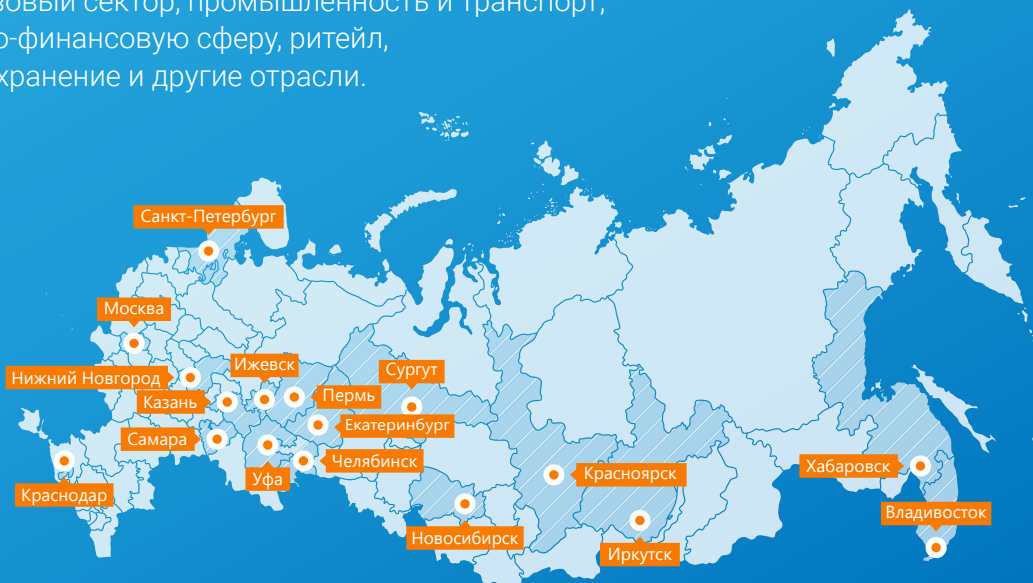
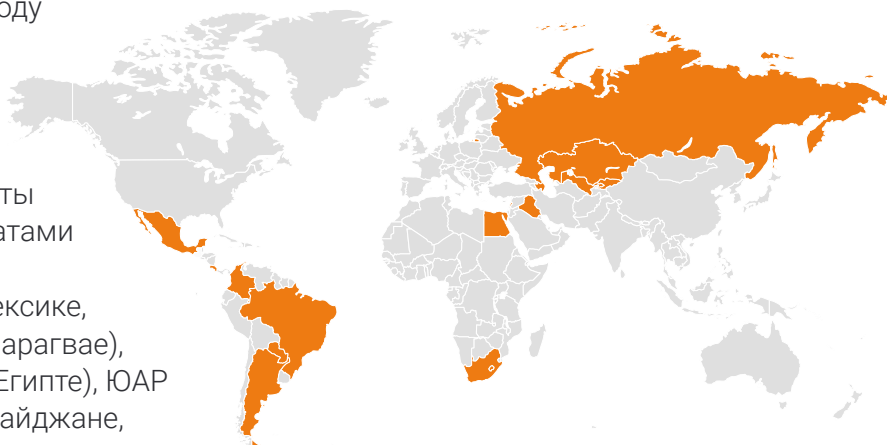


ИССЛЕДОВАНИЕ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПАНИЯХ РОССИИ И МИРА ЗА 2018 ГОД

Аналитики «СёрчИнформ» провели анонимный опрос российских компаний с целью оценить уровень информационной защиты и подход к вопросам ИБ. В исследовании приняли участие 1024 человека: начальники и сотрудники ИБ-подразделений, эксперты отрасли и руководители организаций из коммерческой (74%), государственной (23%) и некоммерческой сфер (3%). Исследование затронуло IT, нефтегазовый сектор, промышленность и транспорт, кредитно-финансовую сферу, ритейл, здравоохранение и другие отрасли.



Исследование ежегодное. В этом году мы уточнили методику, добавили дополнительные вопросы, касающиеся корпоративного мошенничества. Впервые в этом году «СёрчИнформ» сравнила ответы по некоторым вопросам с результатами в других регионах присутствия: Латинской Америке (Аргентине, Мексике, Коста-Рике, Бразилии, Колумбии, Парагвае), Ближнем Востоке (Ираке, Ливане, Египте), ЮАР и странах СНГ (Узбекистане, Азербайджане, Киргизии, Казахстане).



“

Комментирует руководитель отдела аналитики «СёрчИнформ» Алексей Парфентьев:

– Выходя на новые рынки, мы еще раз убеждаемся, что какие бы нормы локальных законов, требований, рекомендаций и постановлений ни работали в том или ином регионе (а они очень разные от страны к стране), реальную ситуацию все равно определяют доступные технологии.

ОГЛАВЛЕНИЕ

1. Часть I Россия и мир	3
2. Часть II В разрезе отраслей	11
3. Кредитно-финансовая сфера	11
4. Сфера IT	17
5. Нефтегазовая сфера	23
6. Промышленность	29
7. Ритейл	35
8. Недвижимость и строительство	41

ЧАСТЬ I РОССИЯ И МИР

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

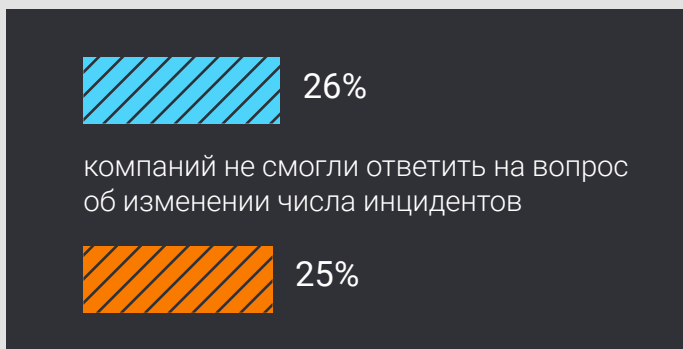
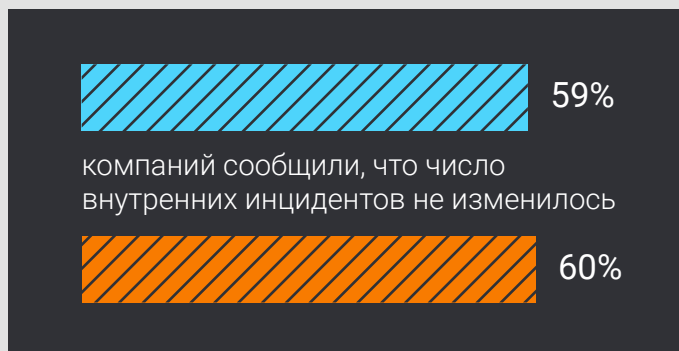
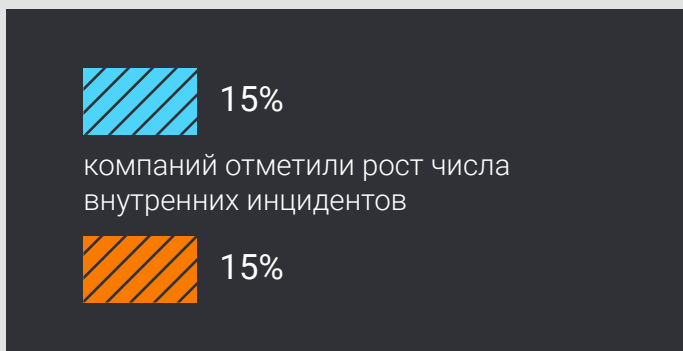
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:

* % ОТ ЧИСЛА ОТВЕТОВ



ДИНАМИКА

* % ОТ ЧИСЛА ОТВЕТОВ ■ ДАННЫЕ ПО РОССИИ ■ ЗАРУБЕЖЬ



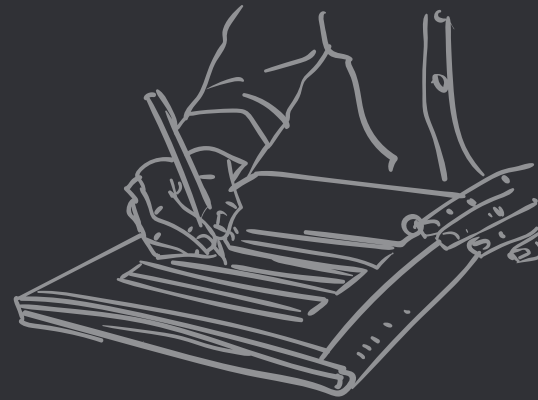
Алексей Парфентьев:

– Исследование показывает явное повышение осведомленности бизнеса об ИБ-угрозах. С этой точки зрения неважно, увеличилось или уменьшилось количество ИБ-инцидентов (а оно год от года растет). Важно, что их стали чаще выявлять, это однозначно положительный тренд.

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

81%

РОССИЙСКИХ КОМПАНИЙ ПОДПИСЫВАЮТ
С СОТРУДНИКАМИ СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ



БЮДЖЕТ НА БЕЗОПАСНОСТЬ

*% ОТ ЧИСЛА ОТВЕТОВ



30%

компаний заявили
о росте бюджета
на безопасность



12%

компаний
сократили бюджет
на безопасность



58%

компаний сообщили
об отсутствии динамики
в изменении бюджета
в 2018 году

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

■ данные по России ■ ЗАРУБЕЖЬЕ

Средство защиты	России (%)	Зарубежье (%)
Антивирусная программа	97%	83%
Средства администрирования Windows	87%	56%
NGFW (Firewall и Proxy)	78%	79%
DLP-система	32%	23%
IDS/IPS	19%	34%
SIEM-система	9%	18%

* МОЖНО БЫЛО ВЫБРАТЬ НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТОВ



Алексей Парфентьев:

– Такая динамика объясняется новым фактором – требованием регуляторов. И в России, и в мире начали работу знаковые ИБ-законы. В нашем случае речь идет о ФЗ-187, в случае зарубежья – о директивах GDPR, имеющих экстерриториальное действие. Как разработчик ИБ-продуктов мы наблюдаем стабильно высокий интерес к программному обеспечению из-за новых требований. Есть все основания полагать, что в ближайшем будущем он только усилится, ведь прикладное выполнение данных требований – процесс и длительный, и сложный.

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

* % ОТ ЧИСЛА ОТВЕТОВ

■ ДАННЫЕ ПО РОССИИ

■ ЗАРУБЕЖЬЕ



29% | 26%

Электронная
почта

20% | 15%

Внешние
носители

14,8% | 10%

Телефония



12% | 9%

Документы,
отправляемые
на печать

11% | 8%

Интернет-
мессенджеры
(Telegram и т.д.)

8,6% | 11%

Облачные
хранилищаРАБОТОДАТЕЛИ ОБРАЩАЮТ ВНИМАНИЕ НА ТАКИЕ
ОСОБЕННОСТИ ПОВЕДЕНИЯ СОТРУДНИКОВ:

* % ОТ ЧИСЛА ОТВЕТОВ

23%

Распространение негативных
отзывов о компании

21%

Саботирование работы

21%

Нелояльное отношение к компании

16%

Подверженность
опасным зависимостям

10%

Симпатия к экстремистским и/или
террористическим организациям

9%

Извращенные,
девиантные интересы

УТЕЧКИ ИНФОРМАЦИИ



ЧТО УТЕКАЛО?

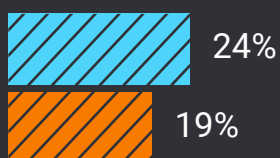
*% ОТ ЧИСЛА ОТВЕТОВ

■ ДАННЫЕ ПО РОССИИ

■ ЗАРУБЕЖЬЕ



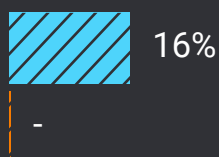
Информация
о клиентах и сделках



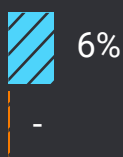
Техническая
информация



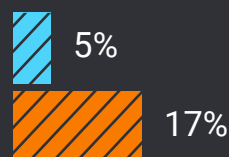
Персональные
данные



Информация
о партнерах



Внутренняя
бухгалтерия



Другое

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

* % от числа ответов

■ данные по России

■ ЗАРУБЕЖЬ



69% | 62%

опрошенных компаний
скрыли инцидент и не
делали никаких
оповещений



27,5% | 31%

сообщили
пострадавшим об
инциденте и принесли
извинения



3,5% | 7%

сделали официальное
заявление в СМИ



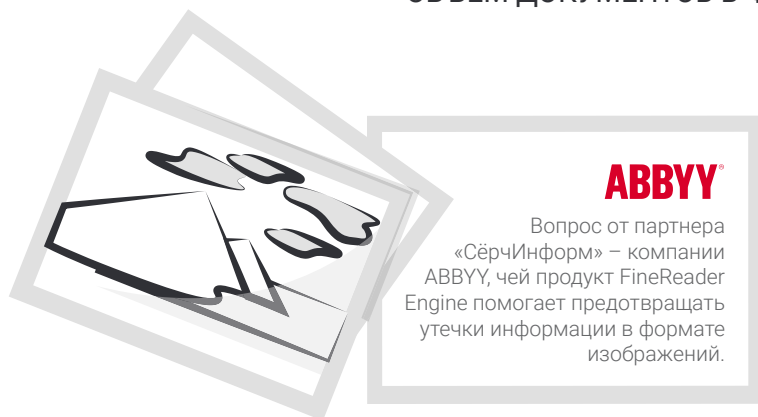
Алексей Парфентьев:

– Проблема утечек актуальна для всего мира. Это подтверждают и объективные данные, и личные впечатления. При общении с иностранными заказчиками становится очевидно: проблемы, риски, приоритеты в общем-то те же. Конечно, прикладной аспект реализации и нейтрализации угроз довольно разный – это объясняется скорее различием в бизнес-процессах и используемых средствах, нежели географической принадлежностью как таковой.

Нельзя не отметить позитивный момент – доля компаний в РФ, признающих ответственность за инцидент, неуклонно растет (в этом году мы увидели значимый скачок) и в скором времени сравняется с показателями стран ЕС и США.

Это довольно интересный тренд, ведь санкции в России и в мире кардинально различаются. Например, в России штраф за разглашение персональных данных измеряется десятками тысяч (рублей), а в Евросоюзе – миллионами (евро). Таким образом, именно личная ответственность, сознательность отечественных компаний является главной причиной признания ответственности, а вовсе не угроза штрафа.

ОБЪЕМ ДОКУМЕНТОВ В ФОРМАТЕ ИЗОБРАЖЕНИЙ



54%

КОМПАНИЙ ХРАНИТ ПОЛОВИНУ И БОЛЬШЕ ВСЕХ СВОИХ ДОКУМЕНТОВ В ФОРМАТЕ ИЗОБРАЖЕНИЙ

Количество документов в виде изображений – сканов, фотографий, скриншотов, PDF – за последнее время значительно увеличилось. Еще 3 года назад таких документов в организациях было не более трети. Как показало исследование «СёрчИнформ», сегодня в 54% компаний половина информации и более хранится в графических форматах. У некоторых организаций таких документов до 80-90%. Паспорта, кредитные карты, водительские удостоверения и другие документы часто передаются за пределы контура безопасности в форматах JPEG, PNG, TIFF.

@ 30%

утечек таких документов происходит по электронной почте

📱 30%

документов сотрудники выносят на мобильных устройствах



Дмитрий Шушкин, генеральный директор ABBYY Россия:

– Количество документов в формате изображений продолжит расти: одна из причин – распространение мобильных приложений и доступность смартфонов с хорошими камерами. Чтобы зарегистрироваться в сервисах, оформлять счета или договоры, совершать платежи и получать скидки, клиенты все чаще представляют данные и документы в виде фотографий и сканов в крупные банки, магазины, операторам.

Для этих организаций защита персональных данных и другой конфиденциальной информации пользователей от утечек становится критически важной, чтобы избежать финансовых и репутационных рисков. Помочь в этом могут технологии оптического распознавания и искусственного интеллекта ABBYY в составе DLP-систем: они позволяют определять тип документа по его содержанию и внешнему виду, распознавать данные на сложных изображениях, вовремя выделять критичную информацию и предотвращать ее утечку.

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

В этом году мы поинтересовались у сотрудников служб безопасности, какие инциденты кроме утечек информации они регистрировали чаще всего.

* % ОТ ЧИСЛА ОТВЕТОВ



Использование ресурсов компании в личных целях (майнинг, фриланс, онлайн-игры и т.п.)



Попытки откатов



Промышленный шпионаж/ работа в пользу конкурентов



Другое



Организация фирмы-боковика

УЩЕРБ ОТ ИНЦИДЕНТОВ

* % ОТ ЧИСЛА ОТВЕТОВ

28%

Имиджевый

12%

Compliance-риск (угроза или факт наказания от регулятора)

13%

Крупный финансовый ущерб

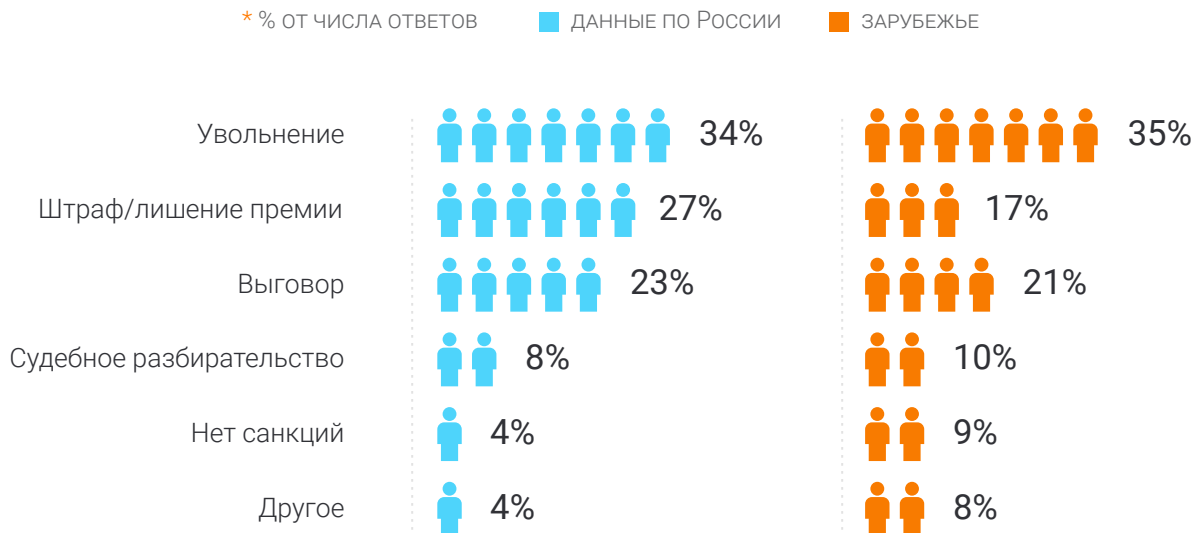
28%

Мелкий финансовый ущерб

17%

Ущерба не было

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО



Алексей Парфентьев:

– Несмотря на наблюдаемую разницу в подходах нарушителей, очевидно желание работодателя действовать на качественно ином уровне – понимать мотивы внутренних нарушителей, то есть предвидеть проблему заранее.

Причем интересы выходят за рамки мониторинга лояльности (негативные отзывы, нелояльное отношение, саботаж). Работодателю важно понимать личностные проблемы сотрудников, которые могут быть опасны для бизнеса и коллектива: наркозависимость, разделение экстремистских убеждений. Безусловно, такая работа позитивно сказывается не только на внутренних процессах компании, но и повышает уровень безопасности в стране в целом.

ЧАСТЬ II В РАЗРЕЗЕ ОТРАСЛЕЙ

КРЕДИТНО-ФИНАНСОВАЯ СФЕРА

Кредитно-финансовая сфера традиционно хорошо оснащена ИБ-инструментарием. В значительной степени это связано с пристальным надзором со стороны регулятора, высоким уровнем квалификации специалистов и достаточным бюджетированием. Это настолько эффективный контроль, что сейчас финансовая сфера – одна из самых защищенных, и внешние атаки на нее становятся все более дорогим удовольствием. На этом фоне угроза от внутреннего фактора становится значительнее.



По данным ФинЦЕРТа, человеческий фактор находится на первом месте среди всех причин, которые определяют успешность внешних атак на инфраструктуру. Не снижается угроза злоумышленных действий и со стороны самих сотрудников банков.

Угроза еще более серьезна, учитывая, что значимая доля нарушителей – **руководители и IT-специалисты**, показывает исследование этого года. Эта категория – люди с привилегированным доступом к данным. По нашему опыту, доля злонамеренных и случайных нарушений у них примерно одинаковая.

В рамках опроса представители банковской отрасли в 2 раза чаще прочих заявляли о росте числа внутренних инцидентов – в **31% случаев**.

Гораздо чаще, чем в других отраслях, банки сталкивались с утечками информации –

75%
компаний
заявили
об этом

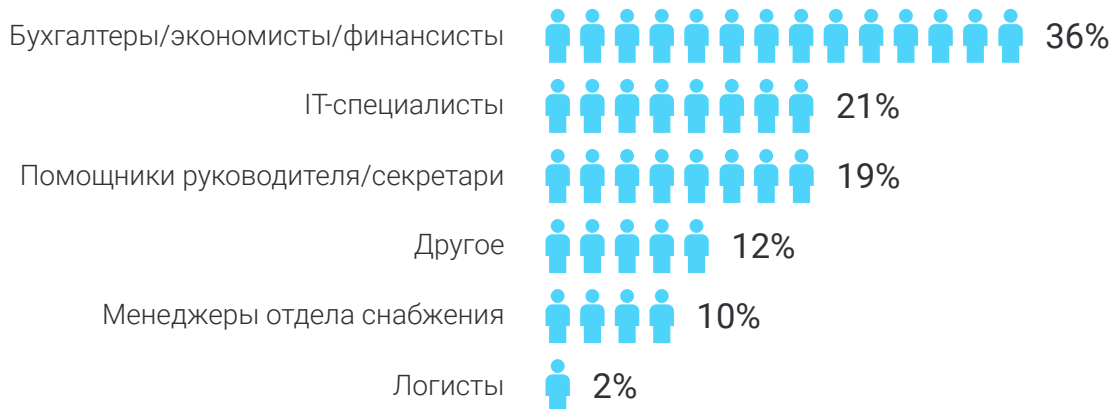


Показатель внедрения современных DLP-систем в банках довольно высок (судя по ответам в рамках исследования, 57% компаний располагают таким ПО). Однако часто ситуация складывается парадоксальным образом, когда программные комплексы не эксплуатируются в полную силу. Это позволяет судить о том, что **угроза человеческого фактора в банковской сфере сохраняется на высоком уровне**.

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

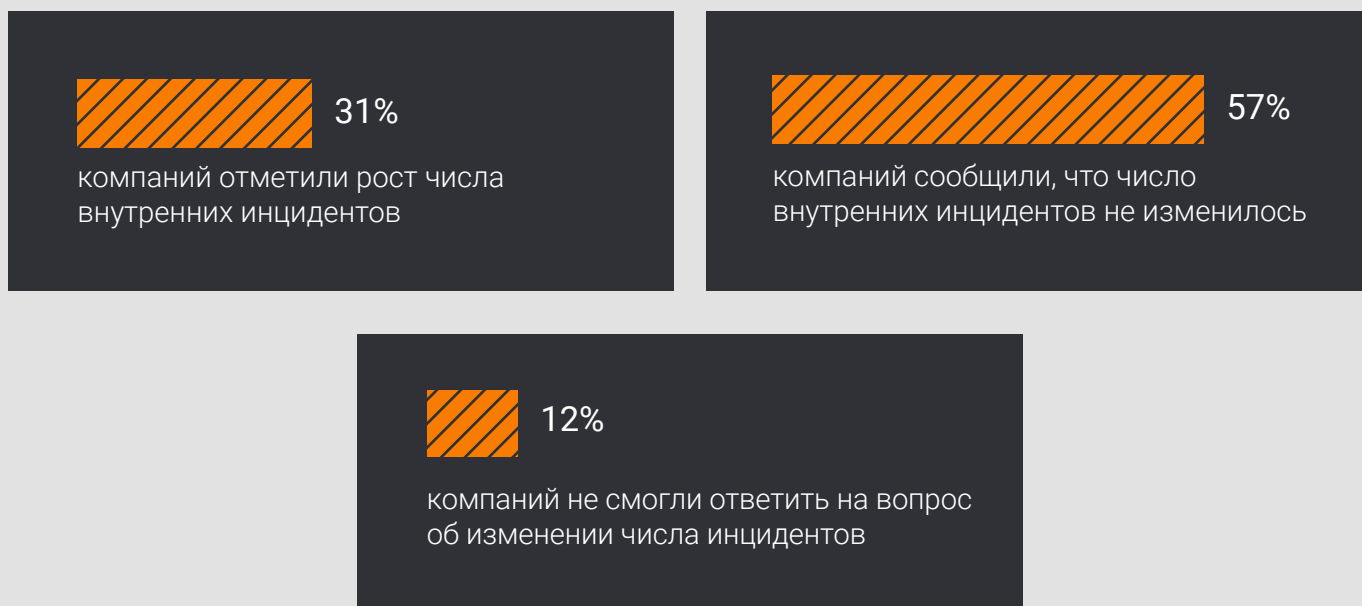
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:

* % ОТ ЧИСЛА ОТВЕТОВ



ДИНАМИКА

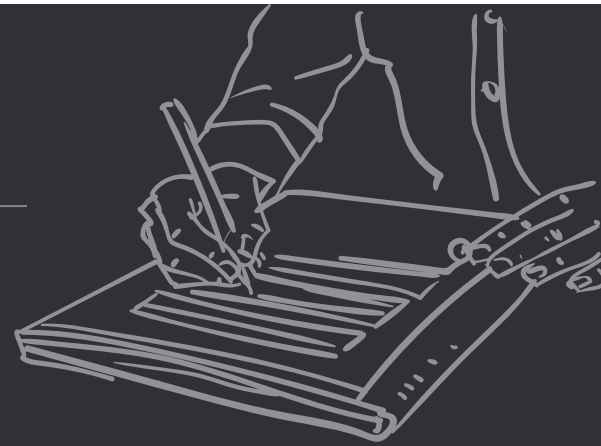
* % ОТ ЧИСЛА ОТВЕТОВ



СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

89%

РОССИЙСКИХ КОМПАНИЙ ПОДПИСЫВАЮТ
С СОТРУДНИКАМИ СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ



БЮДЖЕТ НА БЕЗОПАСНОСТЬ

* % ОТ ЧИСЛА ОТВЕТОВ



32%

компаний заявили
о росте бюджета
на безопасность



6%

компаний
сократили бюджет
на безопасность



62%

компаний сообщили
об отсутствии динамики
в изменении бюджета
в 2018 году

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа		92%
Средства администрирования Windows		81%
NGFW (Firewall и Proxy)		76%
DLP-система		57%
IDS/IPS		38%
SIEM-система		16%

* МОЖНО БЫЛО ВЫБРАТЬ НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТОВ

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

* % ОТ ЧИСЛА ОТВЕТОВ



28%

Электронная почта



23%

Внешние носители



16%

Документы,
отправляемые на печать



14%

Телефония



10%

Интернет-мессенджеры
(Telegram и т.д.)



7%

Облачные хранилища

РАБОТОДАТЕЛИ ОБРАЩАЮТ ВНИМАНИЕ НА ТАКИЕ ОСОБЕННОСТИ ПОВЕДЕНИЯ СОТРУДНИКОВ:

* % ОТ ЧИСЛА ОТВЕТОВ

32%

Распространение негативных
отзывов о компании

21%

Нелояльное отношение
к компании

16%

Саботирование работы

18%

Подверженность
опасным зависимостям

8%

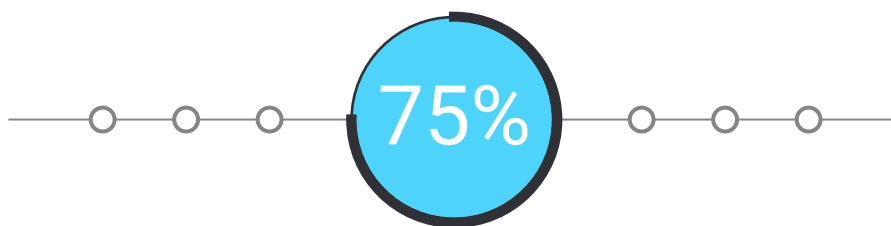
Симпатия к экстремистским и/или
террористическим организациям

5%

Извращенные,
девиантные интересы



УТЕЧКИ ИНФОРМАЦИИ



БАНКОВ СТОЛКНУЛИСЬ С УТЕЧКАМИ
ИНФОРМАЦИИ В 2018 ГОДУ

ЧТО УТЕКАЛО?

* % ОТ ЧИСЛА ОТВЕТОВ



38%

Персональные
данные



28%

Информация
о клиентах и сделках



21%

Информация
о партнерах



13%

Техническая
информация



0%

Внутренняя
бухгалтерия

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

* % ОТ ЧИСЛА ОТВЕТОВ



54%

опрошенных компаний
скрыли инцидент и не
делали никаких
оповещений



46%

сообщили
пострадавшим об
инциденте и принесли
извинения



0%

сделали официальное
заявление в СМИ

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

В этом году мы поинтересовались у сотрудников служб безопасности, какие инциденты кроме утечек информации они регистрировали чаще всего.

* % ОТ ЧИСЛА ОТВЕТОВ



Использование ресурсов компании в личных целях (майнинг, фриланс, онлайн-игры и т.п.)



Промышленный шпионаж/ работа в пользу конкурентов



Попытки откатов



Другое



Организация фирмы-боковика

УЩЕРБ ОТ ИНЦИДЕНТОВ

* % ОТ ЧИСЛА ОТВЕТОВ



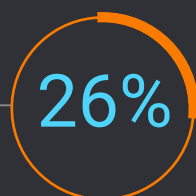
Имиджевый



Compliance-риск (угроза или факт наказания от регулятора)



Крупный финансовый ущерб



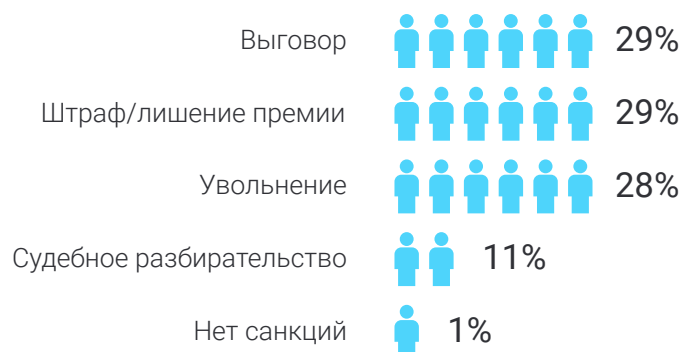
Мелкий финансовый ущерб



Ущерба не было

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО

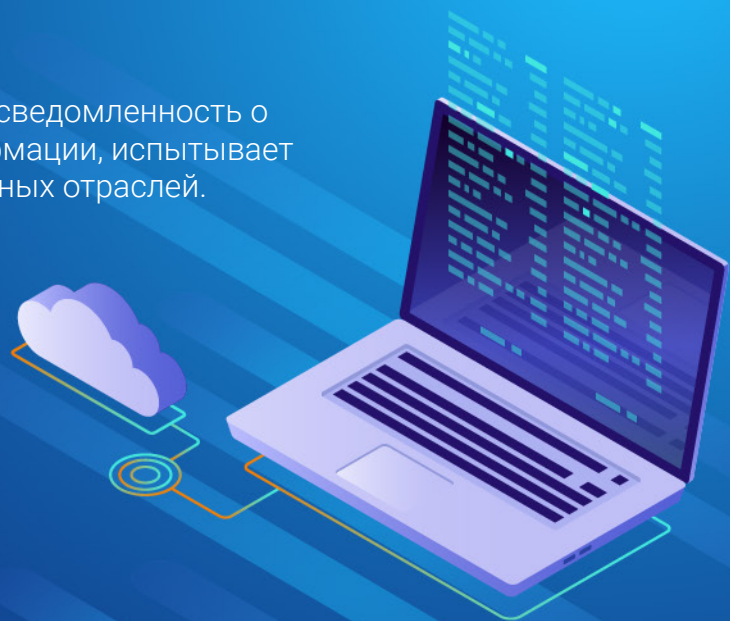
* % ОТ ЧИСЛА ОТВЕТОВ



СФЕРА IT

IT-сфера, несмотря на «продвинутость» и осведомленность о существующих технологиях защиты информации, испытывает те же проблемы, что и компании из остальных отраслей.

69% компаний из сферы IT сообщили о том, что фиксировали в 2018 году утечки информации. Чаще всего они касались данных о клиентах и сделках.



Из других инцидентов внутренней безопасности чаще всего IT-компании сталкивались с использованием сотрудниками ресурсов компании в своих целях – **46%**.

Инциденты почти в равной степени приводили к имиджевому и мелкому финансовому ущербу (26 и 31% ответов соответственно). Еще в 18% случаев ИБ-специалисты фиксировали факты промышленного шпионажа или работы в пользу конкурентов, что, по сути, означает риск передачи ключевых ноу-хау, главного актива IT-компаний.



В этом раскладе закономерно выглядит и то, что чаще всего ИБ-специалисты обращают внимание на **нелояльное отношение сотрудников к своей компании**. Те сотрудники, которые распространяют негативные слухи о компании и саботируют работу, также на особом контроле у ИБ-специалистов (21 и 23% ответов).

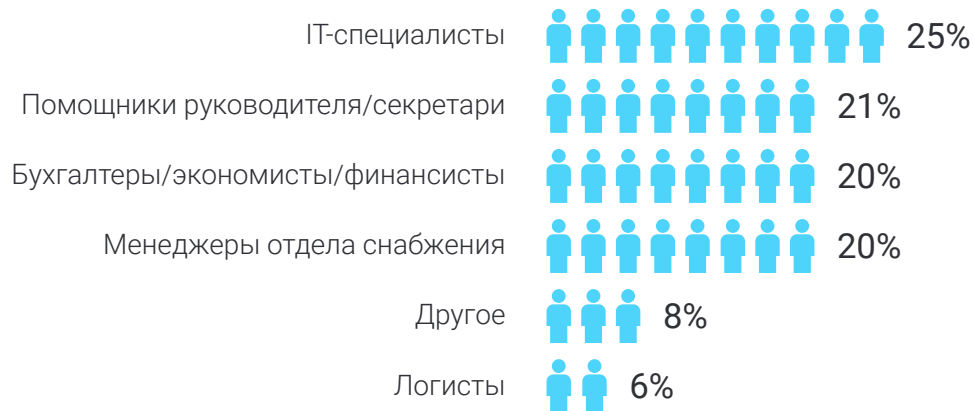
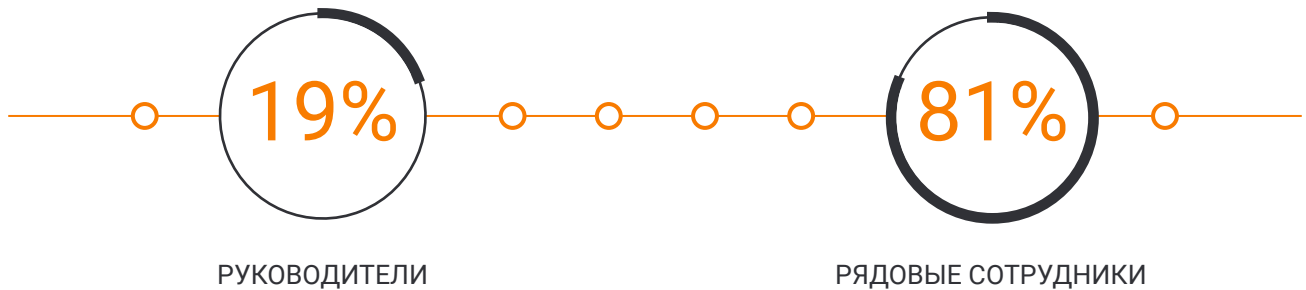


Увольнение – самое часто применяемое наказание к сотрудникам-нарушителям. Чаще всего ими оказываются рядовые сотрудники – в 81% случаев. Это сами IT-специалисты (в четверти случаев), еще по 20% случаев нарушений приходится на помощников руководителей, финансистов и снабженцев.

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

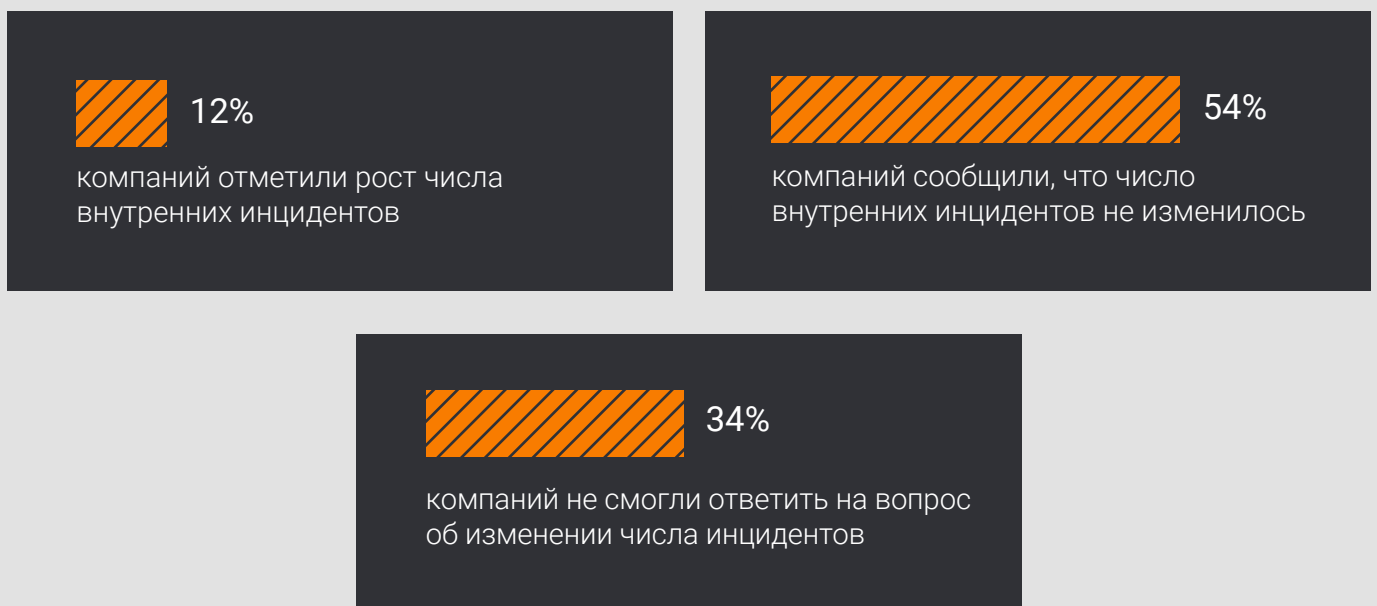
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:

* % ОТ ЧИСЛА ОТВЕТОВ



ДИНАМИКА

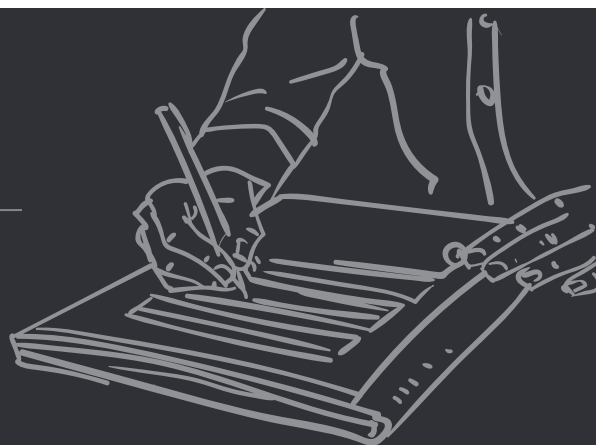
* % ОТ ЧИСЛА ОТВЕТОВ



СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

80%

РОССИЙСКИХ КОМПАНИЙ ПОДПИСЫВАЮТ
С СОТРУДНИКАМИ СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ



БЮДЖЕТ НА БЕЗОПАСНОСТЬ

* % ОТ ЧИСЛА ОТВЕТОВ



26%

компаний заявили
о росте бюджета
на безопасность



14%






компаний
сократили бюджет
на безопасность



60%

компаний сообщили
об отсутствии динамики
в изменении бюджета
в 2018 году

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа		95%
NGFW (Firewall и Proxy)		79%
Средства администрирования Windows		79%
DLP-система		27%
IDS/IPS		22%
SIEM-система		11%
Свой вариант		4%
Никакие		2%

* МОЖНО БЫЛО ВЫБРАТЬ НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТОВ

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

* % ОТ ЧИСЛА ОТВЕТОВ



27%

Электронная почта



19%

Телефония



17%

Внешние носители



12%

Облачные хранилища



11%

Документы,
отправляемые на печать



10%

Интернет-мессенджеры
(Telegram и т.д.)

РАБОТОДАТЕЛИ ОБРАЩАЮТ ВНИМАНИЕ НА ТАКИЕ ОСОБЕННОСТИ ПОВЕДЕНИЯ СОТРУДНИКОВ:

* % ОТ ЧИСЛА ОТВЕТОВ

26%

Нелояльное отношение
к компании

23%

Саботирование работы

13%

Подверженность
опасным зависимостям

21%

Распространение негативных
отзывов о компании

10%

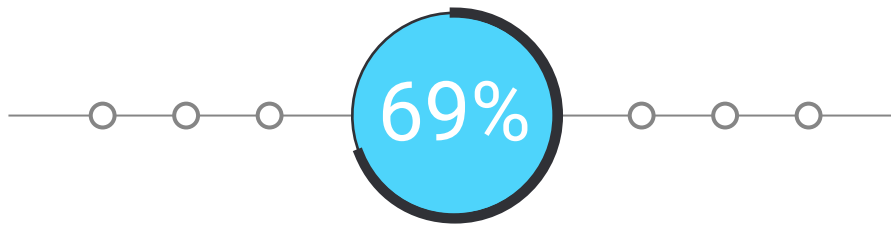
Симпатия к экстремистским и/или
террористическим организациям

7%

Извращенные,
девиантные интересы



УТЕЧКИ ИНФОРМАЦИИ



КОМПАНИЙ СТОЛКНУЛИСЬ С УТЕЧКАМИ
ИНФОРМАЦИИ В 2018 ГОДУ

ЧТО УТЕКАЛО?

* % ОТ ЧИСЛА ОТВЕТОВ



31%

Информация
о клиентах и сделках



26%

Техническая
информация



21%

Информация
о партнерах



13%

Персональные
данные



5%

Внутренняя
бухгалтерия

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

* % ОТ ЧИСЛА ОТВЕТОВ



63%

опрошенных компаний
скрыли инцидент и не
делали никаких
оповещений



33%

сообщили
пострадавшим об
инциденте и принесли
извинения



4%

сделали официальное
заявление в СМИ

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

В этом году мы поинтересовались у сотрудников служб безопасности, какие инциденты кроме утечек информации они регистрировали чаще всего.

* % ОТ ЧИСЛА ОТВЕТОВ



46%

Использование ресурсов компании в личных целях (майнинг, фриланс, онлайн-игры и т.п.)



18%

Промышленный шпионаж/ работа в пользу конкурентов



13%

Другое



13%

Попытки откатов



10%

Организация фирмы-боковика

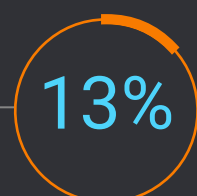
УЩЕРБ ОТ ИНЦИДЕНТОВ

* % ОТ ЧИСЛА ОТВЕТОВ



26%

Имиджевый



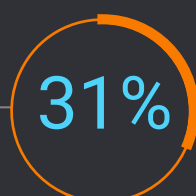
13%

Compliance-риск (угроза или факт наказания от регулятора)



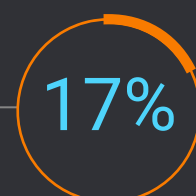
12%

Крупный финансовый ущерб



31%

Мелкий финансовый ущерб



17%

Ущерба не было

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО

* % ОТ ЧИСЛА ОТВЕТОВ

Увольнение



37%

Штраф/лишение премии



25%

Выговор



23%

Судебное разбирательство



7%

Нет санкций



5%

НЕФТЕГАЗОВАЯ ОТРАСЛЬ

В компаниях нефтегазовой отрасли гораздо шире, чем в других сферах, внедрены инструменты защиты информации, даже такие специфические, как SIEM-системы (их применяет 31% компаний – гораздо чаще, чем где-либо в других отраслях) и DLP-системы (в 47% компаний).



40% компаний из нефтегазовой сферы увеличивают бюджет на безопасность.

Серьезность отношения к проблеме подкрепляет и то, что **в отрасли чаще, чем в других, сталкивались с утечками данных в 2018 году**. Рост их числа отметили 25% опрошенных (для сравнения: в общем по другим отраслям показатель составляет 15%).



70%

компаний отрасли

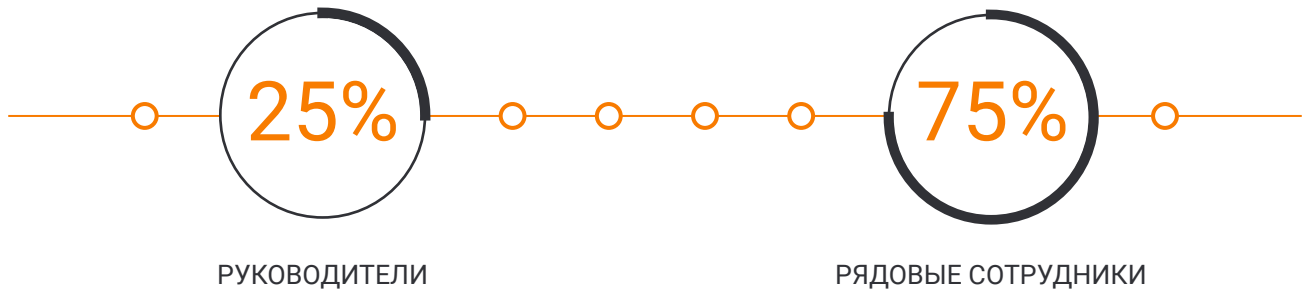
столкнулись с утечками информации, в третьей части случаев компании теряли техническую информацию.

Из других инцидентов корпоративной безопасности чаще всего компании сталкивались с **использованием сотрудниками ресурсов организации в личных целях** (44% ответов). В тройке лидеров среди инцидентов также попытки откатов и промышленный шпионаж/работа в пользу конкурентов.

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

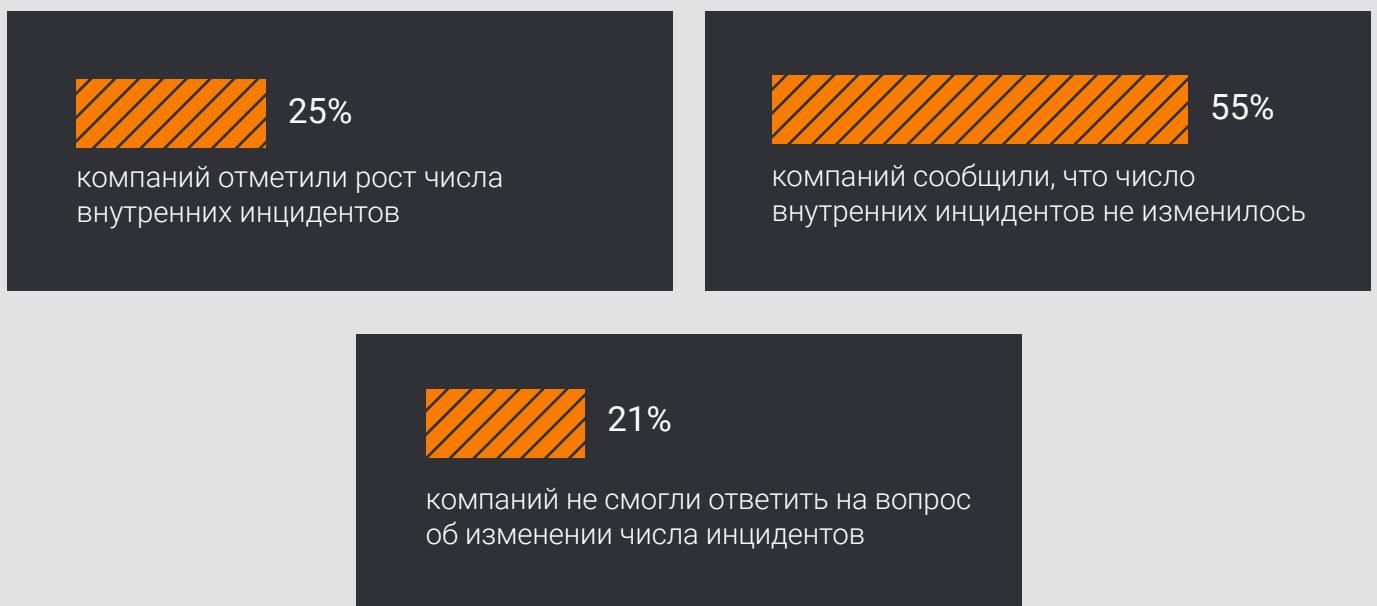
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:

* % ОТ ЧИСЛА ОТВЕТОВ



ДИНАМИКА

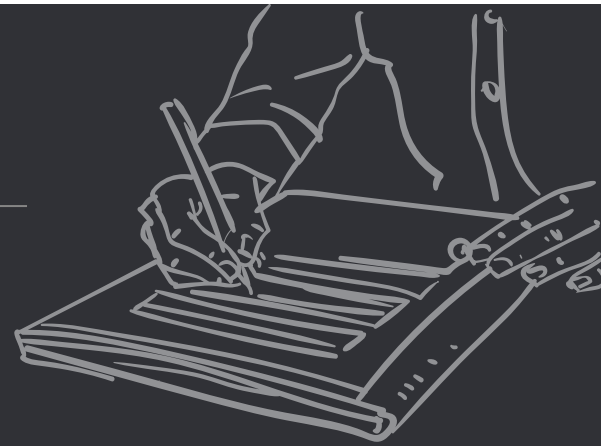
* % ОТ ЧИСЛА ОТВЕТОВ



СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

90%

РОССИЙСКИХ КОМПАНИЙ ПОДПИСЫВАЮТ
С СОТРУДНИКАМИ СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ



БЮДЖЕТ НА БЕЗОПАСНОСТЬ

* % ОТ ЧИСЛА ОТВЕТОВ



39%

компаний заявили
о росте бюджета
на безопасность



17%

компаний
сократили бюджет
на безопасность



44%

компаний сообщили
об отсутствии динамики
в изменении бюджета
в 2018 году

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа		91%
Средства администрирования Windows		80%
NGFW (Firewall и Proxy)		73%
DLP-система		47%
SIEM-система		31%
IDS/IPS		27%
Свой вариант		5%

* МОЖНО БЫЛО ВЫБРАТЬ НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТОВ

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

* % ОТ ЧИСЛА ОТВЕТОВ



30%

Электронная почта



19%

Внешние носители



14%

Интернет-мессенджеры
(Telegram и т.д.)



14%

Документы,
отправляемые
на печать



12%

Телефония



8%

Облачные хранилища



3%

Другое

РАБОТОДАТЕЛИ ОБРАЩАЮТ ВНИМАНИЕ НА ТАКИЕ ОСОБЕННОСТИ ПОВЕДЕНИЯ СОТРУДНИКОВ:

* % ОТ ЧИСЛА ОТВЕТОВ

26%

Распространение негативных
отзывов о компании

23%

Нелояльное отношение
к компании

14,5%

Подверженность
опасным зависимостям

18%

Саботирование работы

14,5%

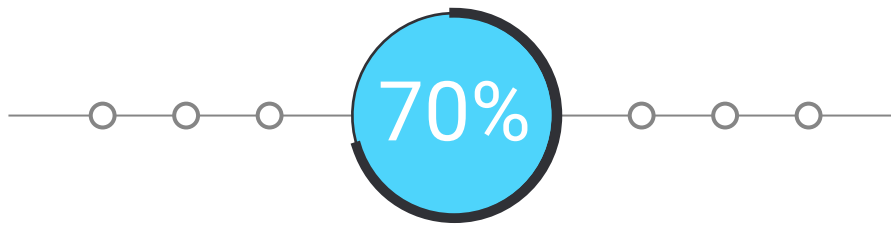
Симпатия к экстремистским и/или
террористическим организациям

4%

Извращенные,
девиантные интересы



УТЕЧКИ ИНФОРМАЦИИ



КОМПАНИЙ СТОЛКНУЛИСЬ С УТЕЧКАМИ
ИНФОРМАЦИИ В 2018 ГОДУ

ЧТО УТЕКАЛО?

* % ОТ ЧИСЛА ОТВЕТОВ



30%

Техническая
информация



22%

Персональные
данные



20%

Информация
о клиентах и сделках



17%

Информация
о партнерах



7%

Другое



4%

Внутренняя
бухгалтерия

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

* % ОТ ЧИСЛА ОТВЕТОВ



75%

опрошенных компаний
скрыли инцидент и не
делали никаких
оповещений



20%

сообщили
пострадавшим об
инциденте и принесли
извинения



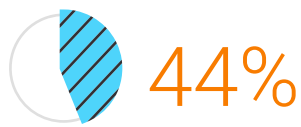
5%

сделали официальное
заявление в СМИ

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

В этом году мы поинтересовались у сотрудников служб безопасности, какие инциденты кроме утечек информации они регистрировали чаще всего.

* % ОТ ЧИСЛА ОТВЕТОВ



Использование ресурсов компании в личных целях (майнинг, фриланс, онлайн-игры и т.п.)



Промышленный шпионаж/ работа в пользу конкурентов



Попытки откатов



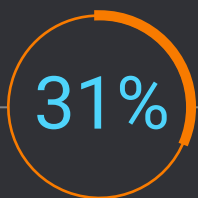
Другое



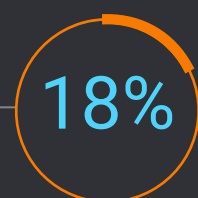
Организация фирмы-боковика

УЩЕРБ ОТ ИНЦИДЕНТОВ

* % ОТ ЧИСЛА ОТВЕТОВ



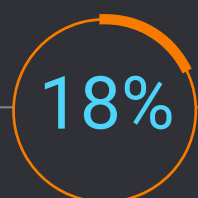
Имиджевый



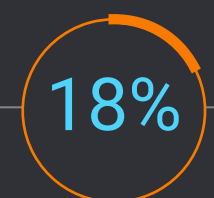
Compliance-риск (угроза или факт наказания от регулятора)



Крупный финансовый ущерб



Мелкий финансовый ущерб



Ущерба не было

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО

* % ОТ ЧИСЛА ОТВЕТОВ

Увольнение  34%

Выговор  29%

Штраф/лишение премии  25%

Судебное разбирательство  4%

Нет санкций  4%

ПРОМЫШЛЕННОСТЬ

Финансовые потери – это наиболее часто встречающийся ущерб от внутренних инцидентов, который фиксировали в 2018 году производственные компании. Причем почти в 20% случаев речь шла о крупном финансовом ущербе. К таким последствиям чаще всего приводят использование сотрудниками ресурсов компании в личных целях (41% ответов), откаты (в 26% случаев).



Сохранение конфиденциальной информации (коммерческой тайны, чертежей, образцов продукции, ноу-хау) – одна из главных задач информационной безопасности для промышленных компаний.



В то же время именно такие данные утекают в 22% случаев промышленного шпионажа.

При этом производственные компании меньше, чем организации из других отраслей, финансировали защиту ИБ в 2018 году. О росте бюджета заявили 24% компаний (против 30% по другим сферам). 15% заявили о сокращении финансирования. Специализированные системы для защиты и расследования инцидентов по вине сотрудников – DLP-системы – стоят в 31% компаний.

Чаще всего ИБ-специалисты стараются контролировать электронную почту сотрудников (27% ответов) и внешние носители (23%). На третьем месте – документы, которые сотрудники распечатывают (14%).



27%

Электронная почта



23%

Внешние носители



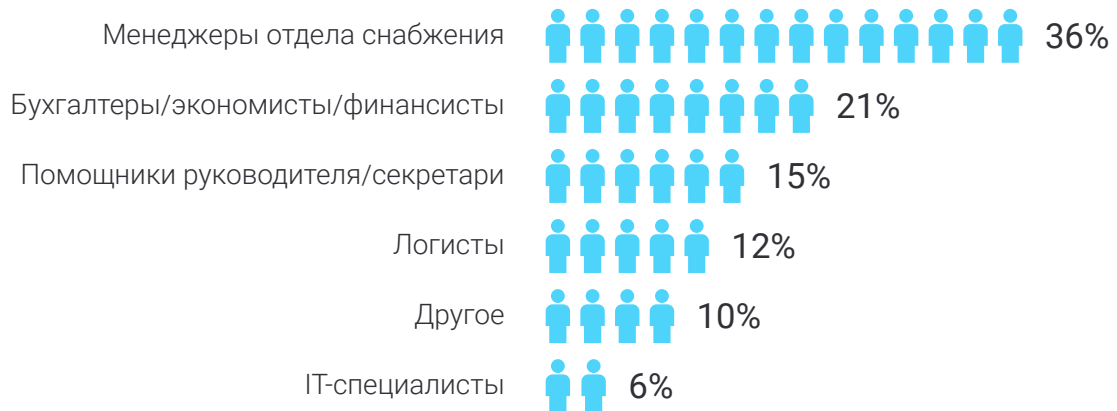
14%

Документы, отправляемые на печать

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

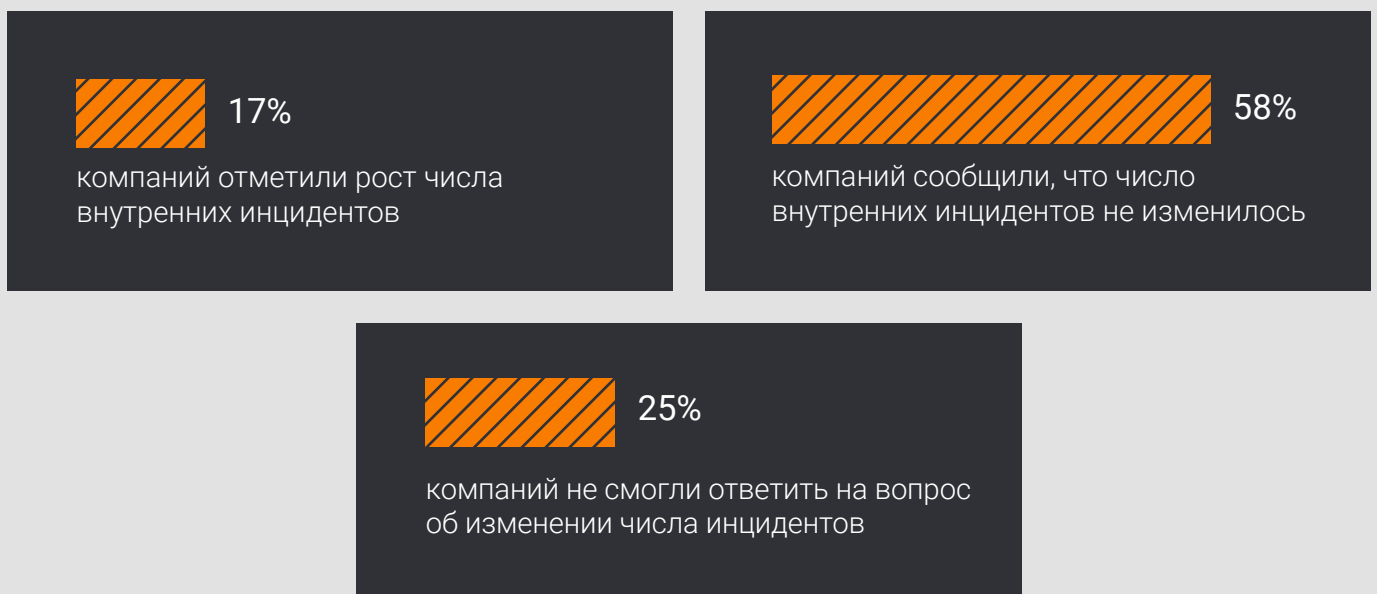
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:

* % ОТ ЧИСЛА ОТВЕТОВ



ДИНАМИКА

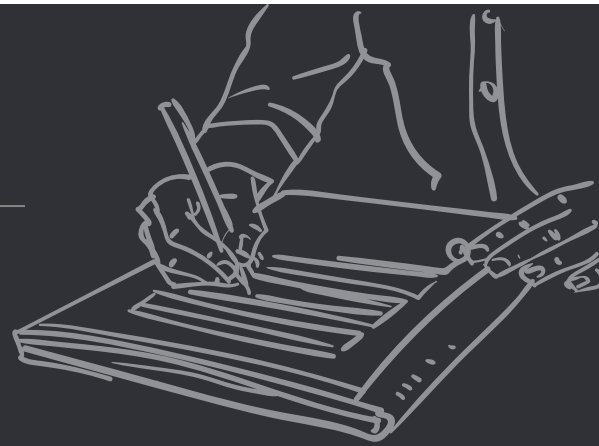
* % ОТ ЧИСЛА ОТВЕТОВ



СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

89%

РОССИЙСКИХ КОМПАНИЙ ПОДПИСЫВАЮТ
С СОТРУДНИКАМИ СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ



БЮДЖЕТ НА БЕЗОПАСНОСТЬ

* % ОТ ЧИСЛА ОТВЕТОВ



24%

компаний заявили
о росте бюджета
на безопасность



16%

компаний
сократили бюджет
на безопасность



60%

компаний сообщили
об отсутствии динамики
в изменении бюджета
в 2018 году

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа		92%
Средства администрирования Windows		82%
Firewall		75%
DLP-система		31%
IDS/IPS		15%
SIEM-система		6%

* МОЖНО БЫЛО ВЫБРАТЬ НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТОВ

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

* % ОТ ЧИСЛА ОТВЕТОВ



27%

Электронная почта



23%

Внешние носители



14%

Документы,
отправляемые на печать



12%

Телефония



9%

Интернет-
мессенджеры
(Telegram и т.д.)



8%

Облачные
хранилища



7%

Другое

РАБОТОДАТЕЛИ ОБРАЩАЮТ ВНИМАНИЕ НА ТАКИЕ ОСОБЕННОСТИ ПОВЕДЕНИЯ СОТРУДНИКОВ:

* % ОТ ЧИСЛА ОТВЕТОВ

21%

Распространение негативных
отзывов о компании

21%

Нелояльное отношение
к компании

16%

Подверженность
опасным зависимостям

21%

Саботирование работы

11%

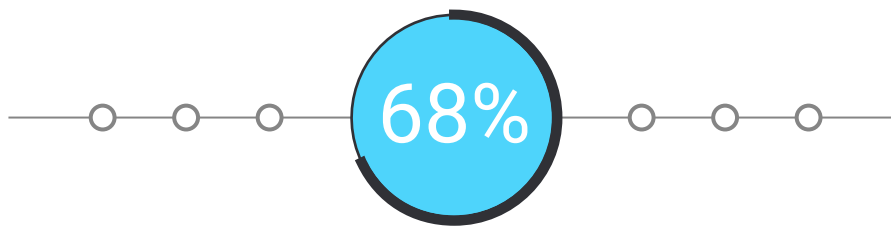
Извращенные,
девиантные интересы

10%

Симпатия к экстремистским и/или
террористическим организациям



УТЕЧКИ ИНФОРМАЦИИ



ПРОМЫШЛЕННЫХ КОМПАНИЙ СТОЛКНУЛИСЬ
С УТЕЧКАМИ ИНФОРМАЦИИ В 2018 ГОДУ

ЧТО УТЕКАЛО?

* % ОТ ЧИСЛА ОТВЕТОВ



35%

Техническая информация



25%

Информация о клиентах и сделках



17%

Информация о партнерах



16%

Персональные данные



5%

Внутренняя бухгалтерия



3%

Другое

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

* % ОТ ЧИСЛА ОТВЕТОВ



66%

опрошенных компаний скрыли инцидент и не делали никаких оповещений



30%

сообщили пострадавшим об инциденте и принесли извинения



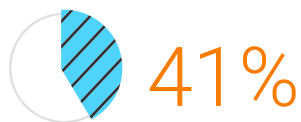
4%

сделали официальное заявление в СМИ

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

В этом году мы поинтересовались у сотрудников служб безопасности, какие инциденты кроме утечек информации они регистрировали чаще всего.

* % ОТ ЧИСЛА ОТВЕТОВ



Использование ресурсов компании в личных целях (майнинг, фриланс, онлайн-игры и т.п.)



Попытки откатов



Промышленный шпионаж/ работа в пользу конкурентов



Организация фирмы-боковика



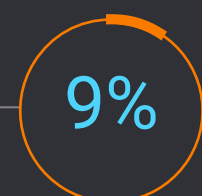
Другое

УЩЕРБ ОТ ИНЦИДЕНТОВ

* % ОТ ЧИСЛА ОТВЕТОВ



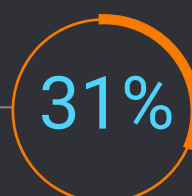
Имиджевый



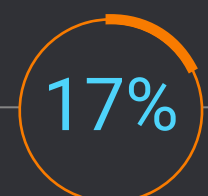
Compliance-риск (угроза или факт наказания от регулятора)



Крупный финансовый ущерб



Мелкий финансовый ущерб



Ущерба не было

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО

* % ОТ ЧИСЛА ОТВЕТОВ

Увольнение  37%

Штраф/лишение премии  27%

Выговор  21%

Судебное разбирательство  11%

Нет санкций  3%

РИТЕЙЛ

Подавляющее большинство компаний из сферы ритейла фиксировали утечки информации в минувшем году. 84% – это почти на 20% больше, чем в среднем по другим отраслям. Чаще всего утечкам подвергалась информация, которая является наиболее критичной для компаний этой отрасли – данные о клиентах и сделках. 80% нарушителей – это рядовые сотрудники. Большинство – менеджеры отдела снабжения (32%).



Гораздо чаще, чем в других отраслях, ритейлеры фиксируют финансовый ущерб **в результате действий инсайдеров**. В 36% случаев компании сообщали о том, что инциденты приводили к мелкому финансовому ущербу, еще в 12% случаев – к крупному.



Увольнение

Наиболее популярная практика, применяемая к нарушителям, – это увольнение. Так поступает 41% ответивших. Еще 36% объявляет выговор или лишает сотрудника премии.

В целом в ритейле наблюдается довольно хорошая оснащенность программными средствами защиты информации от внешних и внутренних угроз. Но при этом 14% компаний сократили бюджет на безопасность в минувшем году.

Доступными ИБ-средствами в ритейле чаще всего контролируют электронную почту, внешние хранилища, телефонию.



26%



19%

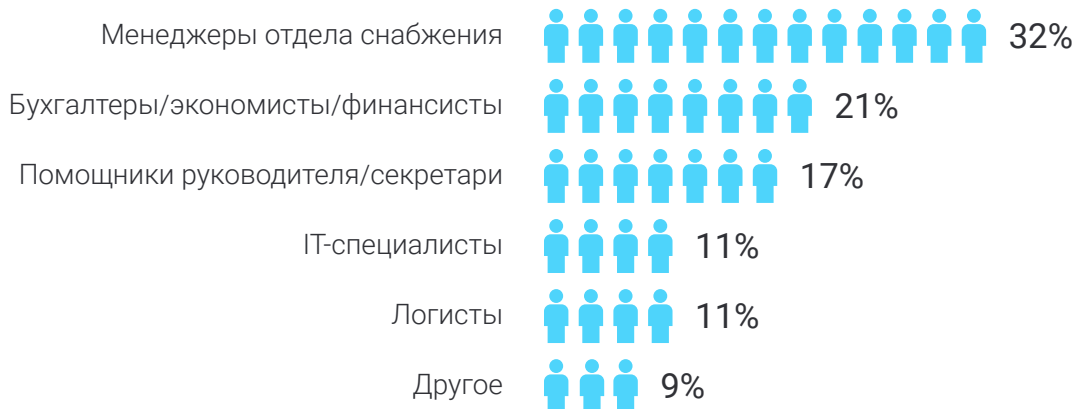


16%

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

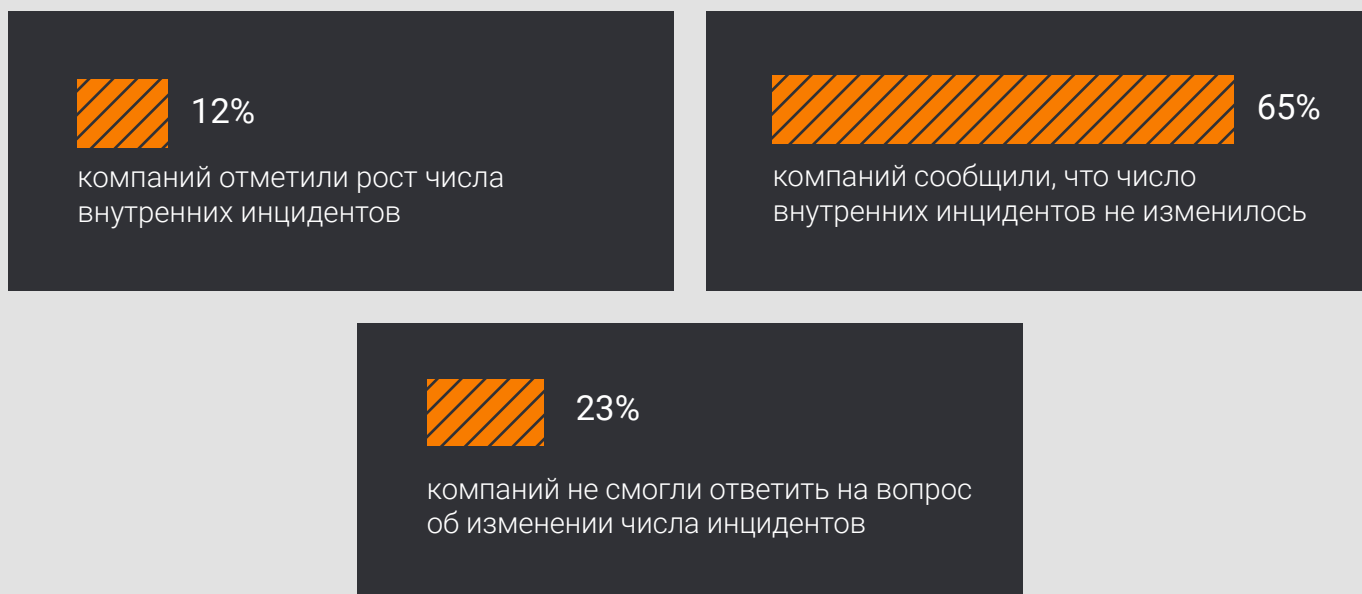
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:

* % ОТ ЧИСЛА ОТВЕТОВ



ДИНАМИКА

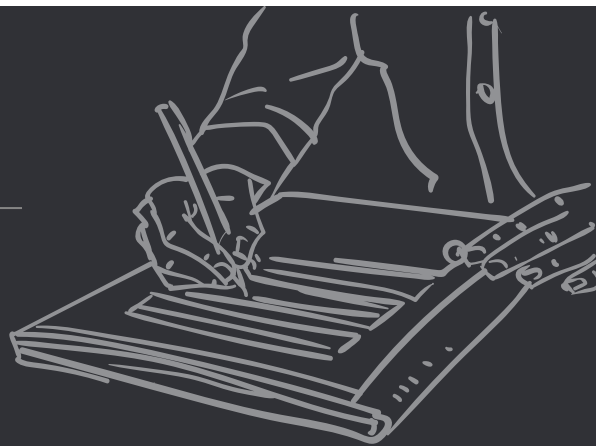
* % ОТ ЧИСЛА ОТВЕТОВ



СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

94%

РОССИЙСКИХ КОМПАНИЙ ПОДПИСЫВАЮТ
С СОТРУДНИКАМИ СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ



БЮДЖЕТ НА БЕЗОПАСНОСТЬ

* % ОТ ЧИСЛА ОТВЕТОВ



23%

компаний заявили
о росте бюджета
на безопасность



14%

компаний
сократили бюджет
на безопасность



63%

компаний сообщили
об отсутствии динамики
в изменении бюджета
в 2018 году

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа		91%
Средства администрирования Windows		85%
NGFW		76%
DLP-система		29%
IDS/IPS		15%
SIEM-система		9%

* МОЖНО БЫЛО ВЫБРАТЬ НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТОВ

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

* % ОТ ЧИСЛА ОТВЕТОВ



26%

Электронная почта



19%

Внешние носители



16%

Телефония



15%

Документы,
отправляемые на печать



10%

Интернет-
мессенджеры
(Telegram и т.д.)



10%

Облачные
хранилища

РАБОТОДАТЕЛИ ОБРАЩАЮТ ВНИМАНИЕ НА ТАКИЕ ОСОБЕННОСТИ ПОВЕДЕНИЯ СОТРУДНИКОВ:

* % ОТ ЧИСЛА ОТВЕТОВ

23%

Нелояльное отношение
к компании

22%

Распространение негативных
отзывов о компании

17%

Подверженность
опасным зависимостям

20%

Саботирование работы

9%

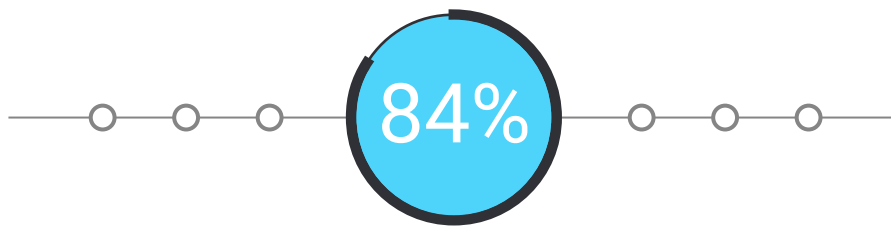
Извращенные,
девиантные интересы

9%

Симпатия к экстремистским и/или
террористическим организациям



УТЕЧКИ ИНФОРМАЦИИ



РИТЕЙЛ-КОМПАНИЙ СТОЛКНУЛИСЬ
С УТЕЧКАМИ ИНФОРМАЦИИ В 2018 ГОДУ

ЧТО УТЕКАЛО?

* % ОТ ЧИСЛА ОТВЕТОВ



33%

Информация
о клиентах и сделках



21%

Персональные
данные



17%

Информация
о партнерах



14%

Внутренняя
бухгалтерия



12%

Техническая
информация

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

* % ОТ ЧИСЛА ОТВЕТОВ



69%

опрошенных компаний
скрыли инцидент и не
делали никаких
оповещений



31%

сообщили
пострадавшим об
инциденте и принесли
извинения



0%

сделали официальное
заявление в СМИ

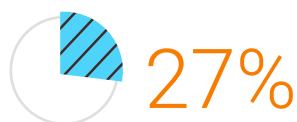
ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

В этом году мы поинтересовались у сотрудников служб безопасности, какие инциденты кроме утечек информации они регистрировали чаще всего.

* % ОТ ЧИСЛА ОТВЕТОВ



Использование ресурсов компании в личных целях (майнинг, фриланс, онлайн-игры и т.п.)



Попытки откатов



Промышленный шпионаж/
работа в пользу конкурентов



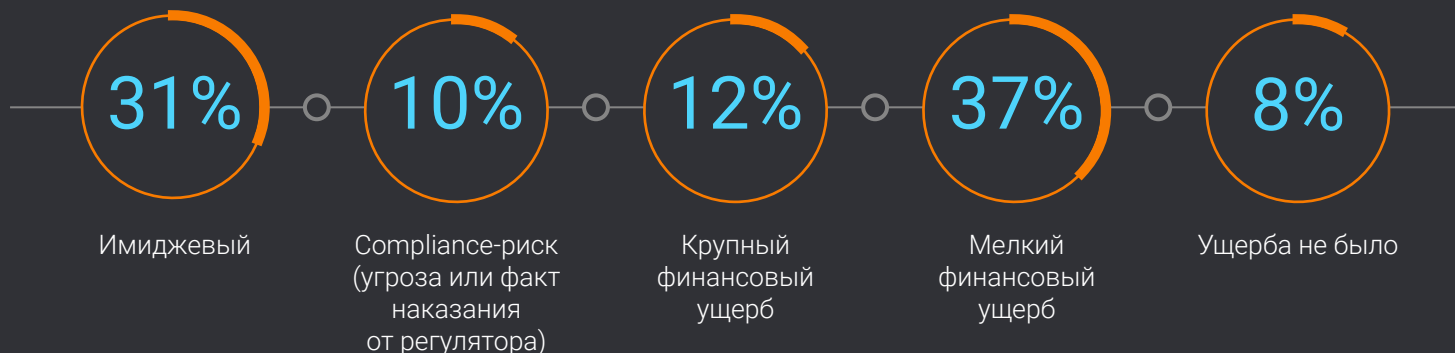
Другое



Организация фирмы-боковика

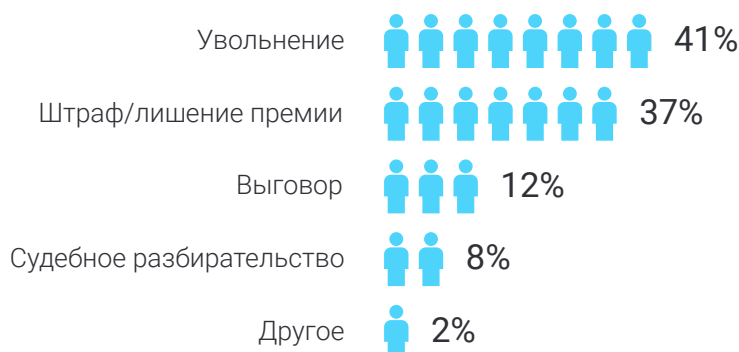
УЩЕРБ ОТ ИНЦИДЕНТОВ

* % ОТ ЧИСЛА ОТВЕТОВ



НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО

* % ОТ ЧИСЛА ОТВЕТОВ



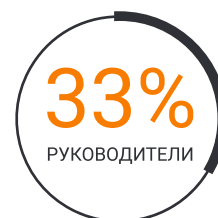
НЕДВИЖИМОСТЬ И СТРОИТЕЛЬСТВО



72% строительных компаний России столкнулись с утечками информации в 2018 году. Ответы о наиболее частых инцидентах информационной безопасности подтверждают, что традиционные для отрасли риски в виде создания боковых и откатных схем, торговли конфиденциальной информацией по-прежнему очень актуальны. По данным, полученным из опроса, в 2018 году чаще всего утекала коммерческая информация: данные о клиентах, сделках и партнерах, внутренняя бухгалтерия. Эти утечки в сумме составляют 50% всех инцидентов. Еще в 21% случаев утекала техническая информация.

Что касается других инцидентов, чаще всего компании сталкиваются с использованием сотрудниками ресурсов компании в личных целях (40%), попытками откатов (24%). Почти поровну распределились ответы о фактах организации боковых схем продаж (10%) и работы в пользу конкурентов (14%).

Среди нарушителей в строительстве, в отличие от других сфер, велико число руководителей – на их долю приходится 33% инцидентов. Среди нарушителей чаще всего встречаются менеджеры отдела снабжения. Второе и третье место занимают бухгалтеры/финансисты и помощники руководителя.

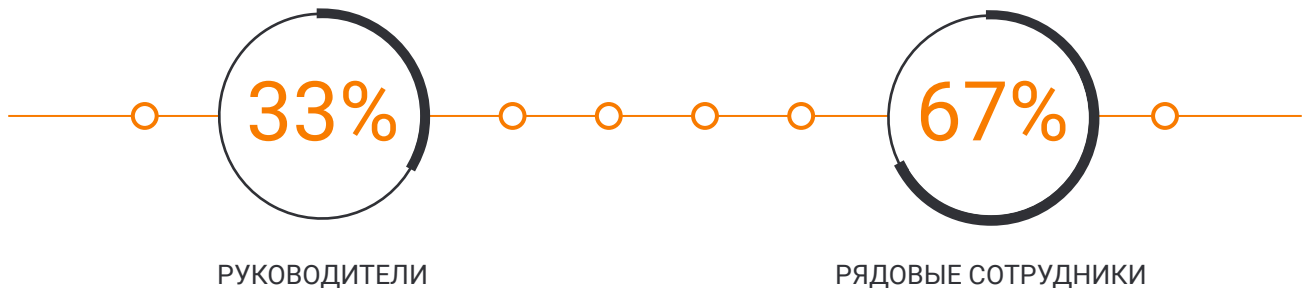


Нарушителей в строительной сфере предпочитают увольнять. В тройке популярных наказаний также выговор и штраф.

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

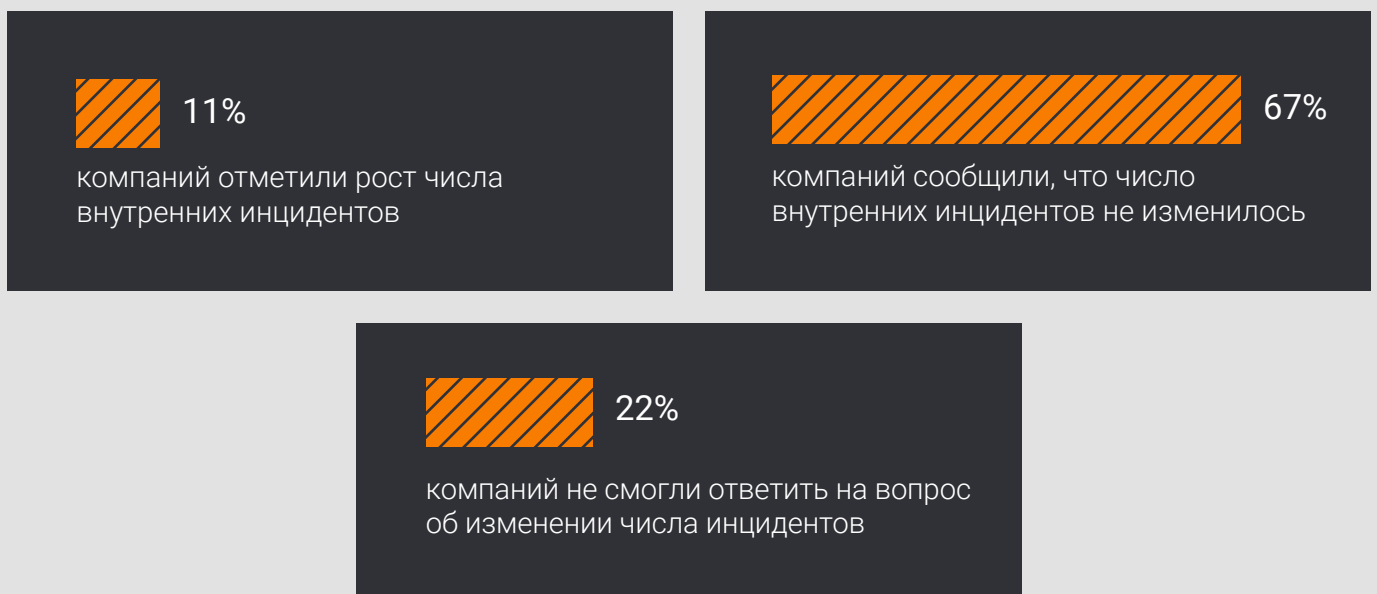
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:

* % ОТ ЧИСЛА ОТВЕТОВ



ДИНАМИКА

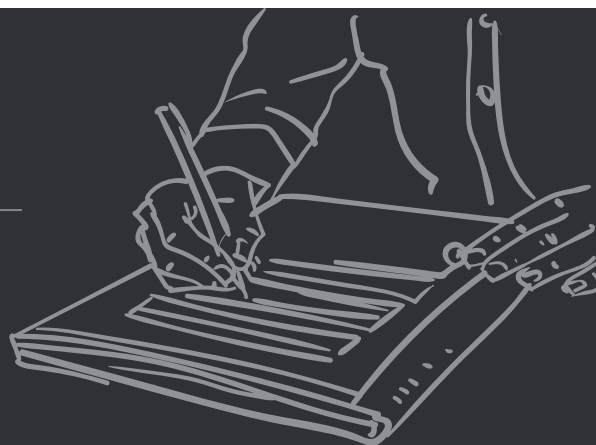
* % ОТ ЧИСЛА ОТВЕТОВ



СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

85%

РОССИЙСКИХ КОМПАНИЙ ПОДПИСЫВАЮТ
С СОТРУДНИКАМИ СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ



БЮДЖЕТ НА БЕЗОПАСНОСТЬ

* % ОТ ЧИСЛА ОТВЕТОВ



26%

компаний заявили
о росте бюджета
на безопасность



15%

компаний
сократили бюджет
на безопасность



59%

компаний сообщили
об отсутствии динамики
в изменении бюджета
в 2018 году

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа		92%
Средства администрирования Windows		78%
NGFW		65%
DLP-система		33%
IDS/IPS		6%
SIEM-система		6%

* МОЖНО БЫЛО ВЫБРАТЬ НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТОВ

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

* % ОТ ЧИСЛА ОТВЕТОВ



27%

Электронная почта



20%

Внешние носители



14%

Телефония



13%

Интернет-мессенджеры (Telegram и т.д.)



11%

Документы, отправляемые на печать



9%

Облачные хранилища



6%

Другое

РАБОТОДАТЕЛИ ОБРАЩАЮТ ВНИМАНИЕ НА ТАКИЕ ОСОБЕННОСТИ ПОВЕДЕНИЯ СОТРУДНИКОВ:

* % ОТ ЧИСЛА ОТВЕТОВ

23%

Саботирование работы

21%

Распространение негативных отзывов о компании

21%

Нелояльное отношение к компании

12%

Подверженность опасным зависимостям

12%

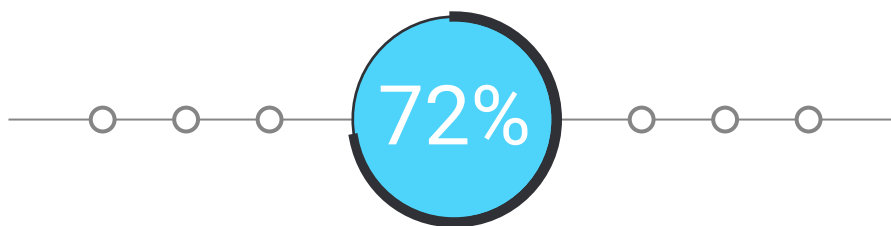
Извращенные, девиантные интересы

11%

Симпатия к экстремистским и/или террористическим организациям



УТЕЧКИ ИНФОРМАЦИИ



КОМПАНИЙ СТОЛКНУЛИСЬ С УТЕЧКАМИ
ИНФОРМАЦИИ В 2018 ГОДУ

ЧТО УТЕКАЛО?

* % ОТ ЧИСЛА ОТВЕТОВ



Информация
о клиентах и сделках



Техническая
информация



Персональные
данные



Информация
о партнерах



Внутренняя
бухгалтерия



Другое

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

* % ОТ ЧИСЛА ОТВЕТОВ



75%

опрошенных компаний
скрыли инцидент и не
делали никаких
оповещений



25%

сообщили
пострадавшим об
инциденте и принесли
извинения



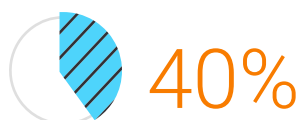
0%

сделали официальное
заявление в СМИ

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

В этом году мы поинтересовались у сотрудников служб безопасности, какие инциденты кроме утечек информации они регистрировали чаще всего.

* % ОТ ЧИСЛА ОТВЕТОВ



Использование ресурсов компании в личных целях (майнинг, фриланс, онлайн-игры и т.п.)



Попытки откатов



Промышленный шпионаж/ работа в пользу конкурентов



Другое



Организация фирмы-боковика

УЩЕРБ ОТ ИНЦИДЕНТОВ

* % ОТ ЧИСЛА ОТВЕТОВ



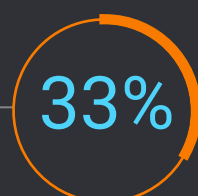
Имиджевый



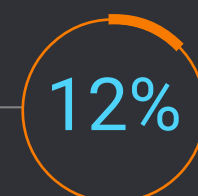
Compliance-риск (угроза или факт наказания от регулятора)



Крупный финансовый ущерб



Мелкий финансовый ущерб



Ущерба не было

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО

* % ОТ ЧИСЛА ОТВЕТОВ

Увольнение  34%

Штраф/лишение премии  26%

Выговор  25%

Судебное разбирательство  11%

Другое  2%