


# Невидимые угрозы

По результатам исследования аналитического центра SearchInform, которое проводилось весной этого года, эксперты выяснили, что уровень информационной защищенности московских компаний в 2014 году стал значительно ниже по сравнению с 2013-м. Такой вывод был сделан на основе опроса 460 респондентов, среди которых были специалисты и начальники отделов информационной безопасности, собственники бизнеса, директора организаций.

 Материал подготовлен специалистами аналитического центра компании SearchInform

**К**оличество отделов по информационной безопасности в московских компаниях в 2014 году незначительно выросло — с 30 до 31% (по сравнению с 2013 годом). Некоторая часть респондентов отметила, что вопросами информационной безопасности в их компаниях занимается ИТ-отдел, и тенденция передачи подобных обязанностей постепенно растет — 32% в 2014 году против 29% в 2013-м. Одновременно с этим наблюдается рост количества компаний, которые не возлагают вопросы кибербезопасности на отдельные подразделения — таких ответов по итогам исследования было 2%, тогда

как в прошлом исследовании этот показатель составлял менее 1%.

В большинстве случаев для несанкционированной передачи информации третьим лицам сотрудники компаний используют электронную почту. Соответственно, этот ресурс проверяется специалистами в первую очередь (36% респондентов против 27%). На втором месте по степени опасности эксперты выделяют внешние носители (18%, ранее — 22%). Далее следуют печатные документы (15%, ранее — 19%) и интернет-мессенджеры (15%, ранее — 4%).

Значительно уменьшилось количество компаний, которые проводят инструктаж

с сотрудниками по вопросам политики информационной безопасности внутри организации (68%, ранее — 94%). Однако при этом 87% опрошенных отметили, что в их компаниях сотрудники подписывают соглашение о неразглашении конфиденциальной корпоративной информации, остальные 13% не выдвигают такого требования.

53% респондентов указывают на наличие ограничений для работников по использованию различных информационных ресурсов (например, Skype и социальные сети). Однако, как считают эксперты SearchInform, данные запреты действуют не столько в интересах информационной безопасности, сколько

## РЕЗУЛЬТАТЫ ОПРОСА

В случае утечек персональных данных ставили ли вы в известность пострадавших от утечки или общественность?



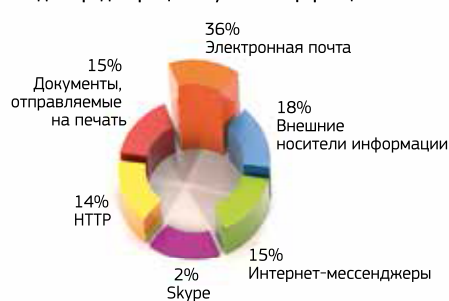
Кто в вашей организации отвечает за ИБ?



Предупреждены ли ваши сотрудники о наличии DLP-системы или других решений ИБ?



Какие каналы передачи данных контролируются для предотвращения утечек информации?



Кто из сотрудников был уличен в нарушении корпоративной политики ИБ?



Какие санкции применяются к сотрудникам, допустившим утечку информации?



для того, чтобы сотрудники в рабочее время не отвлекались на посторонние задачи. Еще более высокий процент опрошенных (94%) ответил, что в организации практикуется разграничение прав доступа к корпоративной информации в локальной сети в зависимости от должности и обязанностей сотрудника.

При этом в 41% компаний нет работающей системы контроля информационных потоков, 25% отметили, что такую систему планируют внедрить. DLP-системы и другие способы защиты информации есть у 34% компаний — и это, согласно исследованию, один из немногих показателей, который вырос по сравнению с 2013 годом, ранее о наличии DLP-систем рассказали только 19% участников опроса.

Еще один источник угрозы — личные электронные устройства сотрудников, которые используются для решения бизнес-задач, что повышает шансы утечки ценной информации. Об этом рассказывают 70% респондентов. Несмотря на это, в 52% организаций эта угроза никак не контролируется, с чем в большинстве случаев и связан высокий уровень угроз информационной безопасности.

Наличие превентивных мер, соглашений о неразглашении и систем защиты, как показывают результаты опроса, в 2014 году не спасло 50% компаний от утечки информации в том или ином виде. Более половины

респондентов признают, что уволившиеся сотрудники пытались унести с собой конфиденциальные данные. Этот показатель по сравнению с 2013 годом вырос почти в два раза — с 28%, — что позволяет делать выводы о значительном росте агрессивности среды, в которой работает бизнес.

В нарушениях политики информационной безопасности чаще всего замечены

В случае инцидента 77% респондентов не сообщают о нем своим клиентам и партнерам, ссылаясь на незначительность ущерба. Только 6% компаний не только информируют об утечке данных все пострадавшие стороны, но и делают официальные заявления в СМИ. Во многом такой низкий процент связан с отсутствием законодательных требований об обязательном уведомлении «жертв»

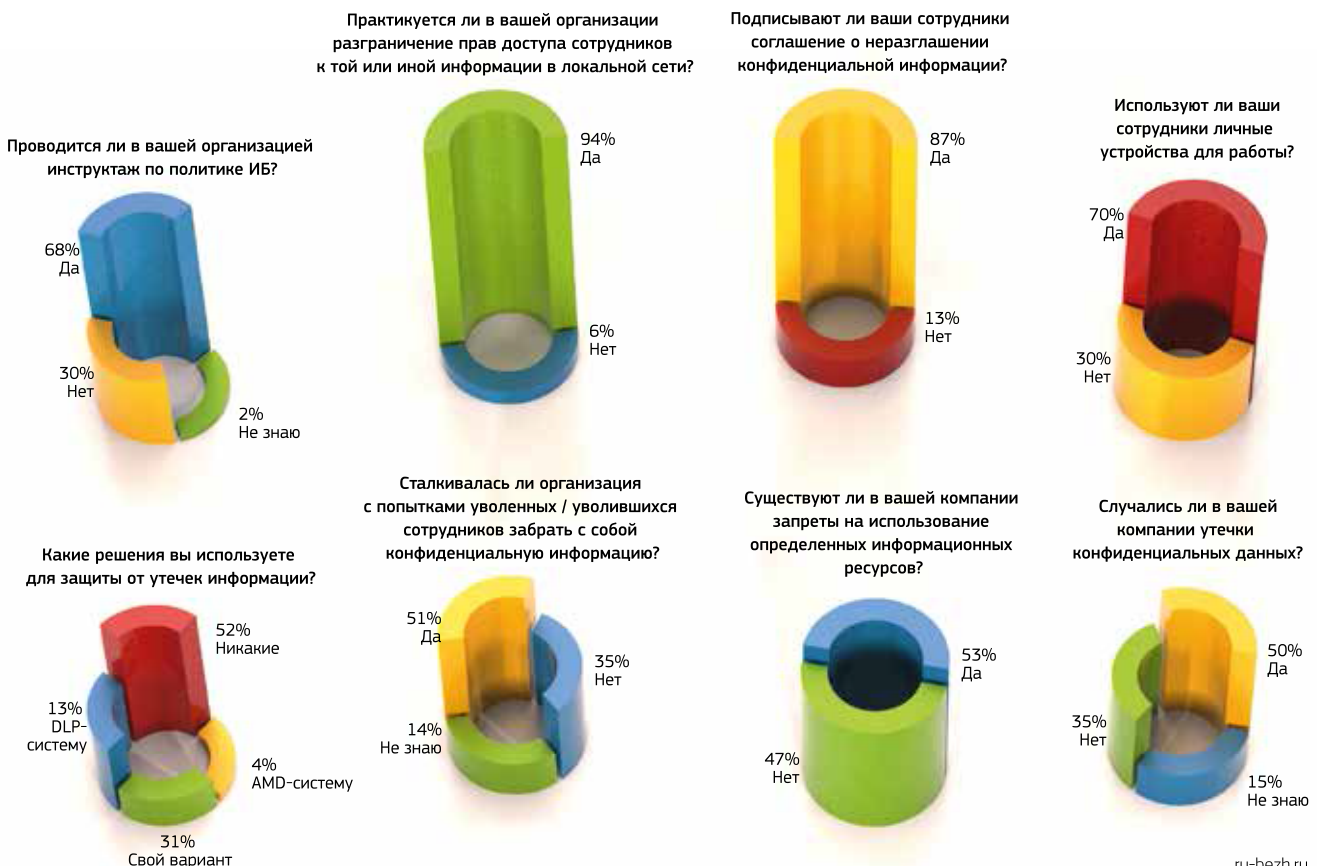
## В 41% московских компаний нет работающей системы контроля информационных потоков.

менеджеры (43%), на втором месте — руководители (16%), незначительная доля приходится на секретариат (4%). Таким образом, специфика столичного региона сегодня заключается в том, что утечку данных чаще всего допускают те, кто так или иначе связан с работой по денежному потокам. В 2013 году менеджеры и руководители в сумме «генерировали» только около 33% утечек среди опрошенных московских компаний.

Как результат, в 40% организаций сотрудников, попавшихся на краже данных, увольняют. 14% компаний не применяют никаких санкций к провинившимся. В остальных случаях практикуются системы штрафов, лишения премий или вынесения выговора.

утечек. В 2013-м о подобных инцидентах не сообщали 96% опрошенных компаний в столичном регионе.

Генеральный директор компании Search-Infom Лев Матвеев считает, что, даже несмотря на относительно низкие показатели уровня информационной защищенности московских компаний, в столичном регионе этот вопрос стоит не так остро, как в других субъектах РФ. Главными тенденциями в области информационной безопасности в ближайшее время будет являться борьба с утечками данных через личные мобильные устройства, а также увеличение количества компаний, которые сообщают об инцидентах пострадавшим.



# Анонсы маркетинговых акций компаний

## Ivideon (ЗАО «Мобильные видеорешения»)

При покупке камеры Hikvision DS-2CD2412F-I на сумму от 200 000 рублей интеллектуальный видеосчетчик Ivideon Counter в подарок!

**Что такое Ivideon Counter?** Это инновационный видеосчетчик, который предоставляет данные о количестве посетителей с точностью 98% и поддерживает потоковую передачу видеоинформации.

**Почему Ivideon Counter** — это ликвидный и востребованный на рынке товар? В последнее время обращение к видеоаналитике в целом и подсчету посетителей в частности становится для многих отраслей бизнеса устойчивой тенденцией. Хотите идти в ногу со временем? Предложите своим клиентам Ivideon Counter!

**Где используется Ivideon Counter?** Видеосчетчик применяется для профессионального подсчета посетителей:

- в магазинах;
  - в торговых центрах;
  - в ресторанах;
  - на выставочных площадках
- и других объектах, где статистика посещаемости представляет интерес.



Срок акции: до 30.09.2015  
Телефон: 8-800-500-49-02  
Сайт: ru.ivideon.com

## Торговый Дом «Видеоглаз»

1. Каждому установщику, впервые купившему Satel Micra Kit, бесплатно вручаются универсальный конвертер USB-RS и четыре кабеля с соответствующими штекерами для настройки любых устройств Satel. А каждому установщику, покупающему Satel Micra Kit два месяца подряд, в подарок — фирменный комбинезон монтажника.

2. При покупке любого биометрического терминала Smartec и программного обеспечения для контроля доступа и учета рабочего времени Timex Base + Timex TA по цене, указанной на сайте, каждый покупатель получает в подарок USB-сканер отпечатков пальцев Smartec ST-FE700.

3. Заморожены цены на продукцию Iptronic. Выгодное предложение — готовые комплекты видеонаблюдения по июльским ценам.

Телефон: 8-800-333-71-70

Сайт: videoglaz.ru

## ООО «Секьюрети Эксперт»

Купите 10 любых IP-камер Optimus — получите скидку 10% на коммутатор UMG1-18/16P.



Срок акции: до 19.10.2015.

Телефоны: Москва: +7 (495) 799-96-77; Пермь: +7 (342) 219-62-92

Сайт: optimus-cctv.ru; sec-e.ru

## Macroscop (ООО «Сателлит Инновация»)

1. Цена на монобрендовое ПО для IP-камер Axis, Bosch, Beward, Dahua снижена почти вдвое

Macroscop снижает цены на монобрендовую версию ПО, поддерживающее IP-камеры Axis, Bosch, Beward и Dahua. Скидка составляет 45% относительно мультибрендовой версии.

**Мультибрендовая версия Macroscop (розничная стоимость):**

- версия ML (для системы до 20 IP-камер, не поддерживает работу интеллектуальных модулей) — 1800 рублей;
- версия ST (нет ограничений по количеству камер и серверов в системе, включает бесплатные модули детекции оставленных предметов, обнаружения лиц, интерактивного поиска и перехвата объектов, трекинга; возможно подключение других интеллектуальных модулей) — 3500 рублей.

**Монобрендовая версия Macroscop для Axis, Bosch, Beward и Dahua (розничная стоимость):** версия ML — 990 рублей; версия ST — 1950 рублей.

Сроки акции: до 30.10.2015.

2. Видеорегистратор Macroscop NVR-16 М на 35% дешевле

Популярный видеорегистратор Macroscop NVR-16 М по специальной рекомендованной розничной цене \$1010, что на \$544 ниже обычной стоимости.

NVR-16 М создан на базе ОС Windows 7 Pro x64, гарантированно обрабатывает видео и аудио с 16 IP-камер разрешением 2 Мп, позволяет устанавливать до 12 жестких дисков объемом до 6 Тб и предназначен как для настольной установки, так и в стойку 19". Цены на NVR Macroscop рассчитываются в условных единицах. 1 у.е. = \$1. Оплата производится в рублях по курсу ЦБ РФ + 3%.

Сроки акции: до 30.09.2015.

Телефон: 8-800-555-0043

Сайт: macroscop.com

## ООО «Альтоника»

### 1. GSM-сигнализация Tavr за 5550 рублей



Автономная GSM-сигнализация Tavr позволяет обеспечить безопасность квартир, коттеджей, дач, гаражей и других объектов имущества. Система предназначена для оповещения владельца охраняемого помещения о несанкционированном проникновении на объект. Она

доступна и проста в установке, а ее применение актуально в любое время года.

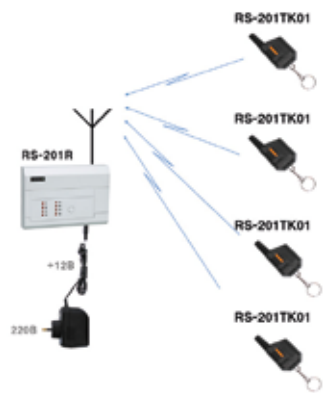
### 2. Тревожная сигнализация: комплектом — выгоднее!

Компания «Альтоника СБ» представляет готовые бюджетные решения на базе тревожных радиокнопок с большой дальностью действия. Несомненным преимуществом приобретения готовых комплектов является удобство

и экономичность: все элементы системы уже настроены между собой, а стоимость комплекта дешевле почти на 20% (по сравнению со стоимостью этого оборудования при покупке элементов по отдельности).

*Стандартный комплект тревожной сигнализации с кнопками RS-201TK01*

Комплект рассчитан на работу с четырьмя кнопками RS-201TK01 с возможностью расширения до восьми кнопок. Оптимально подходит для применения на малых и средних объектах.



### Состав комплекта:

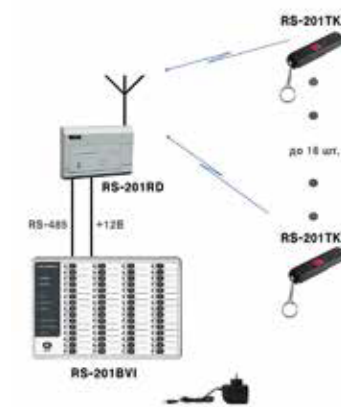
- приемник RS-201R — 1 шт.;
- радиокнопка RS-201TK01 — 4 шт.;
- блок питания — 1 шт.

### Технические характеристики:

- дальность действия — 5 км и более (в условиях прямой видимости);
- рабочая частота: 4 частоты (литеры) в пределах полосы 433,92 МГц ± 0,2%;
- номинальная излучаемая мощность: 10 мВт.

**Стоимость: 8020 рублей.**

*Расширенный комплект тревожной сигнализации с кнопками RS-201TK2*



Комплект рассчитан на работу с 16 кнопками RS-201TK2 с возможностью расширения до 600 кнопок. Оптимально подходит для применения на крупных объектах: в торговых центрах, супермаркетах и на других крупных объектах.

### Состав комплекта:

- выносной приемник RS-201RD — 1 шт.;
- блок выносной индикации RS-201BVI — 1 шт.;
- антенна — 1 шт.;
- радиокнопка RS-201TK2 — 16 шт.;
- блок питания — 1 шт.

**Стоимость: 36 780 рублей.**

Телефон: +7 (495) 797-30-707 (495) 797-30-70

Сайт: altonika-sb.ru

## Digital Security Systems Lab (ООО «ДССЛ»)

### 1. Домофонная система Trassir в подарок при покупке домофонов и вызывных панелей True-IP серии МХ.

Система домофонии Trassir + True-IP позволяет повысить уровень безопасности и комфорта жителей и получить больше за те же деньги.

- Жители ЖК не только услышат, но и увидят на экране, кто к ним пришел, причем в деталях.
- Видеонаблюдение Trassir интегрировано с домофонами, возможность записывать все звонки и разговоры по домофону.
- Возможность оборудовать только одно место консьержа на несколько подъездов — он увидит все на экранах.



• Возможность ответить на звонок домофона с мобильного и открыть дверь.

### 2. Бесплатный дизайн камеры видеонаблюдения «Мой ActiveCam» для вашего проекта.

Как удовлетворить специфические запросы клиентов, защитить проект или выделить свое предложение среди конкурентов?

Линейка камер «Мой ActiveCam» — это богатое разнообразие оформления и подходящие технические характеристики оборудования. Выберите из готовых вариантов или закажите свой дизайн камеры видеонаблюдения.

Осенью специалисты компании работают персональный дизайн камеры для вашего проекта абсолютно бесплатно.

Телефон: +7 (495) 783-72-87

Сайт: dssl.ru

