пользователей в области безопасности Банка?

Данный учебный курс даст ответы на эти вопросы.

Искусственная среда

The screenshot displays the Microsoft Outlook application window. The title bar reads "Входящие - info@compbegin.ru - Outlook". The ribbon menu includes "ФАЙЛ", "ГЛАВНАЯ", "ОТПРАВКА И ПОЛУЧЕНИЕ", "ПАПКА", "ВИД", and "Bluetooth". The "ОТПРАВКА И ПОЛУЧЕНИЕ" ribbon is active, showing options like "Создать сообщение", "Отметить как спам", "Удалить", "Ответить", "Переместить в:", "Правила", "Поиск людей", "Адресная книга", and "Фильтр почты".

The left sidebar shows the "Избранное" (Favorites) section with "Входящие 1" (Inbox 1) selected. Below it, the "info@compbegin.ru" account is listed with folders for "Входящие 1", "Черновики", "Отправленные", "Удаленные", "RSS-каналы", "Исходящие", "Нежелательная почта", and "Папки поиска".

The main pane shows a list of emails. The selected email is from "Валерий Чугунков" (Valeriy Chugunov) with the subject "Тестовое сообщение" (Test message) and time "16:26". The preview pane shows the email content: "Привет! Это тестовое сообщение. <конец>" (Hello! This is a test message. <end>).

The bottom status bar shows "Почта Календарь Люди Задачи ..." (Mail Calendar People Tasks ...) and "ЭЛЕМЕНТЫ: 28 НЕПРОЧИТАННЫЕ: 1" (ELEMENTS: 28 UNREAD: 1). The zoom level is set to 100%.

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. Комиссы в этом месяце получают только те, кто перейдет по ссылке.	Корпоративная Персональная Жадность Любопытство Срочность	Эл. письмо Вложение MS Word Ссылка



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

Любозытство ×

Жадность ×

Желание помочь ×

 внешняя

Невнимательность ×

Срочность ×

Авторитет ×

отчеты за 13 марта

Тестовая атака Секретари

Жадность ×

Авторитет ×

 личная

отчеты за 7 марта

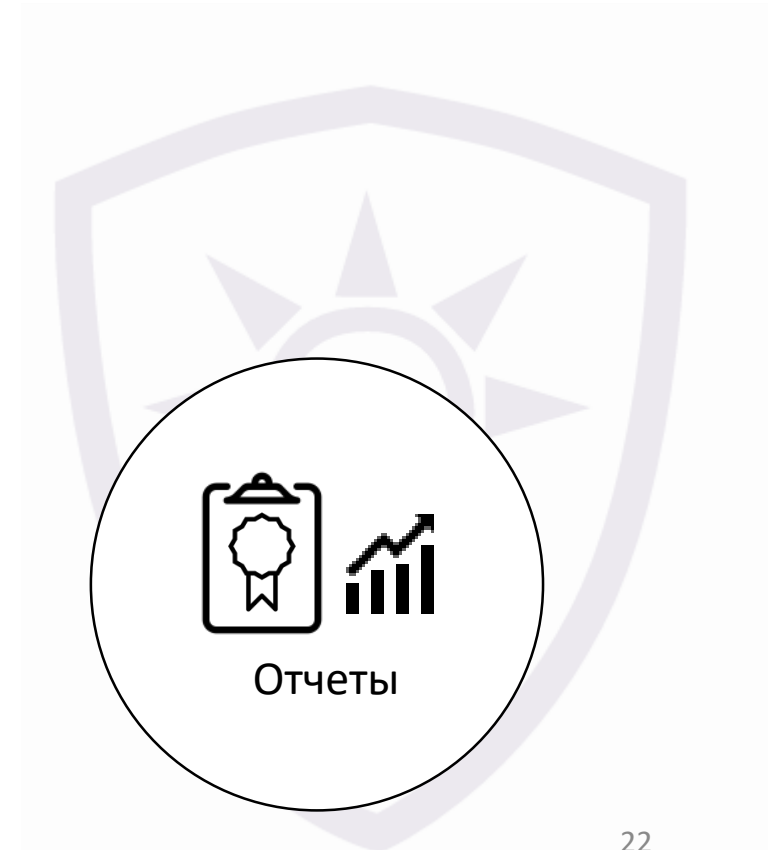
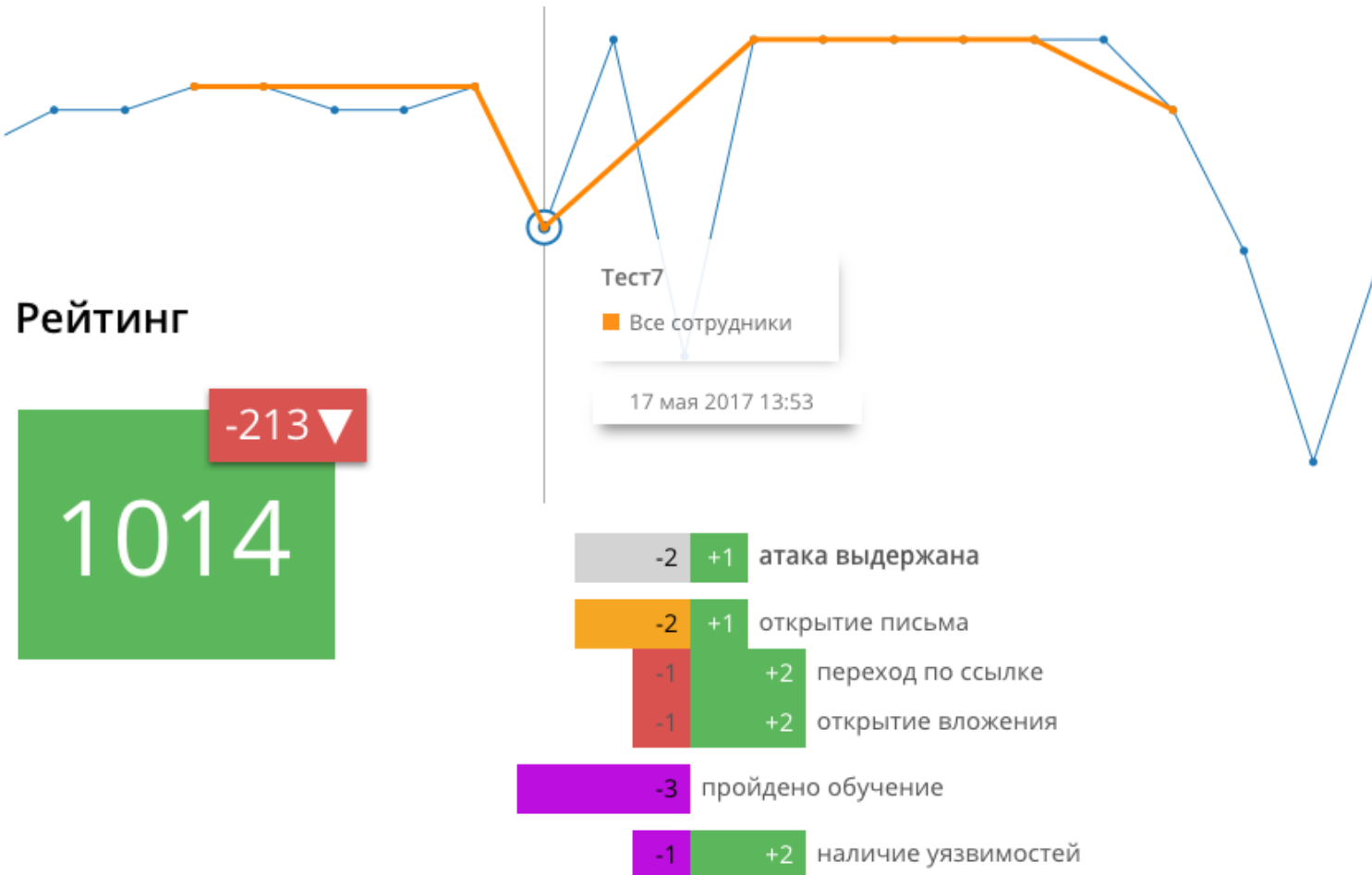
Как люди открывают письма
Переходят по ссылкам
Открывают вложенные файлы
Вводят данные в формы
Подключают съемные устройства

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

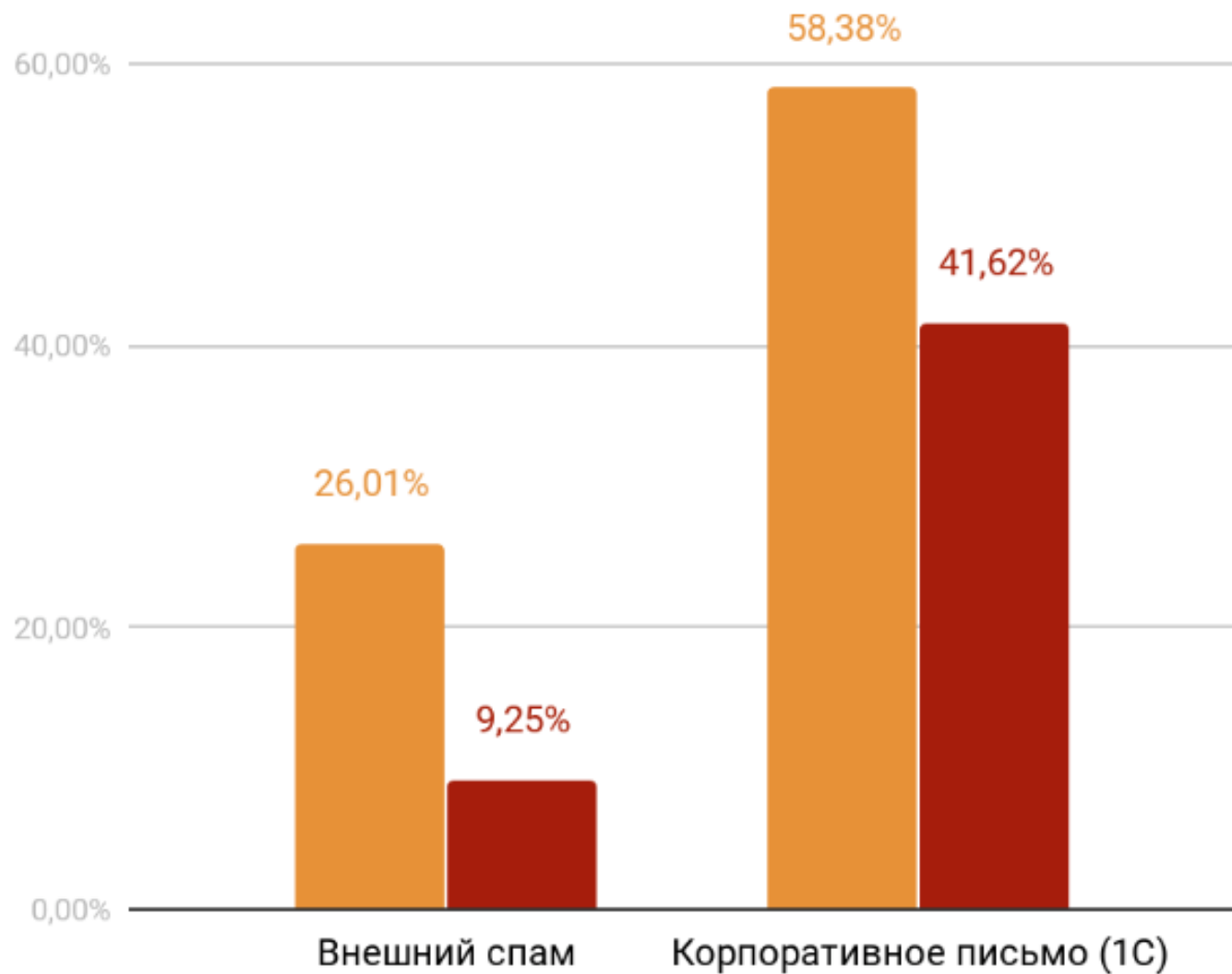
Жадность

Желание помочь

antiphish.ru/classification



Самая опасная атрибуция



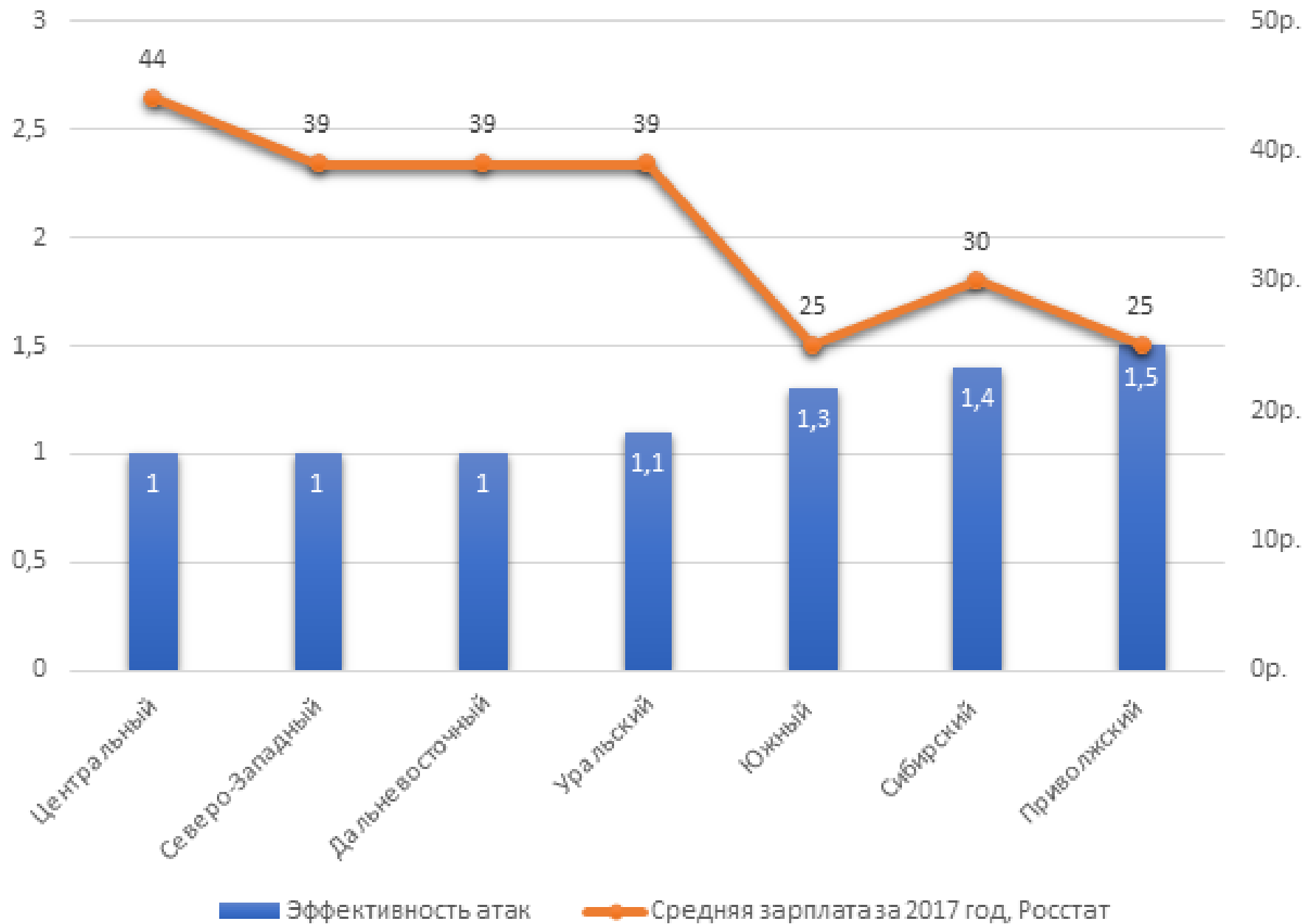
Значимые личностные черты

- 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





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.

НУ ЭТО УЖЕ ПЕРЕБОР



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)

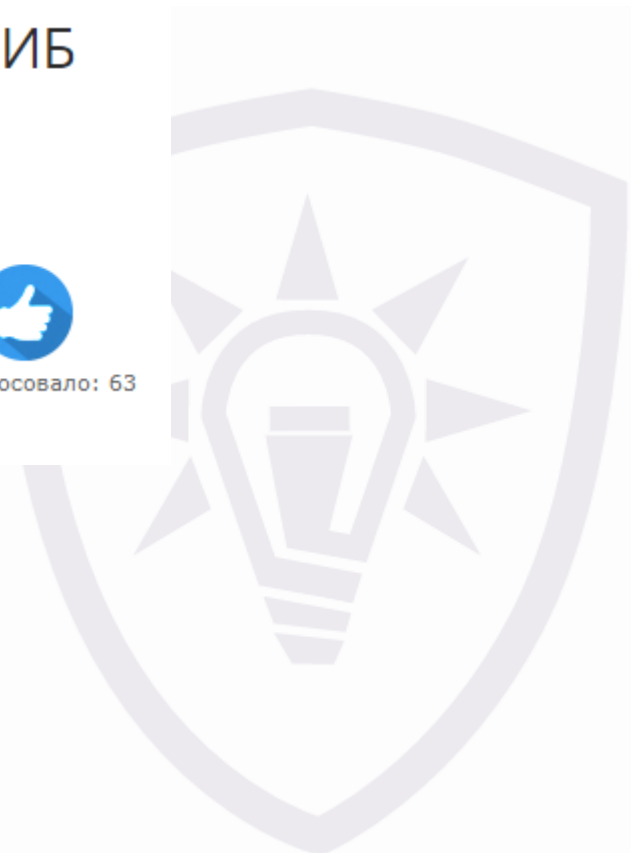


Сергей Горюнов

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	Detect
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 поднимать 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:



ЕЖЕМЕСЯЧНЫЙ МОТИВИРОВАННЫЙ ОПРОС ГРАЖДАН О ПЛАТЕЖНОЙ СИСТЕМЕ ПАО СБЕРБАНК РОССИИ.
ОСТАВЬТЕ СВОЕ МНЕНИЕ И ПОЛУЧИТЕ ВОЗНАГРАЖДЕНИЕ ДО 600 000 РУБ

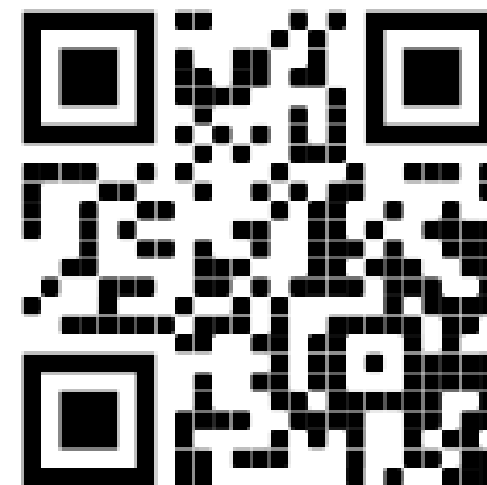


Денежных бонусов
осталось: 75



Выплачено бонусов за
месяц:
34763841 руб

ПОМОГИТЕ КОМПАНИИ ПАО СБЕРБАНК УЛУЧШИТЬ КАЧЕСТВО СЕРВИСА, ОТВЕТИВ НА НЕСКОЛЬКО ПРОСТЫХ ВОПРОСОВ И



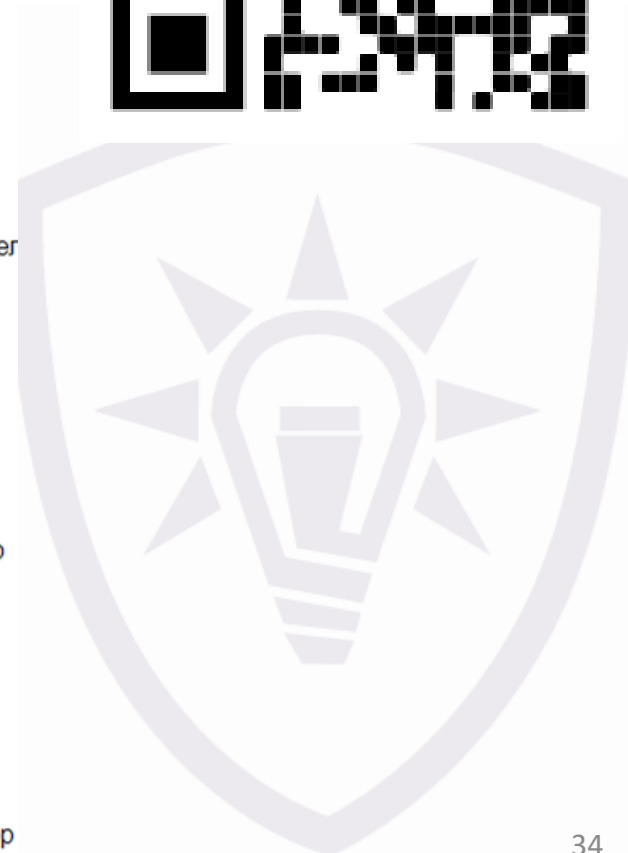
Андрей Жаркевич
редактор, ИТ-руководитель



Артеми́й Богданов
технический директор



Сергей Волдохин
выпускающий редактор

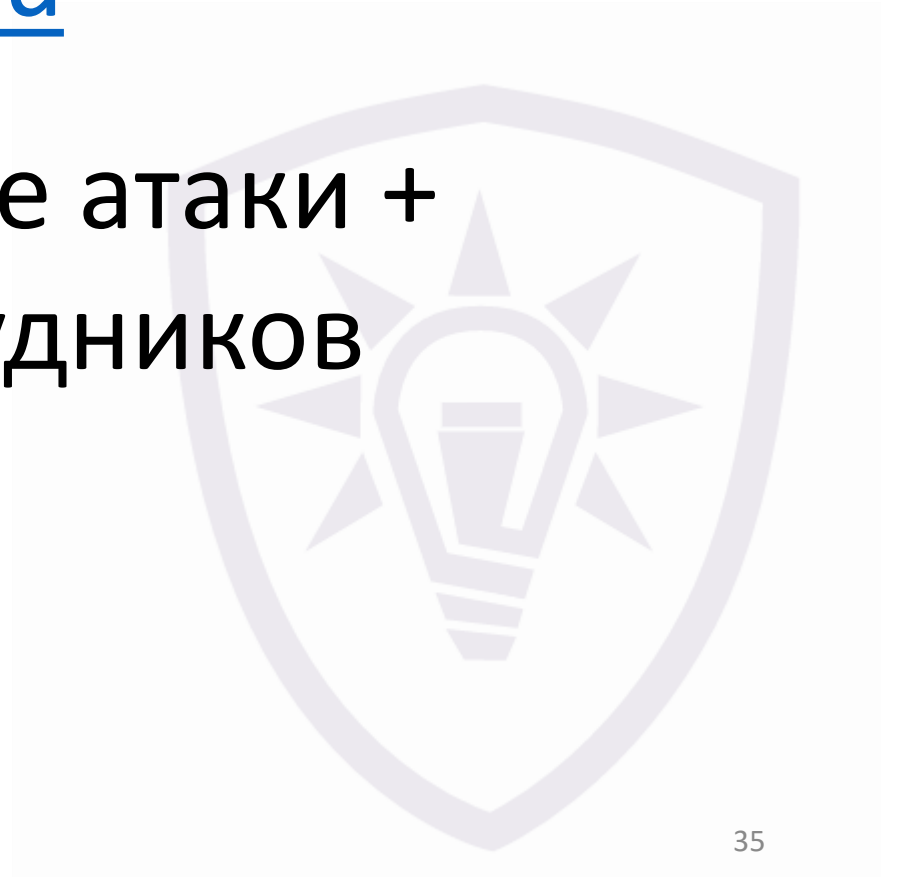


Присоединяйтесь к исследованиям



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