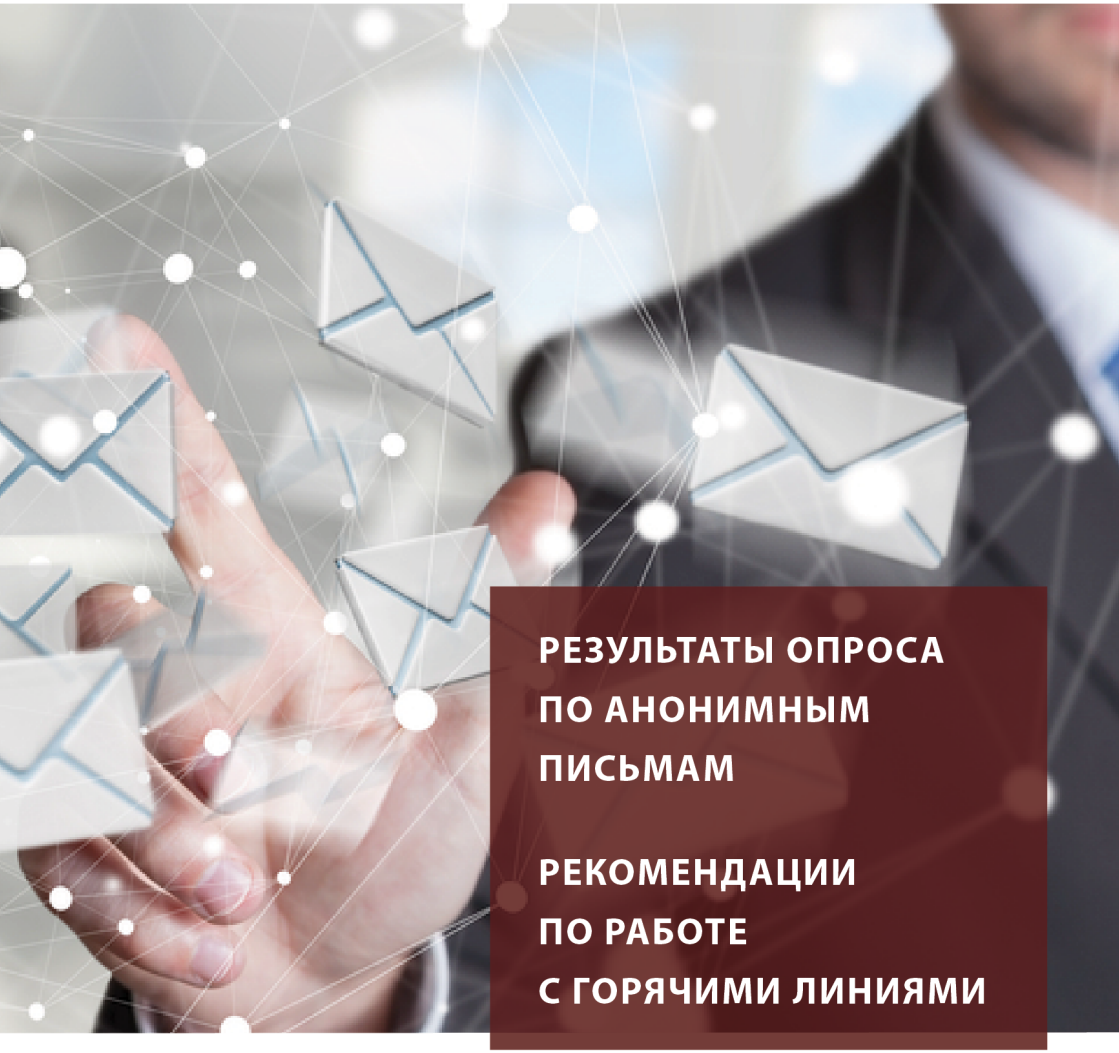
ПОДБИРАЕМ КЛЮЧИ К ЛЮДЯМ

НИЦКБ

ТЕМА ИССЛЕДОВАНИЯ: №1017

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ РАССЫЛКИ АНОНИМНЫХ ПИСЕМ



РЕЗУЛЬТАТЫ ОПРОСА ПО АНОНИМНЫМ ПИСЬМАМ

РЕКОМЕНДАЦИИ ПО РАБОТЕ С ГОРЯЧИМИ ЛИНИЯМИ

WWW.SRCCS.SU

ПОДБИРАЕМ КЛЮЧИ К ЛЮДЯМ

НИЦКБ

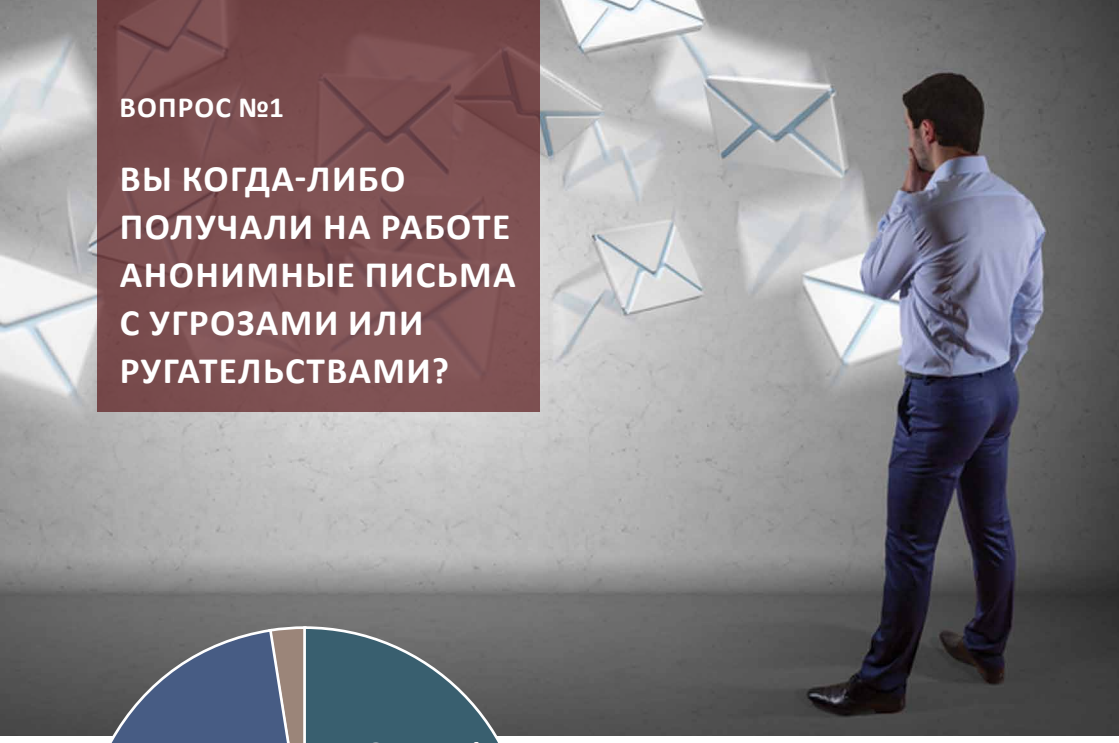
В ИССЛЕДОВАНИИ УЧАСТВОВАЛИ:

Руководители служб безопасности, внутренние аудиторы, юристы, владельцы и собственники бизнеса.

О ТЕМЕ:

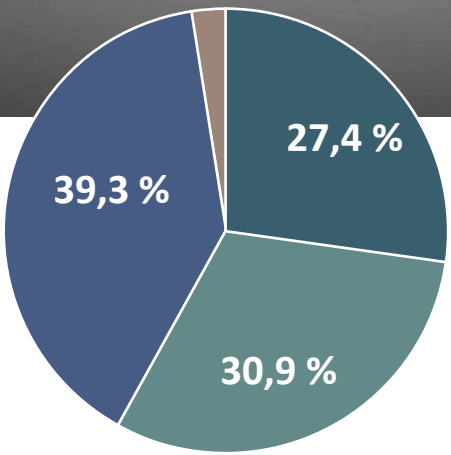
В этом году к нам часто обращались за расследованием инцидентов, связанных с анонимными письмами.
Поскольку эта тема имеет множество граней и сложностей мы решили провести исследование, собрать опыт различных специалистов и систематизировать его. Данная методичка поможет Вам принять правильные решения, если вы столкнётесь с подобной проблемой.
Также здесь рассмотрены рекомендации и стратегия внедрения Линии доверия в компании.

2017
Москва



ВОПРОС №1

ВЫ КОГДА-ЛИБО ПОЛУЧАЛИ НА РАБОТЕ АНОНИМНЫЕ ПИСЬМА С УГРОЗАМИ ИЛИ РУГАТЕЛЬСТВАМИ?

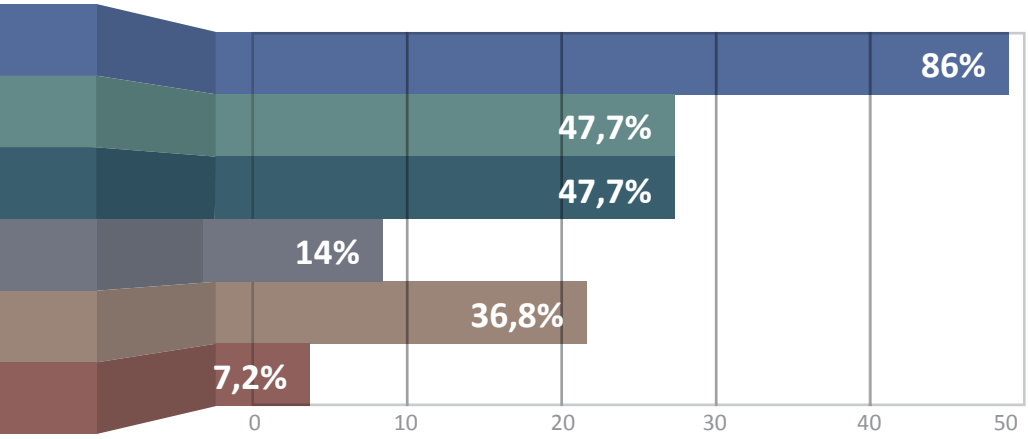


- Нет, никогда не сталкивался и ничего не знаю о подобном
- Получали коллеги/родственники друзья, я - нет
- Да, получал на свою почту (корпоративную почту)
- Другое

Данная проблема имеет две стороны медали. С одной стороны человек хочет нанести вред, и, чаще всего, мотивы отправки анонимного письма – получить какую-то выгоду. В этом году наша команда расследовали около 12 эпизодов получения «анонимок», в каждом из случаев были репутационные или финансовые риски для компании.

С другой стороны – это один из способов получения информации, некоторые сотрудники не знают, как обратиться с проблемой или боятся публичного разоблачения, хотя их мотивы: быть услышанным.

ПО ВАШЕМУ МНЕНИЮ ЗАЧЕМ ДЕЙСТВУЮЩИЙ/ УВОЛИВШИЙСЯ СОТРУДНИК МОЖЕТ ОТПРАВЛЯТЬ АНОНИМНЫЕ ПИСЬМА КОЛЛЕГАМ?



Его чем-то обидели условия работы (зарплата, отношение коллег/начальства)

Он не лоялен к компании и хочет навредить коллективу (вызвать ссоры, конфликты, увольнения)

Он располагает информацией о чьих-то нарушениях, но хочет сохранить анонимность

Ему просто хочется внимания или нечем заниматься

Он отчаялся, что иными путями не может обратить внимание на существующую проблему или идею

Другое

Главное на этом этапе учитывать, что любое поведение возможно прогнозировать. Сам факт письма уже информация. Психолингвистика текста может дать множество информации: эмоциональное состояние, особенности мышления, реальные мотивы.

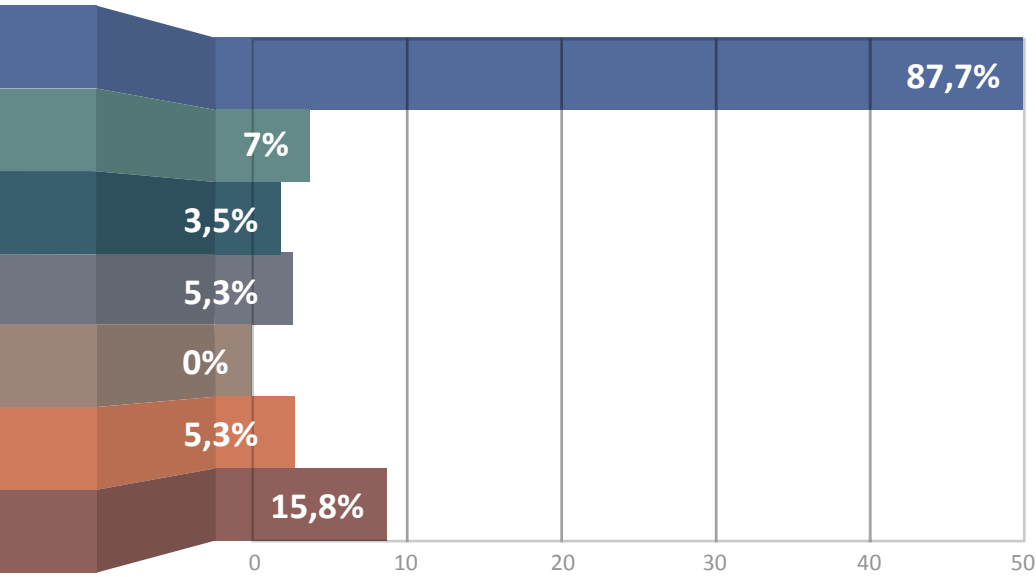
КАКИЕ РИСКИ МОГУТ ВОЗНИКНУТЬ У КОМПАНИИ?

- Репутационные
- Моральные (сотрудники будут чувствовать неопределенность и неизвестную угрозу)
- Увольнения из-за содержания писем
- Никаких рисков это не представляет
- Самосуд или попытки расследования собственными силами
- Проверки контролирующих органов, которым могли отправить подобные анонимные письма

Отдельного внимания заслуживают факты анонимных писем поступающих от ущемленных в чем-то партнеров (потенциальных партнеров), которые сообщают о фактах нарушений сотрудниками компании.

Комментарий участника Online опроса

КАК СТОИТ ОТНОСИТЬСЯ К ПОЛУЧЕНИЮ АНОНИМНЫХ ПИСЕМ?



Сообщить о данном факте в службу безопасности компании и руководству

Рассказать коллегам о произошедшем

Написать автору в ответ

Заявить в полицию

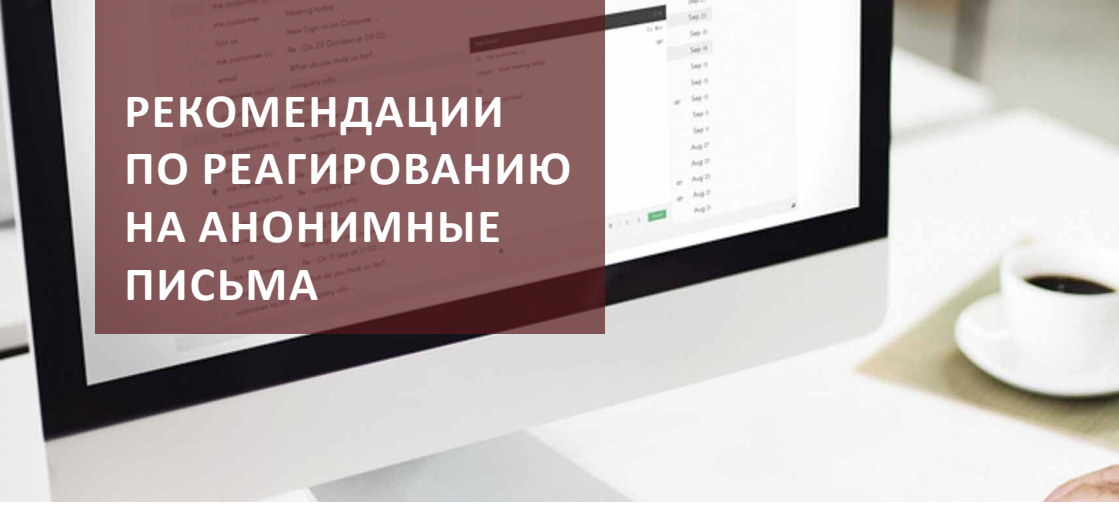
Открыто обвинить предполагаемого автора

Никому не сообщать, просто не обращать внимание

Провести собственное расследование

НЕОБХОДИМО ЛИ УСТАНАВЛИВАТЬ АВТОРА ПИСЬМА?

- Это зависит от информации в письме
- Нет, это личное мнение автора, он имеет право на подобное
- Индивидуально, аналогично предыдущему письму
- Да, поскольку надо установить его мотивы и наказать
- Да, но не стоит на это тратить много ресурсов



РЕКОМЕНДАЦИИ ПО РЕАГИРОВАНИЮ НА АНОНИМНЫЕ ПИСЬМА

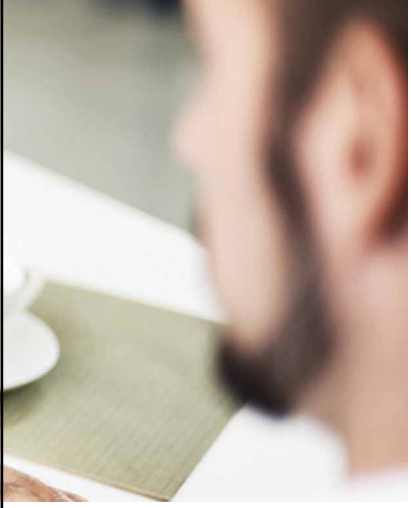
ПЕРВЫЕ ШАГИ

1. **Письмо можно отследить.** По нашим данным только 40-45% пользуются VPN или анонимайзерами. Чаще всего анонимные письма отправляются не с рабочего места (в ТОПе – домашний интернет, кофейни, торговые центры), около 90% писем отправляется в выходные дни. Первый шаг – это внутренними ресурсами IT-департамента посмотреть технические характеристика письма, возможно там остались следы.

2. **Ищите кому это выгодно.** Как правило анонимное обращение появляется спустя неделю – месяц после события, в редких случаях - в тот же день. За счет анализа оперативной информации и карты слухов возможно сократить количество подозреваемых.

3. **Реагируйте.** Если не будет реакции со стороны компании на анонимку, в которой содержатся факты и имена, то в 70% случаев человек продолжает писать «анонимки», либо отправляет жалобы в контролирующие органы (налоговая, трудовая, ОБЭП и др.). Поэтому вариант не обращать внимание может увеличить количество рисков и их последствия.

Большинство писем отправляют недавно уволенные сотрудники, свидетели частых нарушений, завистники и лишенные бонусов/премий.



Когда мы получаем анонимку, мы работаем в двух направлениях: ищем кому это выгодно и подтверждается ли информация.

Руководитель
СБ. Банковский сектор

ОЦЕНКА СОДЕРЖАНИЯ ПИСЬМА

1. По психолингвистике возможно понять пол, возраст, эмоциональное состояние и понять часть особенностей характера. Обратите внимание на термины, речевые обороты, орфографию.

2. Оценка контента может определить мотив (чаще всего обида, зависть, раздражение). Обратите внимание на фразы, конструкции предложений и тон письма.

3. Какие сотрудники и как упоминаются, нужно понять - это внутренний человек или внешний.

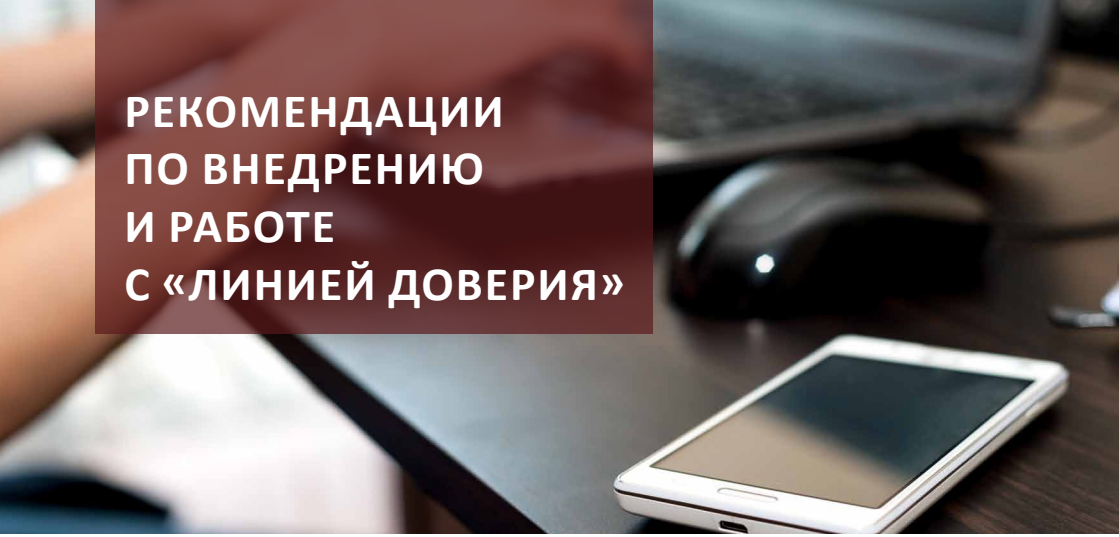
4. Если вы понимаете, что в письме много угроз и возникают существенные риски (репутационные, финансовые), то реагировать нужно оперативно.

ВАРИАНТЫ

• Отправить письмо в ответ. За счет подкрепляемой картинки или файла можно деанонимизировать автора письма. Также нужно проанализировать цифровые следы. Обратитесь в отдел IT.

• Нужно предотвратить распространение информации об инциденте в компании, поскольку это может спровоцировать скандалы и обвинения.

• Посмотрите на внутренние источники информации, возможно подобная тема поднималась ранее.



РЕКОМЕНДАЦИИ ПО ВНЕДРЕНИЮ И РАБОТЕ С «ЛИНИЕЙ ДОВЕРИЯ»

Линия доверия (или как иногда называют – Горячая линия) – наиболее эффективный инструмент противодействия анонимным письмам. Любой сотрудник получает возможность сообщить о противоправных действиях, нарушениях или угрозах.

ЛИНИЯ ДОВЕРИЯ РЕШАЕТ НЕСКОЛЬКО ЗАДАЧ

1. Получение информации от сотрудников различных уровней о различных инцидентах.
2. Повышение лояльности сотрудников, поскольку линия доверия позволяет регулярно получать информацию о трудностях или нарушениях.
3. Дополнительные превентивные и профилактические меры по снижению рисков воровства, сливов информации, мошенничества и др.

Абстрагироваться от ассоциации с тем, что стучать плохо «Ты не стучишь, ты помогаешь». Горячая линия призвана продлить жизнь предприятия. Чем плох фрод – тем, что он влечет увольнения, потерю денег, нечем платить зарплату, компанию обворовали - приходится сокращать людей. А линия доверия помогает участвовать в жизни предприятия. Даже если вы менеджер по чистоте зала – вы можете участвовать в жизни компании.

Внутренний аудитор. Телеком компания

Если в вашей компании горячая линия или линия доверия предполагает только обращение при идентификации личности, то вы можете потерять часть важной информации.

Андрей Акиншин,
директор группы контроля рисков Агротерра

РЕКОМЕНДАЦИИ

1. Разработайте четкий план популяризации линии доверия: где размещать информацию, как это будет позиционироваться от руководства компании и сочетаться с корпоративной культурой.

2. Подберите компетентных операторов Линии доверия. Именно от них будет зависеть качество получаемой информации. Сотрудники должны быть терпеливы, гибки в общении и хорошо осведомлены о деятельности компании.

3. Используйте все внутренние ресурсы коммуникации (рассылки, газеты, доски объявлений, внутренние соц. сети и CRM) для оповещения о возможности. В России звонок на Линию может считаться «стукачеством» или «ябедничеством», тут будет важен момент донесения корпоративных ценностей.

ЧТО ДАЛЬШЕ?

В первые 3 месяца количество обращений может быть очень нестабильным и с множеством лишней информации.

Каждая заявка должна рассматриваться коллегиально. Правильнее, чтобы это делала рабочая группа, комплаенс комитет и т.д. состоящая из СБ, аудита, HR, юристов, как постоянных участников, так и дополнительных экспертов того направления, по которому поступила информация.

Руководитель СБ, FMSG

Линия доверия очень гибкий и интегрируемый инструмент. Постепенно отлаживая ее работу можно получить постоянный источник качественной информации.

О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОМ ЦЕНТРЕ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

ЛИЦЕНЗИЯ НА ПРАВО ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Научно-исследовательский Центр Корпоративной Безопасности ведет свою деятельность с 2012 года. Крупнейшая в СНГ компания на рынке профайлинга в корпоративной безопасности, имеющая опыт работы в различных сферах бизнеса.

Создателем и президентом центра является один из лучших в СНГ экспертов-практиков в области прогнозирования поведения, выявления и предотвращения манипуляций во время коммуникаций, идентификации истинных мотивов собеседника и детекции лжи - **Анна Кулик.**

УНИКАЛЬНАЯ КОМАНДА

Для вас работают лучшие специалисты в своих областях: профайлеры, графологи, полиграфологи, юристы и аудиторы, эксперты в сферах HR, кадрового делопроизводства, внутрикорпоративных расследований и противодействия финансовым махинациям, а также IT-безопасности.

КОНФИДЕНЦИАЛЬНОСТЬ

Центром обеспечиваются строгие условия сохранения конфиденциальности при работе с клиентами в части сохранения как коммерческих секретов компаний, так и самих персоналий наших клиентов. Значительная часть работы экспертов Центра носит закрытый характер и известна лишь нашим нанимателям.

www.srccs.s **+7 (499) 394 40 35** **mail@srccs.su**

ПРИМЕР КЕЙСА ПО РАССЛЕДОВАНИЮ АНОНИМНЫХ ПИСЕМ

ФАБУЛА

Руководитель службы безопасности одной их международных компаний обратился к экспертам НИЦКБ по факту получения двух анонимных писем на e-mail собственника. Письма содержали компрометирующие факты о ряде управлящих лиц компании.

Необходимо было изучить исходные данные письма и выяснить, откуда оно могло быть направлено, и кем, проанализировать содержимое письма на предмет фактов (конкретики), качества написания, пунктуации, использования определенных слов и других особенностей письменной речи с точки зрения психолингвистики, а также попытаться выяснить пол, степень осведомленности данного человека, составить психологический портрет и сузить круг дальнейших поисков.

РЕШЕНИЕ

После изучения информации, содержащейся в электронном письме, эксперты НИЦКБ выяснили, что электронный ящик был создан специально для отправления писем. Ранее он не использовался, а имя отправителя и возможное техническое устройство, с которого его отправили, установить не удалось.

Психолингвистика, стиль написания, использование фразеологизмов и пунктуации дали основание составить профиль личности автора письма. Исходя из содержания и фактов, было определено несколько лиц, которые имели доступ к данной информации, либо могли узнать о ней из слухов. При содействии собственника и службы безопасности данные личности были исследованы и круг, потенциально причастных, сузился до трех человек.

В дальнейшем был разработан план, образцы писем, чтобы войти в переписку с отправителем письма, узнать больше конкретной информации. Для этого эксперты НИЦКБ составили и выверили письмо исходя из психологических особенностей, подходивших всем трем участникам.

После проведения данного этапа работы осталось два потенциально возможных лица, которые могли отправить анонимные письма. Исходя из полученных результатов, были детализированы психологические портреты и даны рекомендации службе безопасности и юристам для дальнейшей беседы с данными лицами.

По итогам интервью виновник был найден, а руководству компании передана вся информация, полученная в ходе участия в расследовании.

Напоминаем, что все персонажи и места изменены.
Любые совпадения случайны.

РИСКИ ПРИ УВОЛЬНЕНИИ И ОСОБЕННОСТИ АУТПЛЕЙСМЕНТА В РОССИИ

ПРИМИТЕ УЧАСТИЕ В

ОПРОСЕ НА САЙТЕ

srccs.su/materialy

Если у вас интересные истории и кейсы, а также вы можете поделиться практикой и мнениями относительно рисков при увольнении, то мы приглашаем вас пообщаться за чашкой кофе!

ПОДБИРАЕМ КЛЮЧИ К ЛЮДЯМ

НИЦКБ

БЛАГОДАРИМ ЗА УЧАСТИЕ В ИССЛЕДОВАНИИ!

УЧЕБНЫЙ ЦЕНТР

Комплексная информационная поддержка пользователей систем международной информационной группы «Интерфакс»: СПАРК, СКАН, СПАРК-Маркетинг, D&B, АСТРА, X-Compliance, ЭФИР.Наши специалисты проводят мероприятия различного формата, в ходе которых помогают пользователям лучше понимать возможности наших систем и максимально эффективно использовать их в своей работе.

WWW.EVENT.INTERFAX.RU

MIATON IT COMPANY

Обеспечение безопасности каналов связи, проведение аудитов ИТ безопасности, защиты корпоративных сетей и внедрению отказоустойчивых информационных систем, включая решения по электронной почте, видео-конференц связи, виртуализации и т.д. Системная интеграции для компаний и пост проектное сопровождение решений.

WWW.MIATON.RU