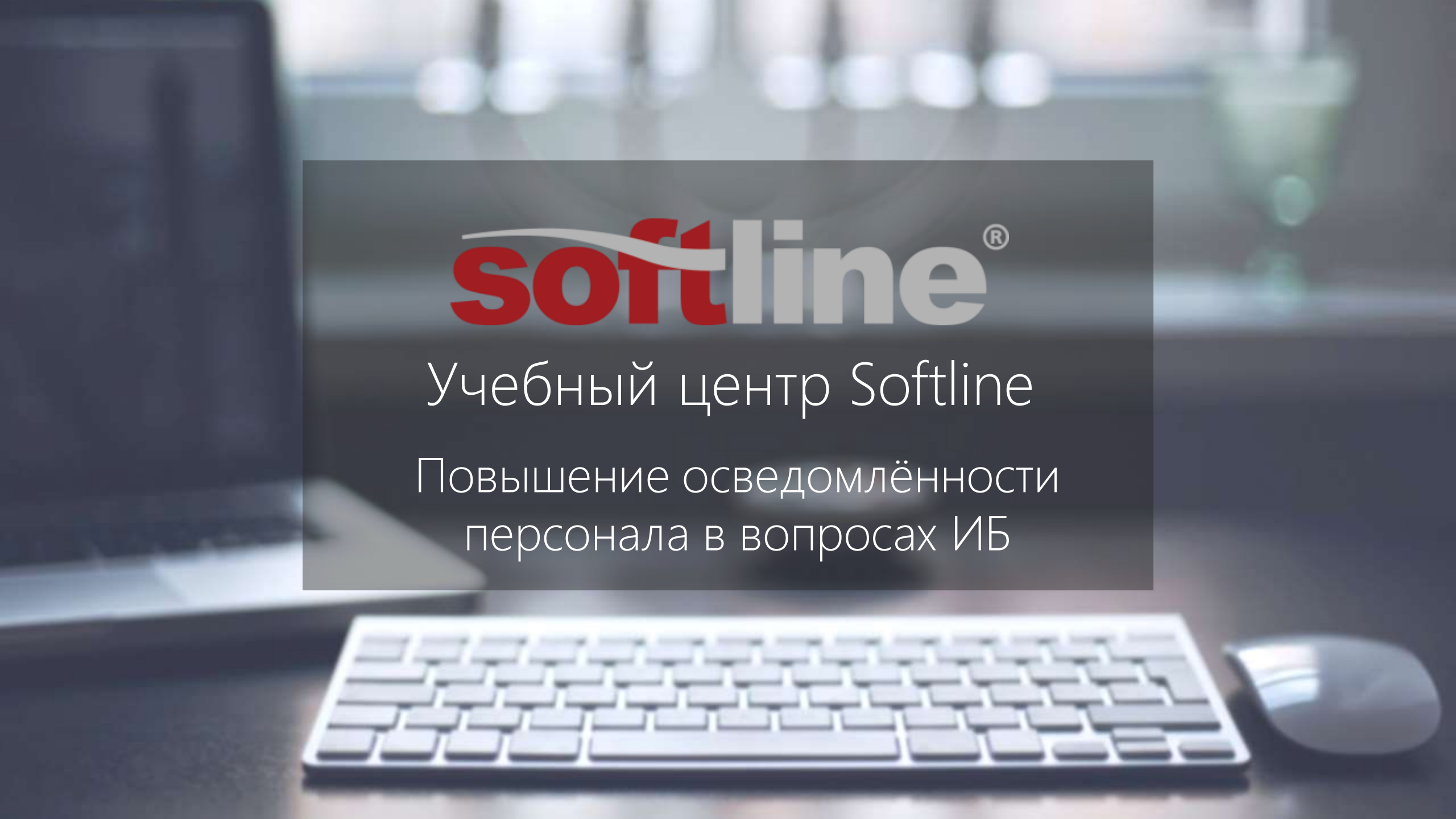


softline®

Учебный центр Softline

Повышение осведомлённости персонала в вопросах ИБ

Спикер

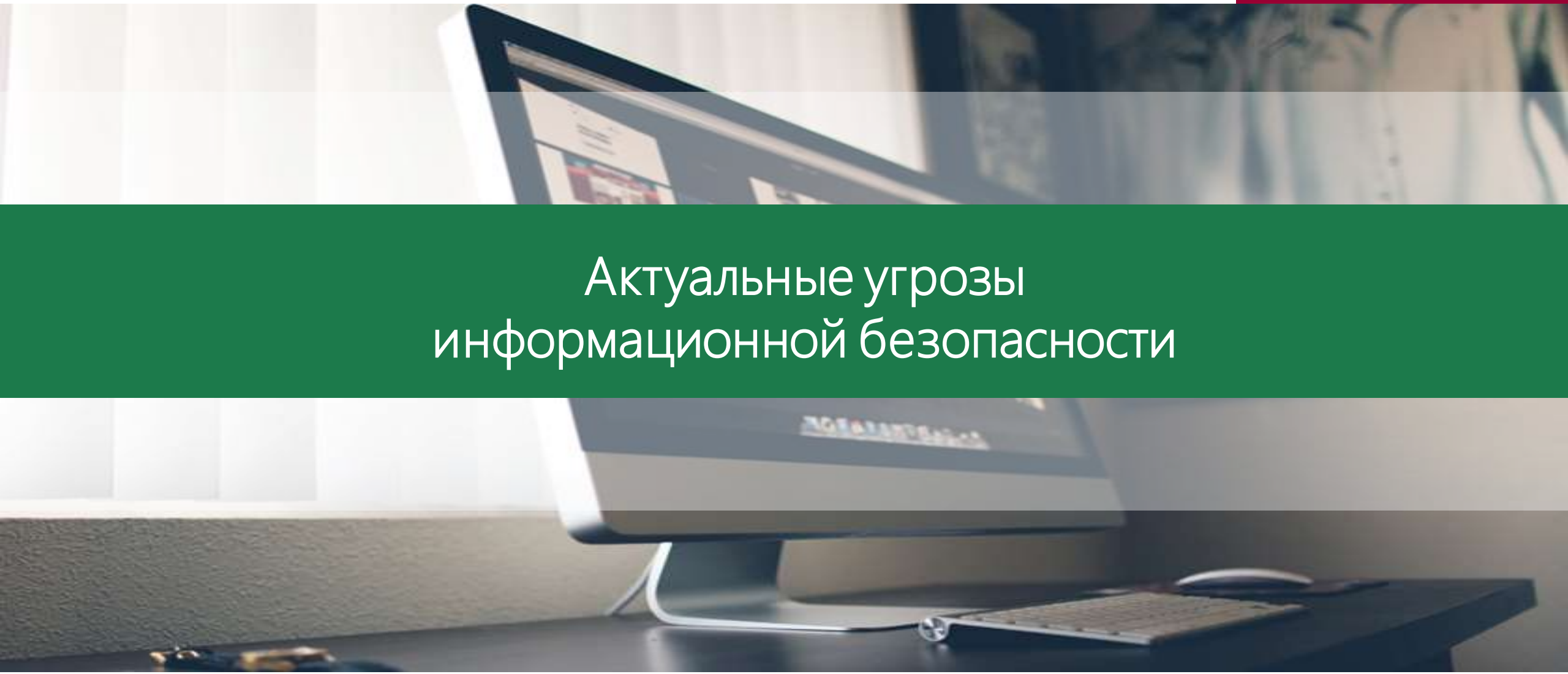
Учебный центр

Земцов Иван
- Инженер, преподаватель, Softline
- Старший преподаватель кафедры безопасности информационных технологий СибГУ им. М.Ф. Решетнева.

Образование:
Магистр,
Информационная безопасность, СибГУ им. М.Ф. Решетнева

Опыт:
заведующий сектором информационной безопасности КГПУ им. В.П. Астафьева.
вед. специалист, ФГБОУ ВО СибГУ им. М.Ф. Решетнева.
преподаватель, информационная безопасность, Аэрокосмический колледж.

Учебный центр

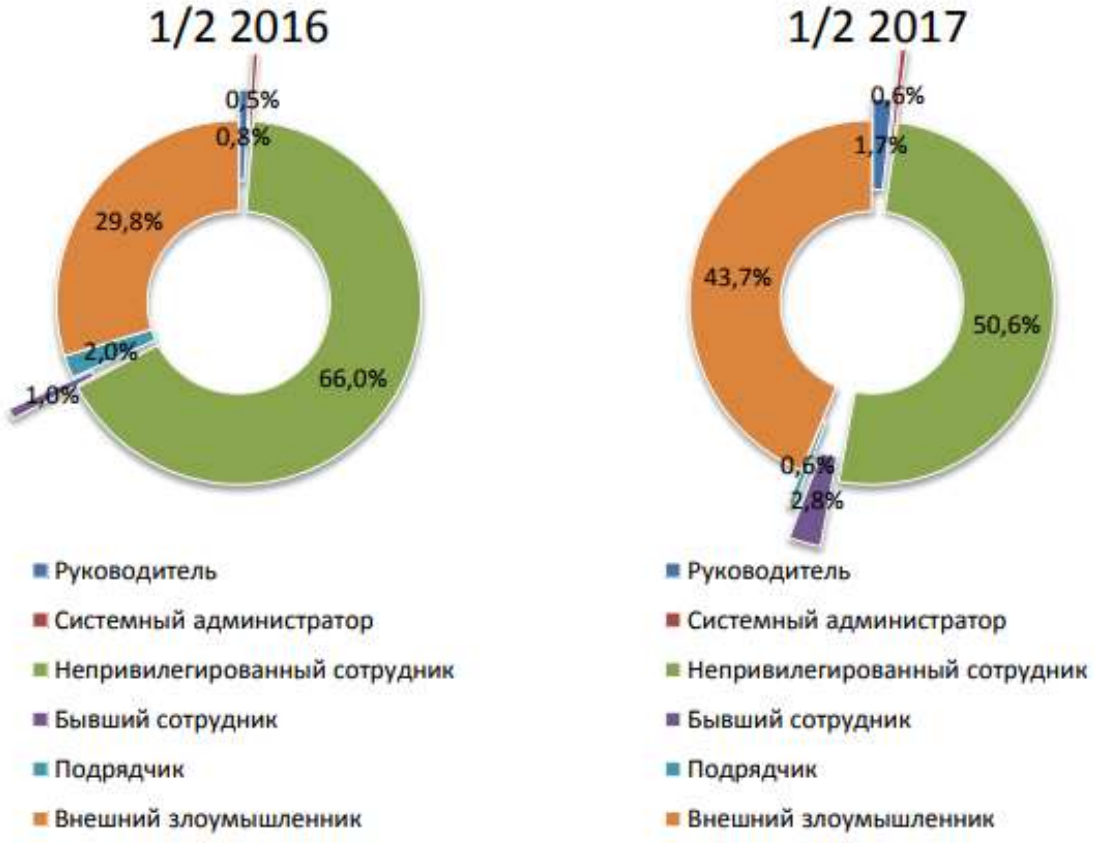


Актуальные угрозы информационной безопасности

Источники утечки информации

Учебный центр

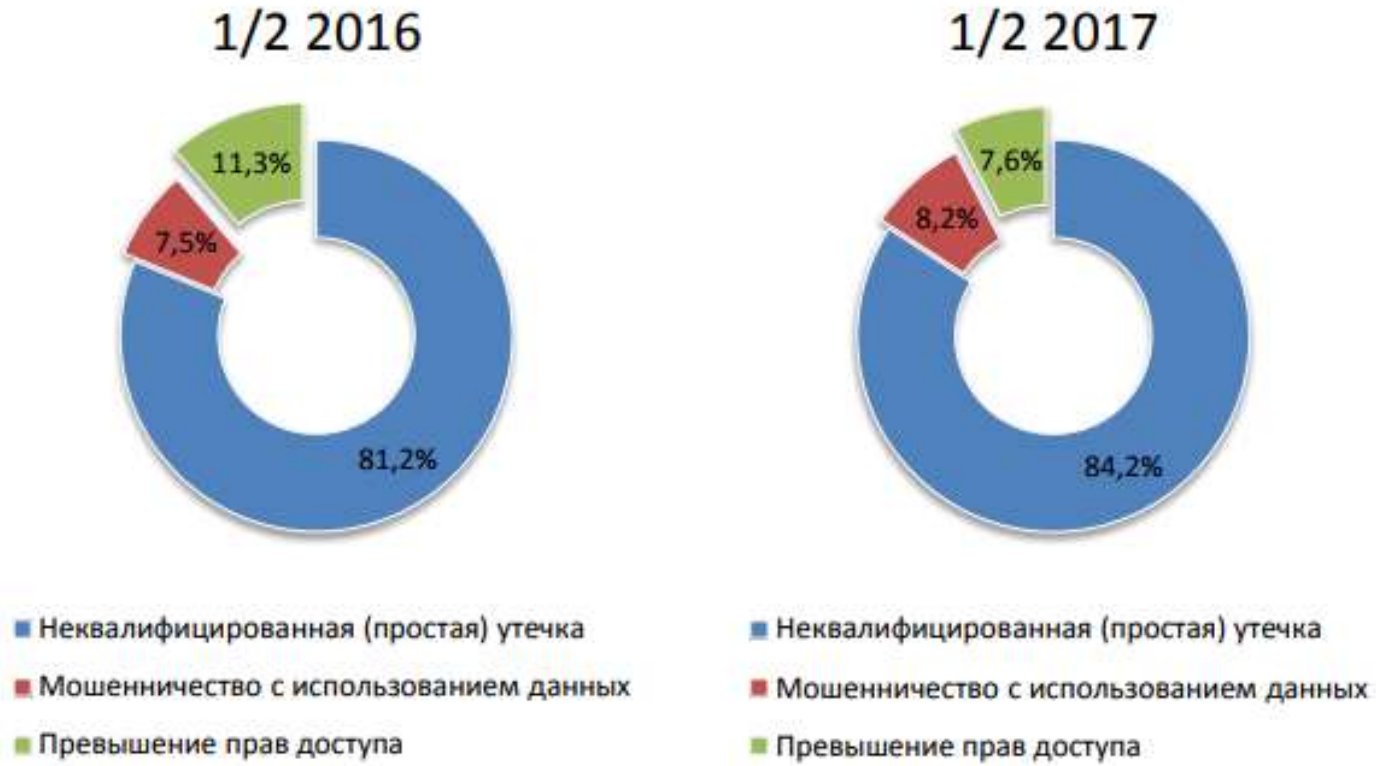
По данным компании Infowatch **собственные сотрудники** являются основным **источником утечки информации**.



Источники утечки информации

Учебный центр

По данным компании Infowatch **84%** зафиксированных **утечек** относятся к типу **неквалифицированных**. Они не сопряжены с дополнительными нарушениями — **отсутствует превышение прав доступа** или использование данных в целях мошенничества.



Источники утечки информации

Учебный центр

Пользователи являются частью информационной системы организации.

У пользователей часто отсутствуют:

- **знания** в сфере ИТ и ИБ;
- **навыки использования инструментов** защиты информации;
- **привычки** безопасной работы.

Источники утечки информации

Цель повышения осведомлённости: **повышение реального уровня информационной безопасности** организации путем формирования **безопасного поведения** персонала в информационном пространстве.

Задачи:

- дать полезные **знания** в сфере ИТ и ИБ;
- показать эффективные **инструменты** защиты информации и способы их использования;
- выработать **привычки безопасной работы**.

Источники утечки информации

Учебный центр

По данным компании Infowatch основные каналы утечки информации – ресурсы сети Интернет (сайты, электронные письма).

Привычка 1. Проверять ссылки

Учебный центр

Знания. Проще всего определить фишинговый сайт по его адресу.
Например, обратите внимание на адреса этих фишинговых сайтов, которые выглядят как сайты сервисов Яндекса:

Привычка 1. Проверять ссылки

Знания. Доменная адресация в сети.
Адрес в сети состоит из доменных имен разного уровня разделенных точкой.
Большинству популярных сайтов принадлежит имя второго уровня.
Например:

Yandex.ru

Yandex – доменное имя второго уровня.
Ru – доменное имя первого уровня, также называется зоной сети.

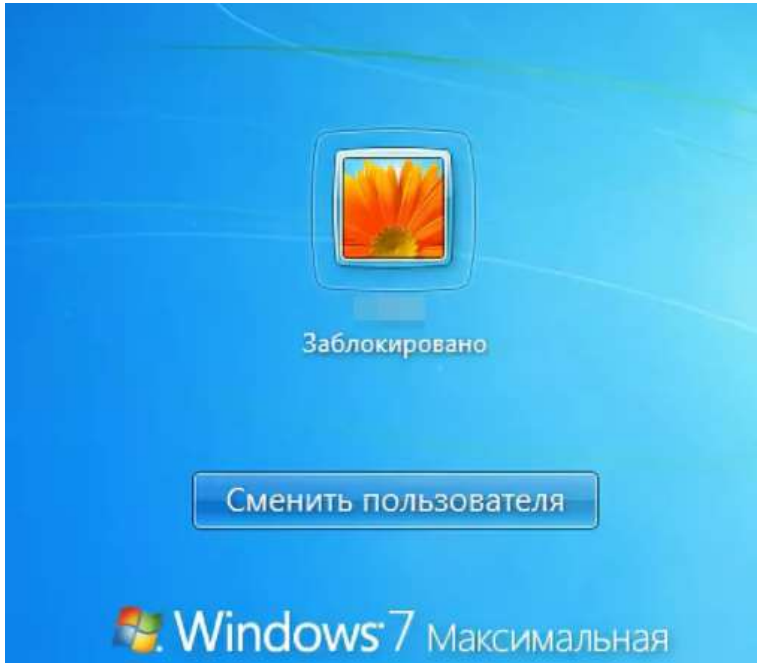
После имени первого уровня может идти только «/»!
До имени первого уровня могут располагаться имена других уровней разделенные точкой. Имя второго уровня при этом не меняется!
Во всех других случаях вас обманывают!

Привычка 2. Блокировать компьютер

Учебный центр

Знания. Политика чистого экрана.

При каждом оставлении компьютера без присмотра – блокируйте.

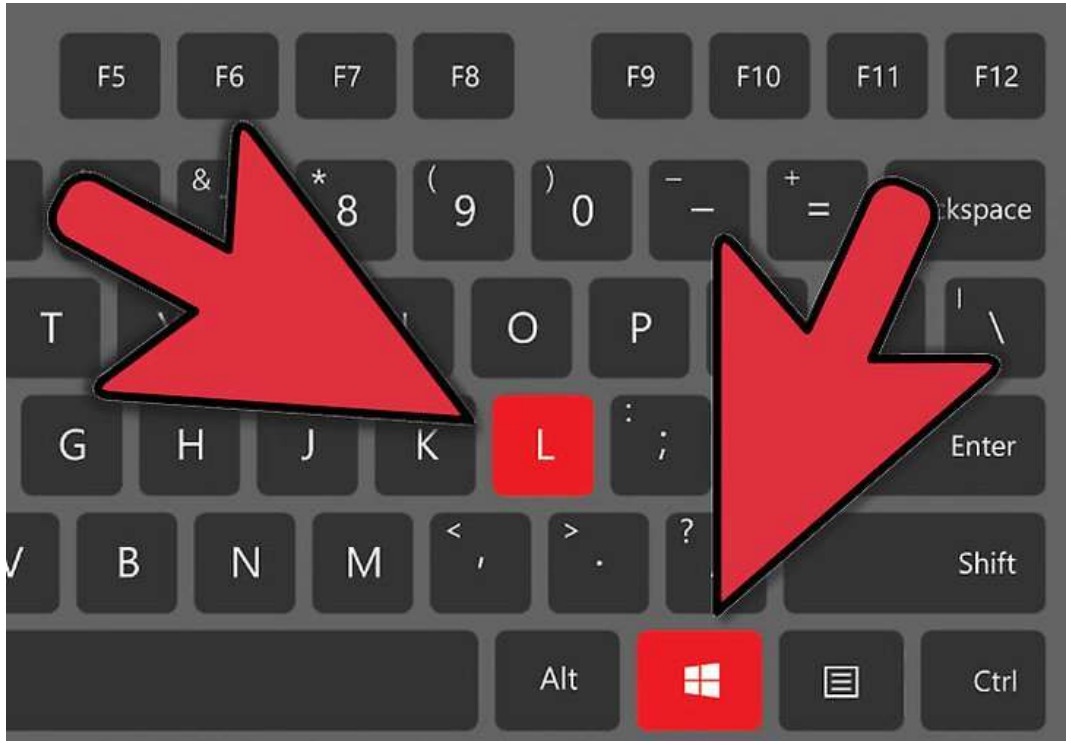


Привычка 2. Блокировать компьютер

Учебный центр

Инструмент. Win+L.

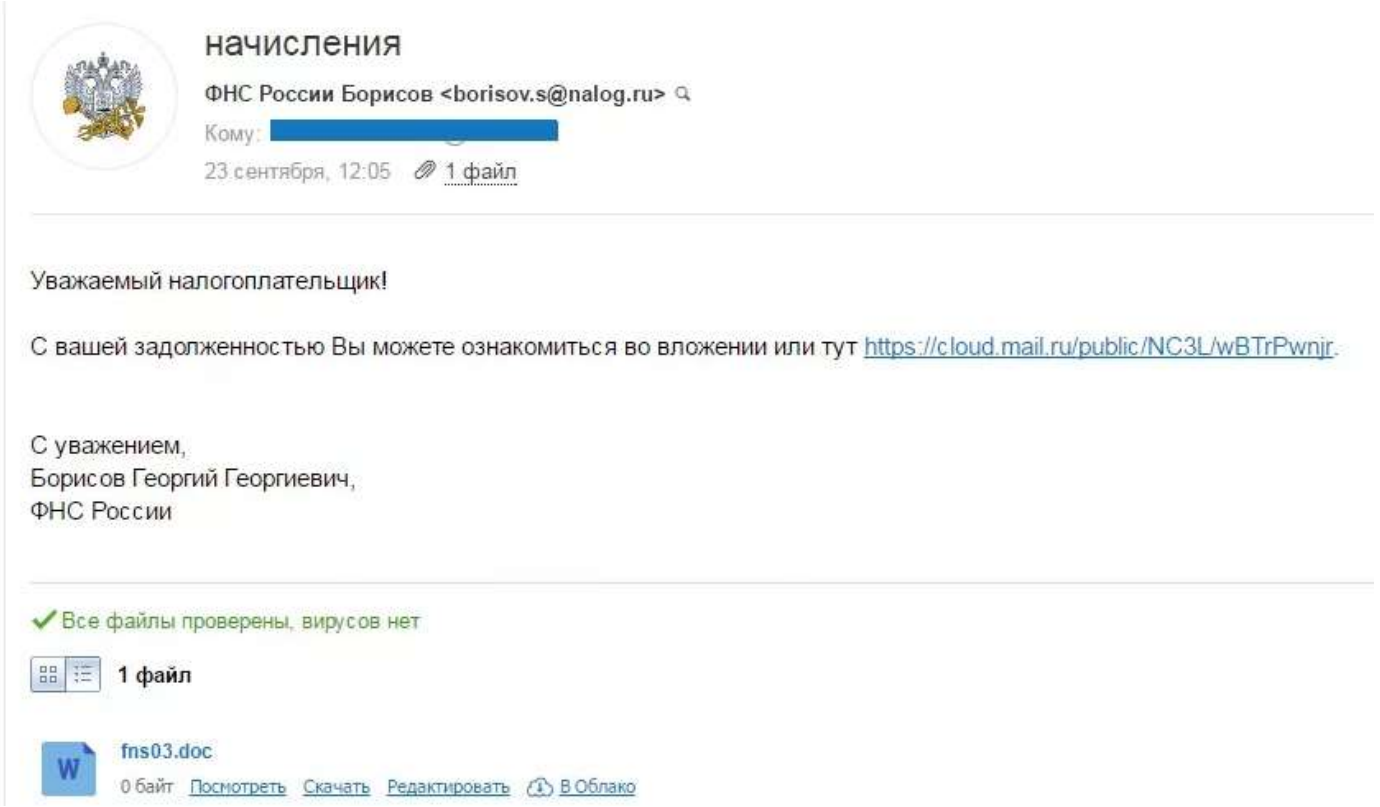
Заблокировать Windows – Windows Lock – Win+L



Привычка 3. Проверять отправителя

Учебный центр

Знания. Подделать сообщение электронной почты очень просто.
Все видимые пользователю признаки официального письма легко подделать.

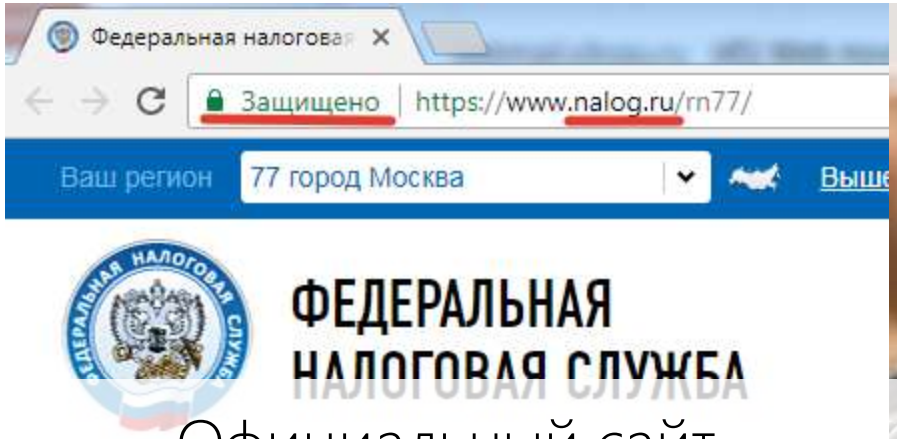


Совет 3. Проверяйте отправителя

Учебный центр

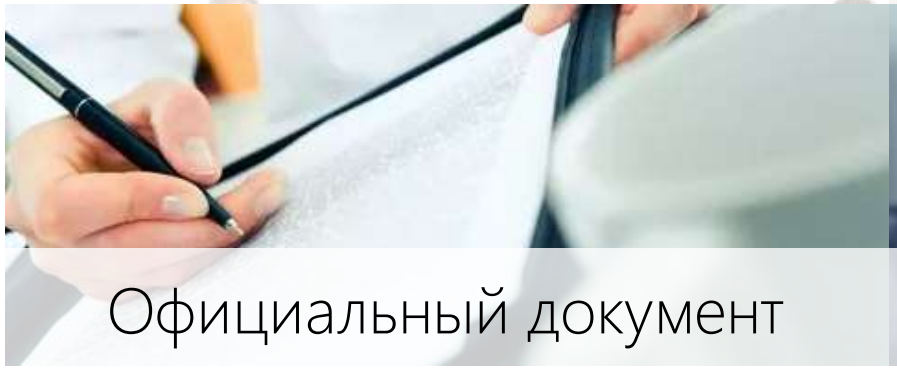
Инструменты. Достоверные источники.

Проверяйте информацию из проверенных достоверных источников.



Официальный сайт

Обратный звонок



Официальный документ

Личная встреча

Привычка 4. Разделять пространства

Учебный центр

Знания. Личные данные на рабочем месте проблема и компании и работника.
При пользовании рабочими устройствами в личных целях утечка происходит в обе стороны!

Привычка 4. Разделять пространства

Учебный центр

Инструменты. Личные и рабочие устройства, носители, аккаунты.

Разные аккаунты

Отдельные адреса

Личные устройства

Защищенные носители

Привычка 5. Проверять полномочия

Знания. Для доступа к информации необходимо иметь допуск.

Допуск - это процедура оформления права лиц на доступ к информации.

Допуск к информации не всегда соответствует занимаемой должности или выполняемым обязанностям.

Допуск ограничен во времени и может истечь или не начаться.

Допуск не может передаваться другому лицу.

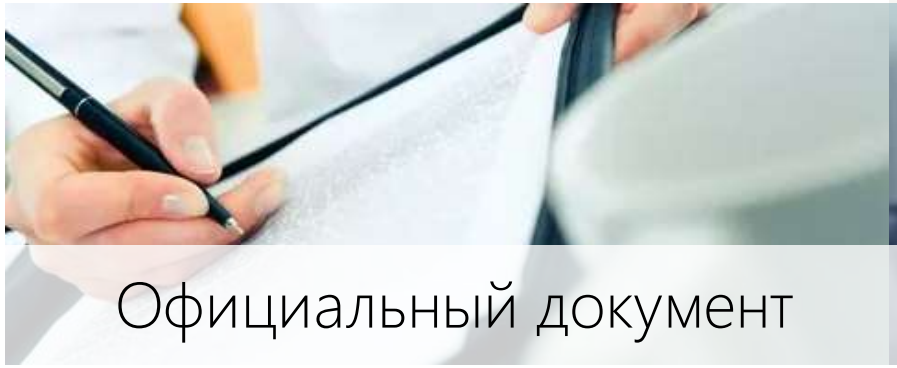
Привычка 5. Проверять полномочия

Учебный центр

Инструменты. Достоверный источник полномочий удостоверение, документ, служба безопасности, руководитель.

Удостоверение

Служба безопасности



Официальный документ

Руководитель

Привычка 6. Поддерживать порядок

Знания. Порядок – основа безопасности.

У каждого документа или файла должно быть свое место.

Место должно соответствовать требованиям безопасности.

Все файлы и документы нужно убирать на место каждый раз, когда беретесь за другое дело.

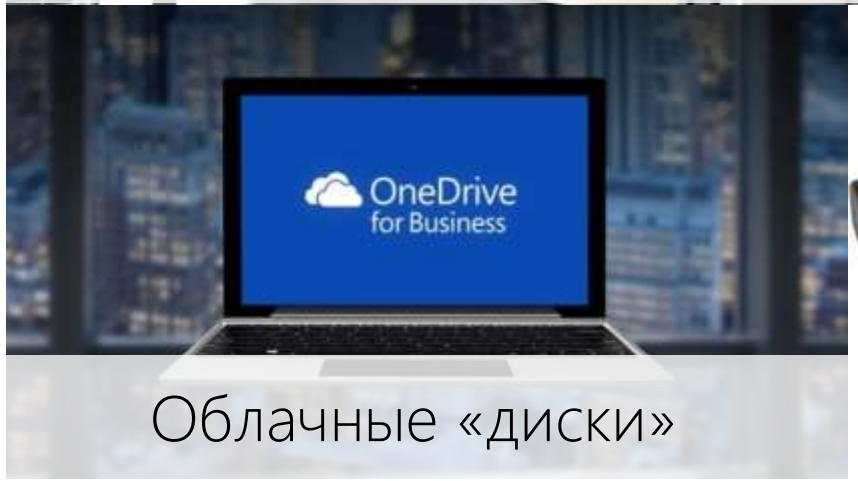
Привычка 6. Поддерживать порядок

Учебный центр

Инструменты. Места архивного и оперативного хранения.

Запирающиеся шкафы

Запирающиеся тумбы



Облачные «диски»

Защищенные носители

Привычка 6. Поддерживать порядок

Учебный центр

Инструменты. Политика чистого стола.

Документы только для одной задачи!

Привычка 7. Запомнить алгоритм

Учебный центр

Знания. Использование своего алгоритма формирования пароля позволяет формировать и «запоминать» много сложных паролей.

- Использование парольных фраз для формирования паролей.
- Использование правил формирования парольной фразы.

Пример.
В организации используется 5 сервисов с разными паролями. К каждому сервису установлены требования сложности. Пароли меняются раз в 90 дней.
Длина пароля не менее 8 символов.

В год 20 паролей (и это только рабочих)!

Парольная фраза:

(название сервиса) + (время года) + (год по китайскому календарю) + (свое слово) = 1Ска зимой собака глючит = 1Crpbvcj,uk. (1Скзимсобглю)

У каждого алгоритм должен быть свой!

Привычка 8. Дружить с безопасниками

Знания. Контакты службы безопасности и опасные ситуации.

Работникам должны быть всегда **доступны актуальные контакты** службы безопасности.

Должны быть **сформулированы обстоятельства**, при наступлении которых необходимо обращаться к безопасникам (опасные ситуациии).

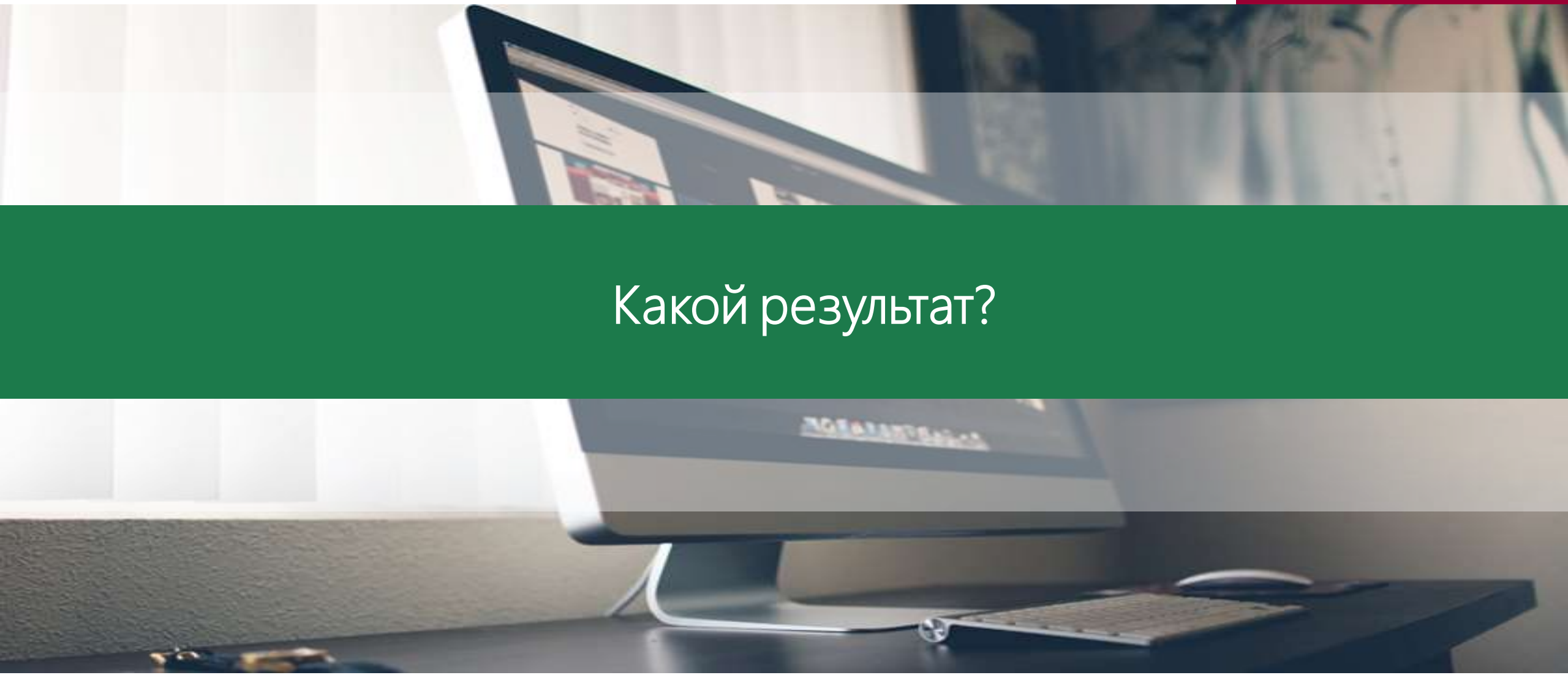
Привычка 8. Дружить с «безопасниками»

Знания. Опасные ситуации.

- ✓ Пришло письмо странного содержания (например, от доверенного источника, но с необычной просьбой).
- ✓ Пришел человек, требующий выдать информацию, и при этом нет возможности проверить его полномочия.
- ✓ Необычное «поведение» техники.
- ✓ Много спама.
- ✓ и т.п.

Безопасное поведение

1. Проверять адрес сайта.
2. Блокировать компьютер.
3. Проверять отправителя.
4. Разделять пространства.
5. Проверять полномочия.
6. Поддерживать порядок.
7. Запомнить алгоритм формирования пароля.
8. Дружить с безопасниками.



Какой результат?

Уровень защищённости

Учебный центр

Методы контроля в зависимости от целей

Знания ваших сотрудников -
безопасность вашего бизнеса!

Учебный центр

Перечень услуг в рамках комплексного проекта:

- Консалтинг – оценка текущего состояния осведомлённости сотрудников, профессиональных компетенций, проведение санкционированных провокационных рассылок, аттестация, и др.
- Разработка очных курсов;
- Разработка электронных учебных курсов;
- Разработка видео/флеш роликов, видео-уроков;
- Разработка методик оценки эффективности комплекса мероприятий по повышению осведомленности персонала компании по ИБ;
- Разработка листовок, брошюр, памяток, плакатов, скринсейверов;
- Подписка на библиотеку типовых электронных курсов по ИБ;
- LMS/СДО (возможна поставка, аренда)

В партнёрстве с Phishman

PHISHMAN

Учебный центр Softline помогаем повысить уровень осведомлённости следующим группам персонала

- **Основной группе** – сотрудникам, партнерам и консультантам компании, которые имеют доступ к активам компании.
- **Техническим специалистам** – специалистам отдела информационных технологий и ИБ, разработчикам программного обеспечения, службе технической поддержки и другим техническим специалистам.
- **Топ-менеджерам** – руководству компании, начальникам отделов, руководителям проектов.

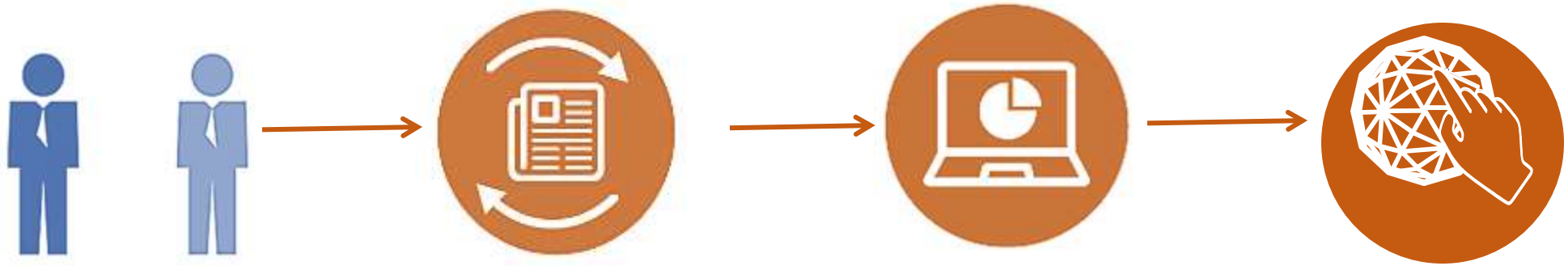
Выгоды от внедрения комплексного проекта

- оперативное ознакомление всех сотрудников с существующей документацией, регламентирующей вопросы ИБ в Компании
- снижение рисков возникновения инцидентов по вине сотрудников
- накопление и сохранение интеллектуального капитала в Компании
- повышение ответственности сотрудников компании за совершение действий/бездействий при возникновении предпосылок для инцидентов ИБ
- дополнительная мотивация сотрудников компании соблюдать требования по защите информации

Знания ваших сотрудников -
безопасность вашего бизнеса!

Учебный центр

Четыре простых шага для реализации комплексного проекта



Заполнить бриф-анкету

Выбрать подходящий вариант реализации

Утвердить концепцию решения

Реализовать проект

Не ждите, пока незнание обойдётся слишком дорого!

ВОПРОСЫ?

8 800 505 05 07 edu.softline.ru edusales@softline.ru