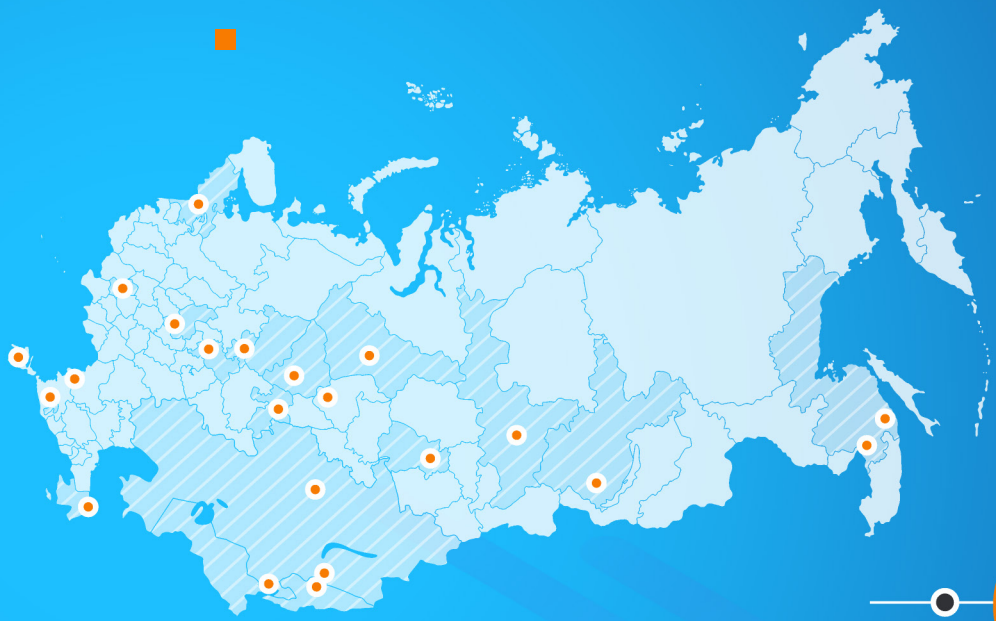
SEARCHINFORM

INFORMATION SECURITY

ИССЛЕДОВАНИЕ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В КОМПАНИЯХ РОССИИ И СНГ ЗА 2019 ГОД



www.searchinform.ru

2019

SEARCHINFORM
INFORMATION SECURITY

ИССЛЕДОВАНИЕ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПАНИЯХ РОССИИ И СНГ ЗА 2019 ГОД

Аналитики «СёрчИнформ» провели анонимный опрос компаний России и СНГ с целью оценить уровень информационной защиты и подход к вопросам ИБ. В исследовании приняли участие 1052 человека: начальники и сотрудники ИБ-подразделений, эксперты отрасли и руководители организаций из коммерческой (76%), государственной (22%) и некоммерческой сфер (2%).

Исследование затронуло IT, нефтегазовый сектор, промышленность и транспорт, кредитно-финансовую сферу, ритейл, здравоохранение и другие отрасли.

Комментирует руководитель отдела аналитики «СёрчИнформ» Алексей Парфентьев:

Предметом исследования были четыре темы: кто и в каких обстоятельствах становится нарушителем; насколько хорошо компании обеспечены защитными средствами; как часто бизнес сталкивается с утечками информации и другими инцидентами внутренней безопасности; какой ущерб несут работодатели и как наказывают нарушителей.

Сбор статистики по России и СНГ отдельно обусловлен тем, что существует разница в ИБ-практике этих регионов. Методики ИБ-специалистов из стран СНГ менее однородны, т.к. они аккумулируют и перенимают как российский, так и европейский опыт. Второй аспект – в большей части стран СНГ регулирование развивается медленнее, чем в России, и это отражается на том, с какими угрозами сталкиваются компании и в каком темпе внедряют защитные средства. И последний крайне важный фактор – российские компании обеспечены бюджетами на защиту информации лучше. В сумме это и определяет разницу в статистической картине.

ОГЛАВЛЕНИЕ

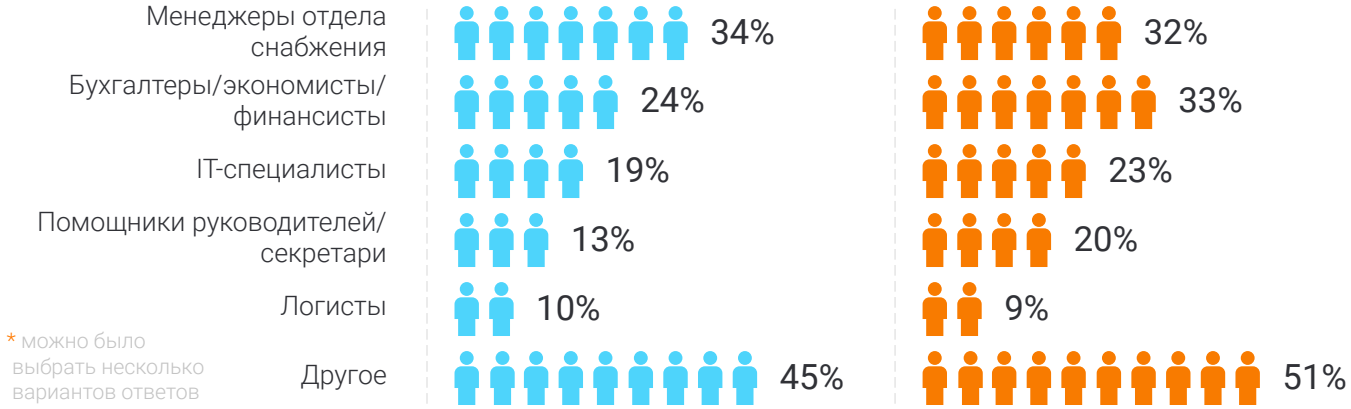
ЧАСТЬ I РОССИЯ И СНГ

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

77%
компаний считают внутренние инциденты более опасными, чем внешние

ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:

Руководители | Рядовые сотрудники



* можно было выбрать несколько вариантов ответов

40% компаний в России и 30% в СНГ сталкивались с попытками уволенных сотрудников навредить компании

ДИНАМИКА

16%
18%
компаний отметили рост числа внутренних инцидентов

52%
46%
компаний сообщили, что число внутренних инцидентов не изменилось

32%
36%
компаний не смогли ответить на вопрос об изменении числа инцидентов

Алексей Парфентьев:

Опрошенные единодушны: сотрудники могут нанести бизнесу больше вреда, чем киберпреступники и мошенники со стороны. Довольно однозначна и картина по типичному нарушителю. Это те, кто имеет доступ к ресурсам компании. Менеджеры снабжения, финансисты, секретари и помощники, которые близки к информации из «первых рук», к сожалению, оказываются в зоне риска. Еще более настораживают цифры по уволенным сотрудникам, которые пытаются навредить своему бывшему работодателю – в некоторых отраслях число пострадавших компаний приближается к 50%.

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

БЮДЖЕТ НА БЕЗОПАСНОСТЬ

25% 35%

компаний заявили о росте бюджета на безопасность

11% 11%

компаний сократили бюджет на безопасность

64% 54%

компаний сообщили об отсутствии динамики в изменении бюджета в 2019 году

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа	99%	97%
Средства администрирования Windows	87%	71%
NGFW (Firewall и Proxy)	63%	64%
Шифрование (криптошлюз, ПО)	46%	26%
DLP-система	31%	17%
Контроль целостности	24%	18%
IDS/IPS/EPS	17%	20%
SIEM-система	10%	11%
Другое	4%	3%
DCAP	1%	2%

* можно было выбрать несколько вариантов ответов

МЕТОДЫ ЗАЩИТЫ, КОТОРЫЕ ПРИМЕНЯЮТСЯ В ОРГАНИЗАЦИИ

99% | 84%
Разграничение доступов

75% | 63%
ИБ-инструктаж

60% | 52%
Изоляция критичных объектов IT-инфраструктуры (DMZ, закрытые подсети и т.д.)

59% | 49%
Сканирование инфраструктуры (инвентаризация, поиск уязвимостей и т.д.)

45% | 36%
Автоматизированный мониторинг IT-инфраструктуры (доступности, целостности и т.д.)

12% | 10%
Уменьшение времени детектирования и реагирования (SOC, SIEM)

* можно было выбрать несколько вариантов ответов

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

87% | 83%
Корпоративная почта

55% | 45%
Внешние носители

51% | 50%
ПО для администрирования (TeamViewer и т.п.)

42% | 28%
Документы, отправляемые на печать

40% | 33%
Телефония

37% | 36%
Мессенджеры корпоративные

30% | 29%
Общедоступная почта

27% | 29%
Облачные хранилища

22% | 22%
Мессенджеры общедоступные

9% | 14%
Другое

* можно было выбрать несколько вариантов ответов

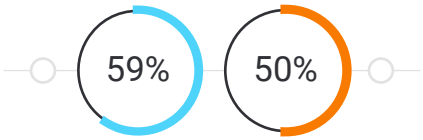
51% компаний в России **50%** компаний из СНГ используют услуги ИБ-аутсорсеров разово или постоянно

Алексей Парфентьев:

Работодатели стали активнее контролировать каналы передачи информации. Компании видят, как много шума в медиа-пространстве создают новости об утечках информации по вине инсайдеров и не хотят повторять чужой печальный опыт. Хотя не все компании обеспечены продвинутыми защитными средствами (см. раздел «используемые средства защиты»), в компаниях осознают важность контроля над основными каналами утечки информации (корпоративная почта, внешние устройства и др.) и осуществляют его доступными способами.

Компании стали более эффективно использовать имеющиеся ИБ-средства, которые уже «стоят на вооружении», в частности DLP-системы. Их настройка требует принятия не только технических мер, но и административных: приходится обучать персонал, разрабатывать политики безопасности и т.п. Компании демонстрируют все более вдумчивый и конструктивный подход в этом деле. Кроме того, половина опрошенных готовы разово или регулярно решать вопрос информационной безопасности более бюджетным и в то же время цивилизованным способом – с помощью аутсорсеров. При том, что компании не торопятся повышать бюджеты на информационную безопасность, готовность оптимизировать свою работу выглядит оптимистично.

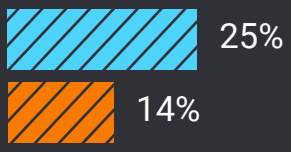
УТЕЧКИ ИНФОРМАЦИИ



российских и компаний в СНГ столкнулись с утечками информации в 2019 году

ЧТО УТЕКАЛО?

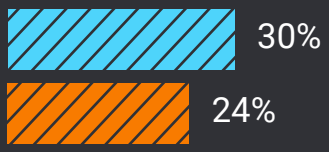
Информация о клиентах и сделках



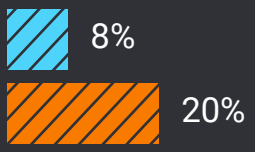
Техническая информация

Персональные данные

Финансовая информация



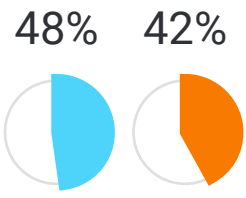
Никакая



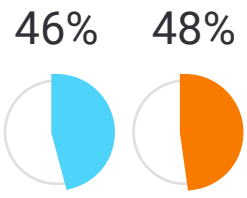
Другое

* можно было выбрать несколько вариантов ответов

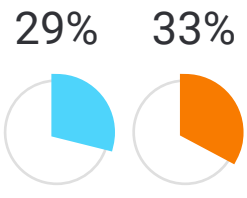
КАНАЛЫ УТЕЧЕК



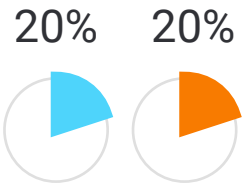
Почта



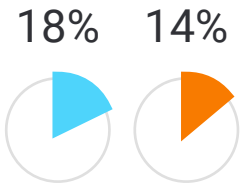
Устройства хранения и мобильные телефоны



Мессенджеры/телефония



Документы, отправляемые на печать



Облачные хранилища

* можно было выбрать несколько вариантов ответов

ABBYY

Вопрос от партнера «СёрчИнформ» – компании ABBYY, чей продукт FineReader Engine помогает предотвращать утечки информации в формате изображений.

51%

опрошенных говорит, что оборот документов в формате изображений в компании увеличился

КАКИЕ ТИПЫ ДОКУМЕНТОВ В ФОРМАТЕ ИЗОБРАЖЕНИЙ ЧАЩЕ ВСЕГО ПОДВЕРЖЕНЫ УТЕЧКАМ В ВАШЕЙ КОМПАНИИ?

46%

Юридически значимые документы (договоры с клиентами, контрагентами и пр.)

32%

Документы финансовой отчетности (бухгалтерские балансы, отчеты о прибылях и убытках и др.)

26%

Документы, удостоверяющие личность (паспорта, СНИЛС, водительские удостоверения и др.)

25%

Другое

Дмитрий Шушкин, генеральный директор ABBYY Россия:

Не первый год участники исследования отмечают рост утечек документов в формате изображений: сканов, фотографий, скриншотов и так далее. При этом в последнее время злоумышленников больше интересуют юридически значимые документы, такие как договоры. Это связано с тем, что на российском рынке, особенно в промышленной и нефтегазовой отрасли, усиливается конкуренция: компании борются за клиентов, стремясь обойти соперников по стоимости продукции, условиям контракта, срокам выполнения обязательств.

Потеря таких данных грозит не только репутационными рисками для компании, но и может привести к срыву сделок. Защитить бизнес призваны DLP-системы, усиленные интеллектуальными технологиями ABBYY. Они помогают определять тип документа и его содержание, позволяя предотвращать возможные утечки.

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

63% | 41%

опрошенных компаний скрыли инцидент и не делали никаких оповещений

27% | 36%

сообщили пострадавшим об инциденте и принесли извинения

15% | 31%

сообщили регулятору об инциденте

0% | 4%

сделали официальное заявление в СМИ

* можно было выбрать несколько вариантов ответов

Алексей Парфентьев:

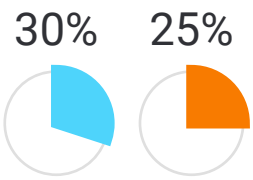
Число утечек хоть медленно, но стабильно снижается, правда это касается только компаний, где действительно занимаются безопасностью. Общее же число растет и в России, и по миру в целом.

Но цена слива становится все выше: СМИ стали гораздо внимательнее относиться к теме безопасности персональных данных, вопрос утечек стали поднимать даже на самом высоком государственном уровне. При этом печально, что отечественные компании так редко уведомляют СМИ о случившемся инциденте. Случаи единичны и в общей статистической картине не выходят за 0%. В СНГ ситуация тоже выглядит не радужно.

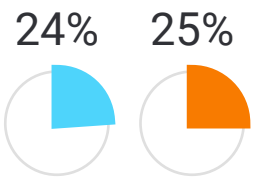
Чем раньше компании придут к пониманию, что им придется снабжать прессу комментариями о случившемся, тем скорее они смогут научиться нивелировать негативный эффект от публикации новостей и смогут смягчить удар по имиджу. В особой зоне риска – кредитно-финансовая сфера и здравоохранение, учитывая то, насколько критичными данными распоряжаются сотрудники этих отраслей в силу служебной необходимости. В банках почти 47% столкнулись с утечками персданных, в медорганизациях – 42% (читайте подробнее на стр. 21 и 46).

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

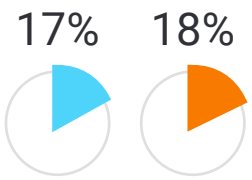
Только 9% российских и 17% компаний из СНГ сообщили, что не фиксировали инциденты внутренней безопасности в 2019 году.



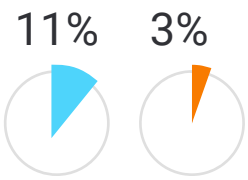
Попытки откатов



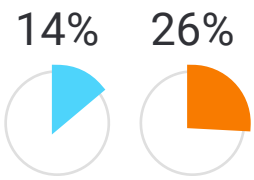
Промышленный шпионаж/ работа в пользу конкурентов



Саботаж



Создание фирмы-боковика

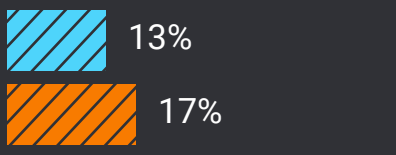


Другое

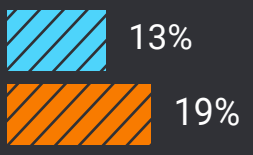
* можно было выбрать несколько вариантов ответов

УЩЕРБ ОТ ИНЦИДЕНТОВ

Имиджевый ущерб



Compliance-риск (угроза или факт наказания от регулятора)



Крупный финансовый ущерб

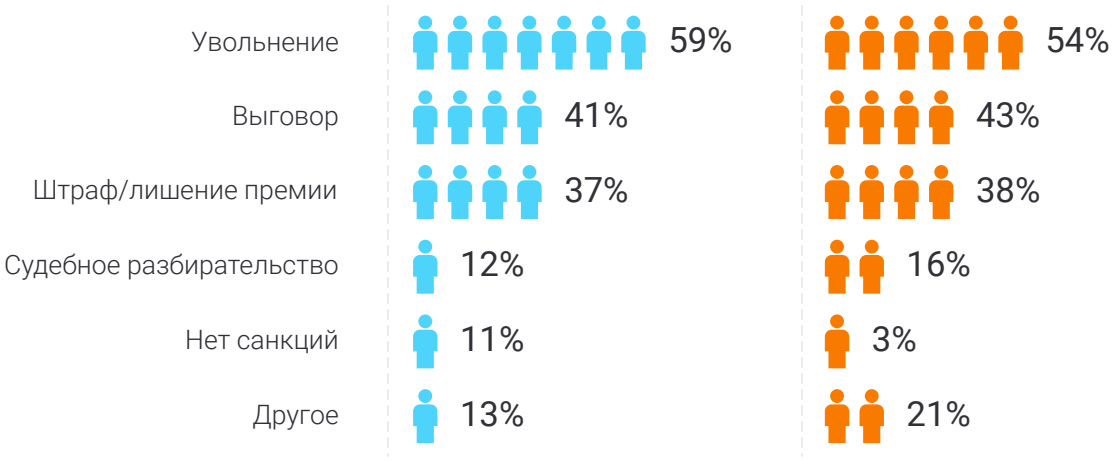
Мелкий финансовый ущерб

Ущерба не было

* можно было выбрать несколько вариантов ответов

SEARCHINFORM
INFORMATION SECURITY

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО:



* можно было выбрать несколько вариантов ответов

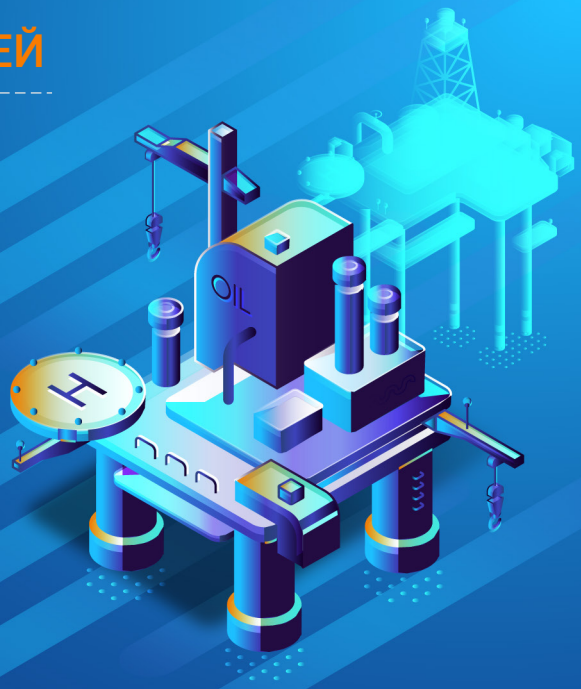
Алексей Парфентьев:

Только одной из десяти российских и 17% компаний из СНГ не пришлось разбираться с внутренними инцидентами. Помимо утечек мы спрашивали о нарушениях, которые приносят компаниям серьезный финансовый ущерб и блокируют продуктивную работу. Так, любопытно, что в тройке самых распространенных инцидентов внутренней безопасности опрошенные компании отметили саботаж. При этом чаще, чем в прошлом году, компании стали говорить о том, что фиксируют финансовый ущерб – об этом сообщили 52% российских и 62% компаний из СНГ.

ЧАСТЬ II В РАЗРЕЗЕ ОТРАСЛЕЙ

НЕФТЕГАЗОВАЯ СФЕРА

Ситуация в нефтегазовой сфере выгодно отличается от других отраслей – оснащенность средствами ИБ тут гораздо выше, а бюджеты растут более быстрыми темпами. 33% компаний заявляют об этом и только 2% бизнесов свои затраты, напротив, сократили.



Причина такого внимания к вопросу безопасности состоит в том числе и в регулировании вопросов защиты критической инфраструктуры. Но в первую очередь влияет объективная необходимость противостоять инцидентам по вине человеческого фактора – 87% компаний сообщили, что столкнулись с такими в минувшем году. Самыми распространенными инцидентами назвали попытки откатов, четверть компаний столкнулись с этим видом мошенничества. Закономерно, что наиболее частые виновники – менеджеры снабжения (в 44% случаев).

87%

компаний из нефтегазовой сферы столкнулись с инцидентами **по вине человеческого фактора**

44%

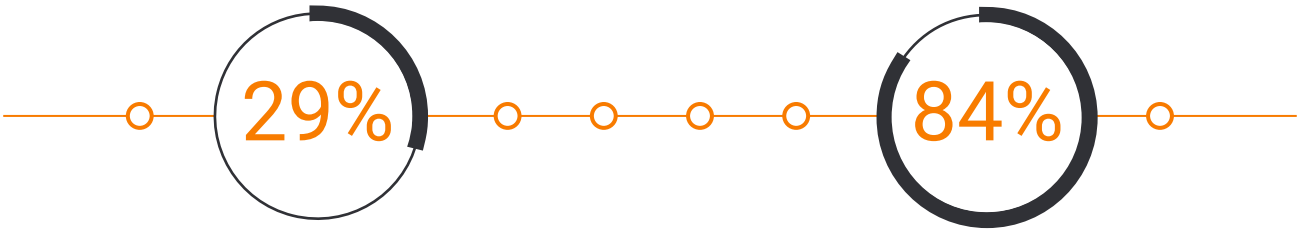
Менеджеры отдела снабжения – наиболее частые виновники мошенничества

60% компаний сообщили об утечках информации. Опасно, что сливается именно дорогая техническая информация – об этом сообщили 43% опрошенных.

SEARCHINFORM
INFORMATION SECURITY

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

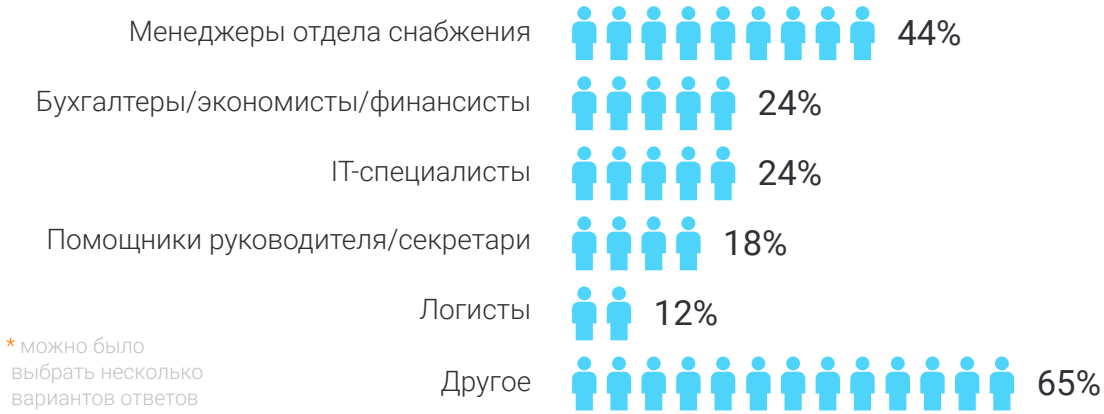
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:



Руководители

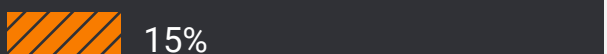
Рядовые сотрудники

* можно было выбрать несколько вариантов ответов



* можно было выбрать несколько вариантов ответов

ДИНАМИКА



компаний отметили рост числа внутренних инцидентов

компаний не смогли ответить на вопрос об изменении числа инцидентов

компаний сообщили, что число внутренних инцидентов не изменилось

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

БЮДЖЕТ НА БЕЗОПАСНОСТЬ

33%
компаний заявили о росте бюджета на безопасность

2%
компаний сократили бюджет на безопасность

64%
компаний сообщили об отсутствии динамики в изменении бюджета в 2019 году

* можно было выбрать несколько вариантов ответов

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа	100%	IDS/IPS/EPS	33%
Средства администрирования Windows	92%	Контроль целостности	31%
NGFW (Firewall и Proxy)	80%	SIEM-система	25%
DLP-система	59%	DCAP	4%
Шифрование (криптошлюз, ПО)	57%	Другое	8%

* можно было выбрать несколько вариантов ответов

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

90%
Корпоративная почта

72%
Внешние носители

63%
Документы, отправляемые на печать

51%
ПО для администрирования (TeamViewer и т.п.)

37%
Мессенджеры корпоративные

31%
Общедоступная почта

27%
Телефония

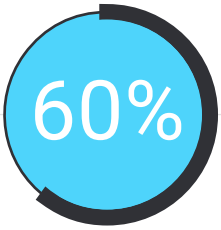
27%
Облачные хранилища

24%
Мессенджеры общедоступные

6%
Другое

* можно было выбрать несколько вариантов ответов

УТЕЧКИ ИНФОРМАЦИИ



компаний нефтегазовой сферы столкнулись со сливом данных

ЧТО УТЕКАЛО?

43%

Техническая информация

30%

Информация о клиентах и сделках

30%

Персональные данные

14%

Финансовая информация

8%

Другое

* можно было выбрать несколько вариантов ответов

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

69%

опрошенных компаний скрыли инцидент и не делали никаких оповещений

25%

сообщили пострадавшим об инциденте и принесли извинения

16%

сообщили регулятору об инциденте

0%

сделали официальное заявление в СМИ

* можно было выбрать несколько вариантов ответов

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

25%

Попытки откатов

15%

Саботаж

13%

Промышленный шпионаж/ работа в пользу конкурентов

3%

Создание фирмы-боковика

15%

Другое

* можно было выбрать несколько вариантов ответов

УЩЕРБ ОТ ИНЦИДЕНТОВ

42% Имиджевый ущерб

40% Мелкий финансовый ущерб

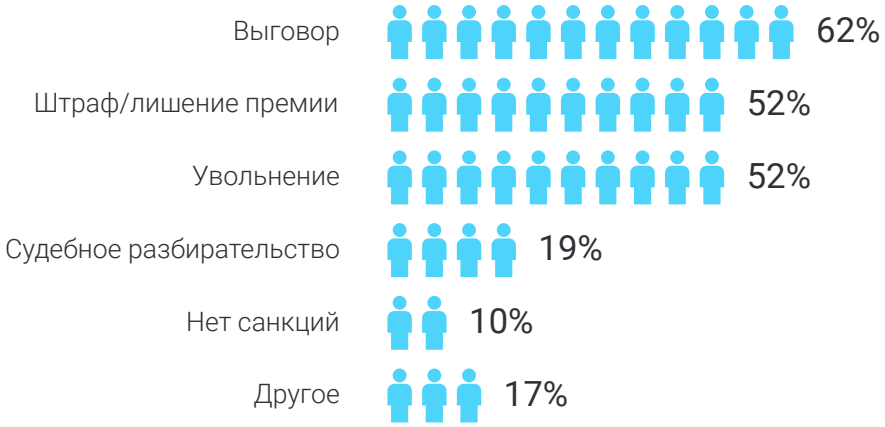
34% Ущерба не было

18% Compliance-риск (угроза или факт наказания от регулятора)

8% Крупный финансовый ущерб

* можно было выбрать несколько вариантов ответов

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО:



Выговор 62%

Штраф/лишение премии 52%

Увольнение 52%

Судебное разбирательство 19%

Нет санкций 10%

Другое 17%

SEARCHINFORM
INFORMATION SECURITY

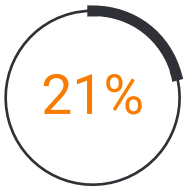
ПРОМЫШЛЕННОСТЬ

Результат опроса показывает, что в промышленности чаще, чем в других отраслях, прибегают к увольнению виновников инцидентов – так делает 70% опрошенных. При том, что профессиональный портрет нарушителя в промышленности выглядит вполне типично (чаще всего, это менеджер снабжения или финансист), в промышленности более распространены нарушения по вине руководителей. На них приходится треть инцидентов.

Для сравнения в ритейле или IT число виновников среди рядовых сотрудников приближается к 100%.

40% компаний сталкивается с откатными схемами

По этому показателю промышленность входит в топ-3 пострадавших от корпоративного мошенничества и воровства.



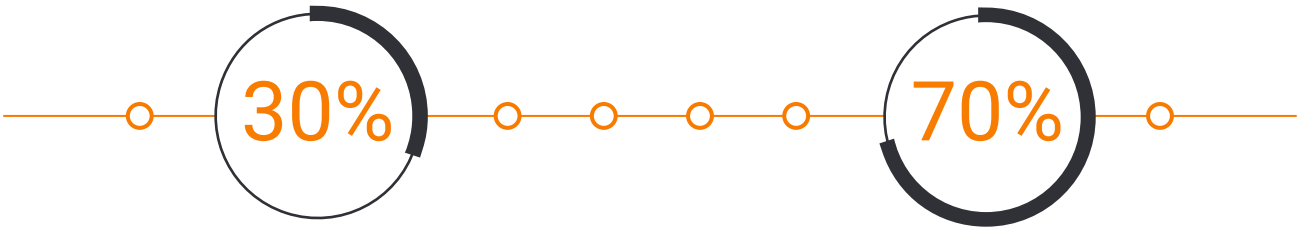
компаний заявляет, что инцидентов в 2019 году было больше, чем годом ранее.

Промышленным компаниям удается обнаруживать и предотвращать последствия инцидентов на ранних этапах. Об этом говорят данные об ущербе и обеспеченности ИБ-средствами, особенно для обнаружения инсайдерских угроз. DLP-системы стоят в 34% компаний.

SEARCHINFORM
INFORMATION SECURITY

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:



Руководители

Рядовые сотрудники

* можно было выбрать несколько вариантов ответов

* можно было выбрать несколько вариантов ответов

ДИНАМИКА

21%

компаний отметили рост числа внутренних инцидентов

34%

компаний не смогли ответить на вопрос об изменении числа инцидентов

45%

компаний сообщили, что число внутренних инцидентов не изменилось

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

БЮДЖЕТ НА БЕЗОПАСНОСТЬ

24%
компаний заявили о росте бюджета на безопасность

11%
компаний сократили бюджет на безопасность

65%
компаний сообщили об отсутствии динамики в изменении бюджета в 2019 году

* можно было выбрать несколько вариантов ответов

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа	97%	Контроль целостности	16%
Средства администрирования Windows	81%	IDS/IPS/EPS	11%
NGFW (Firewall и Proxy)	64%	SIEM-система	5%
Шифрование (криптошлюз, ПО)	43%	DCAP	1%
DLP-система	34%	Другое	2%

* можно было выбрать несколько вариантов ответов

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

86%
Корпоративная почта

53%
Внешние носители

48%
ПО для администрирования (TeamViewer и т.п.)

40%
Мессенджеры корпоративные

39%
Телефония

37%
Документы, отправляемые на печать

26%
Общедоступная почта

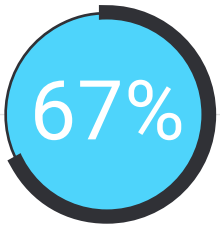
25%
Облачные хранилища

22%
Мессенджеры общедоступные

10%
Другое

* можно было выбрать несколько вариантов ответов

УТЕЧКИ ИНФОРМАЦИИ



промышленных компаний столкнулись
со сливом данных

ЧТО УТЕКАЛО?

47%

Информация
о клиентах и сделках

44%

Техническая
информация

29%

Финансовая
информация

24%

Персональные
данные

8%

Другое

* можно было выбрать несколько вариантов ответов

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

65%

опрошенных компаний скрыли инцидент и не делали никаких оповещений

25%

сообщили пострадавшим об инциденте и принесли извинения

16%

сообщили регулятору об инциденте

0%

сделали официальное заявление в СМИ

* можно было выбрать несколько вариантов ответов

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

40%

Попытки откатов

37%

Промышленный шпионаж/ работа в пользу конкурентов

16%

Создание фирмы-боковика

15%

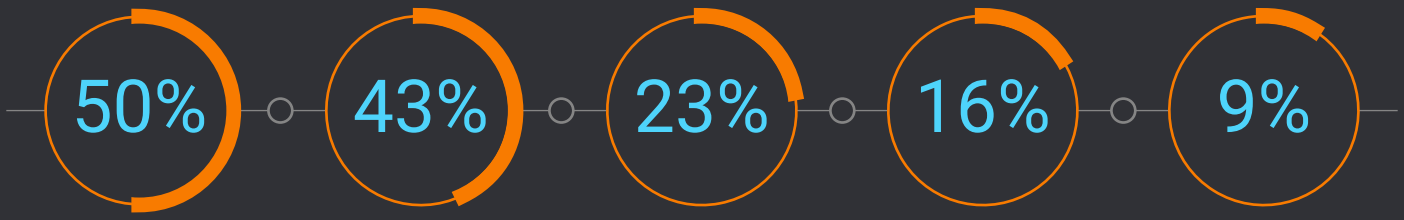
Саботаж

10%

Другое

* можно было выбрать несколько вариантов ответов

УЩЕРБ ОТ ИНЦИДЕНТОВ



50% Мелкий финансовый ущерб

43% Имиджевый ущерб

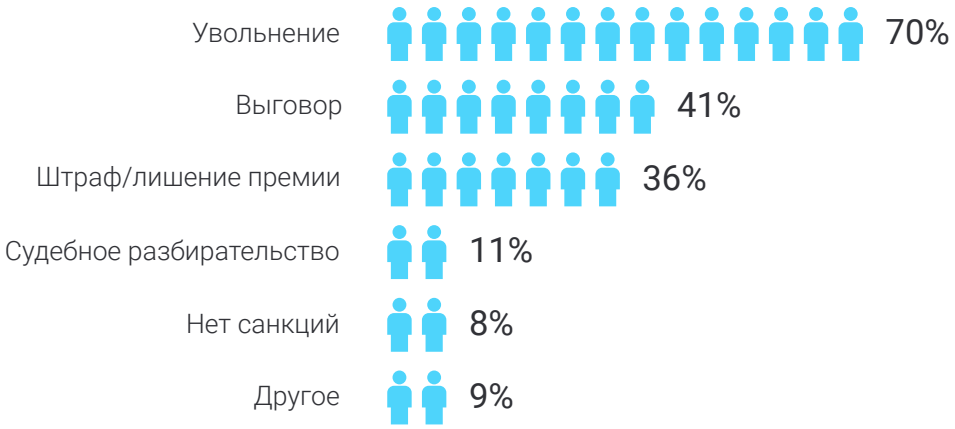
23% Ущерба не было

16% Крупный финансовый ущерб

9% Compliance-риск (угроза или факт наказания от регулятора)

* можно было выбрать несколько вариантов ответов

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО:



SEARCHINFORM
INFORMATION SECURITY

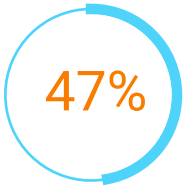
КРЕДИТНО-ФИНАНСОВАЯ СФЕРА

В финансовой сфере, благодаря активным действиям регулятора (Центральный Банк РФ), собраны наиболее объективные данные об информационной безопасности в корпоративном секторе. После года проведения проверок ФинЦЕРТ (подразделение ЦБ РФ) выявил почти 700 нарушений и признал, что все они были связаны с человеческим фактором.

Нарушения банков приводили к тому, что у сотрудников без необходимости расширялись права доступа, а настройки защитных программ снижались.

Данные опроса говорят, что 44% **компаний столкнулись с риском или наказанием от регулятора**, т.е. несли так называемые compliance-риски. Помимо давления регулятора, кредитно-финансовая сфера сильнее, чем другие отрасли, привлекает внимание СМИ: новости об утечках в банках получают большой резонанс.

У общества есть повод для беспокойства: банки, как и другие компании, неохотно подтверждают информацию об утечках – 64% не делают оповещений при том, что 68% столкнулись со сливами данных.



опрошенных сообщили, что утекали персональные данные клиентов.

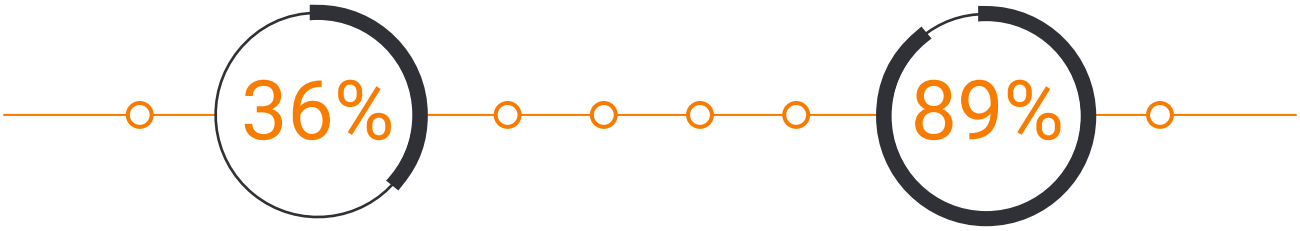
Показатели обращения в суд по фактам инсайдерских нарушений гораздо выше, чем по другим отраслям –

31% **финансовых компаний инициировали разбирательства.**

SEARCHINFORM
INFORMATION SECURITY

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:



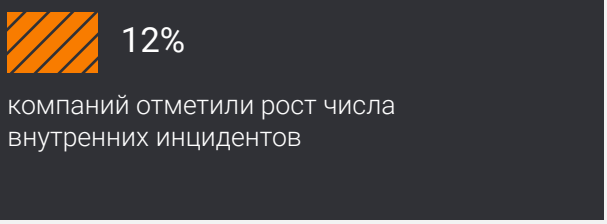
Руководители

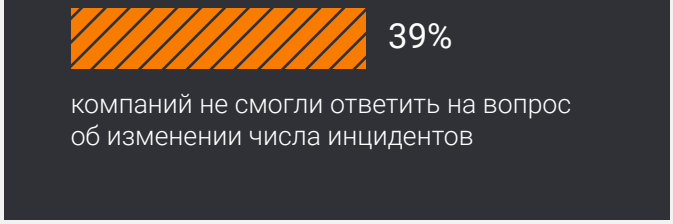
Рядовые сотрудники

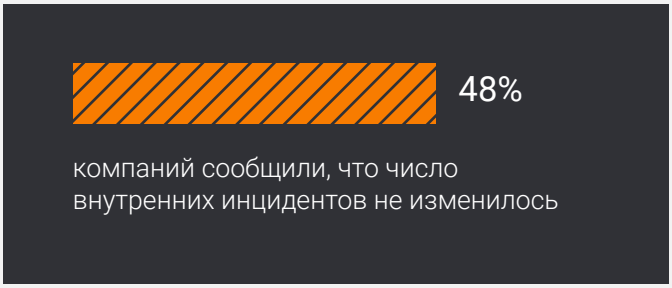
* можно было выбрать несколько вариантов ответов

* можно было выбрать несколько вариантов ответов

ДИНАМИКА







СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

БЮДЖЕТ НА БЕЗОПАСНОСТЬ

30%
компаний заявили о росте бюджета на безопасность

11%
компаний сократили бюджет на безопасность

59%
компаний сообщили об отсутствии динамики в изменении бюджета в 2019 году

* можно было выбрать несколько вариантов ответов

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа	100%	DLP-система	53%
Средства администрирования Windows	91%	IDS/IPS/EPS	40%
NGFW (Firewall и Proxy)	80%	SIEM-система	22%
Шифрование (криптошлюз, ПО)	76%	DCAP	4%
Контроль целостности	56%	Другое	2%

* можно было выбрать несколько вариантов ответов

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

93%
Корпоративная почта

82%
Внешние носители

58%
Документы, отправляемые на печать

51%
Мессенджеры корпоративные

47%
Общедоступная почта

44%
ПО для администрирования (TeamViewer и т.п.)

40%
Телефония

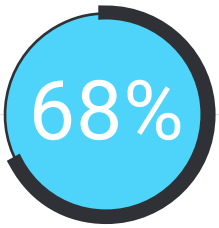
29%
Облачные хранилища

29%
Мессенджеры общедоступные

4%
Другое

* можно было выбрать несколько вариантов ответов

УТЕЧКИ ИНФОРМАЦИИ



финансовых компаний столкнулись
со сливом данных

ЧТО УТЕКАЛО?

53%

Информация
о клиентах и сделках

47%

Персональные
данные

31%

Финансовая
информация

14%

Другое

8%

Техническая
информация

* можно было выбрать несколько вариантов ответов

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

64%

опрошенных компаний скрыли инцидент и не делали никаких оповещений

45%

сообщили регулятору об инциденте

18%

сообщили пострадавшим об инциденте и принесли извинения

0%

сделали официальное заявление в СМИ

* можно было выбрать несколько вариантов ответов

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

19%

Саботаж

16%

Промышленный шпионаж/ работа в пользу конкурентов

10%

Создание фирмы-боковика

6%

Попытки откатов

29%

Другое

* можно было выбрать несколько вариантов ответов

УЩЕРБ ОТ ИНЦИДЕНТОВ

59% Имиджевый ущерб

44% Compliance-риск (угроза или факт наказания от регулятора)

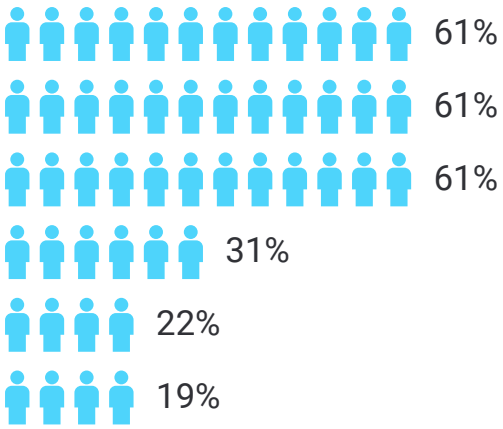
38% Мелкий финансовый ущерб

31% Ущерба не было

16% Крупный финансовый ущерб

* можно было выбрать несколько вариантов ответов

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО:



Увольнение 61%

Выговор 61%

Штраф/лишение премии 61%

Судебное разбирательство 31%

Нет санкций 22%

Другое 19%

SEARCHINFORM
INFORMATION SECURITY

РИТЕЙЛ

Ритейл – одна из самых уязвимых отраслей: 98% опрошенных заявили, что нарушения сотрудников опаснее, чем действия внешних злоумышленников.

92%

опрошенных компаний столкнулись с утечками информации – это абсолютный максимум среди отраслей, на треть больше, чем по сводной статистике.

Утечкам гораздо чаще подвергается информация, которая напрямую влияет на бизнес-процессы и финансовые показатели компаний. 59% опрошенных сказали, что сталкивались со сливами баз клиентов и сделок (складских остатков, условий работы с поставщиками и т. д.), 44% теряли финансовую информацию.

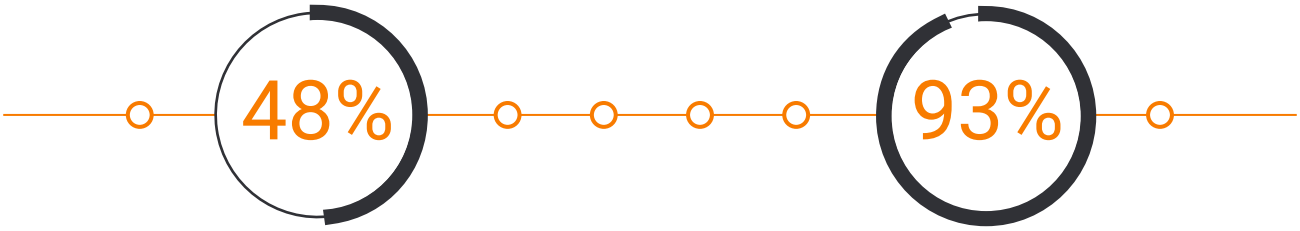
Проблема в том, что бизнес-процессы в ритейле требуют, чтобы доступ к конфиденциальным данным был у широкого круга сотрудников, в том числе удаленно. Таким образом, обеспечить безопасность, не затормозив бизнес-процессы, оказывается сложно.

Компаниям придется наращивать объемы внедрения многофункциональных DLP-систем – пока они установлены только в 29% организаций. Помимо утечек, высок процент и других нарушений по вине сотрудников: откатных схем, работы в пользу конкурентов, саботажа.

Это отражается на том, какой ущерб несут компании. Гораздо реже, чем в целом по другим отраслям, торговые компании фиксируют имиджевые риски. Зато с финансовым ущербом сталкиваются намного чаще. Пятая часть опрошенных ритейлеров понесла крупные финансовые потери, еще 67% зафиксировали мелкий ущерб.

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

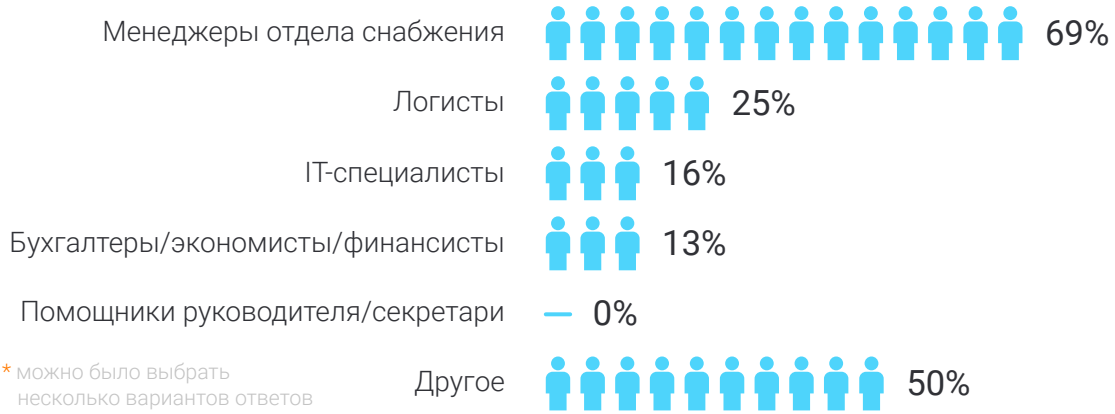
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:



Руководители

Рядовые сотрудники

* можно было выбрать несколько вариантов ответов



* можно было выбрать несколько вариантов ответов

ДИНАМИКА

21%

компаний отметили рост числа внутренних инцидентов

36%

компаний не смогли ответить на вопрос об изменении числа инцидентов

43%

компаний сообщили, что число внутренних инцидентов не изменилось

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

БЮДЖЕТ НА БЕЗОПАСНОСТЬ

29%
компаний заявили о росте бюджета на безопасность

10%
компаний сократили бюджет на безопасность

61%
компаний сообщили об отсутствии динамики в изменении бюджета в 2019 году

* можно было выбрать несколько вариантов ответов

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа	100%	Контроль целостности	20%
Средства администрирования Windows	94%	IDS/IPS/EPS	6%
NGFW (Firewall и Proxy)	69%	SIEM-система	4%
Шифрование (криптошлюз, ПО)	33%	DCAP	0%
DLP-система	29%	Другое	2%

* можно было выбрать несколько вариантов ответов

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

100%
Корпоративная почта

60%
Мессенджеры корпоративные

57%
ПО для администрирования (TeamViewer и т.п.)

43%
Внешние носители

40%
Телефония

40%
Документы, отправляемые на печать

36%
Мессенджеры общедоступные

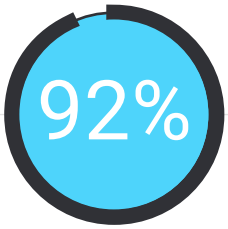
34%
Облачные хранилища

32%
Общедоступная почта

6%
Другое

* можно было выбрать несколько вариантов ответов

УТЕЧКИ ИНФОРМАЦИИ



торговых компаний столкнулись
со сливом данных

ЧТО УТЕКАЛО?

59%

Информация о клиентах и сделках

44%

Финансовая информация

10%

Персональные данные

10%

Техническая информация

3%

Другое

* можно было выбрать несколько вариантов ответов

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

59%

опрошенных компаний скрыли инцидент и не делали никаких оповещений

32%

сообщили пострадавшим об инциденте и принесли извинения

15%

сообщили регулятору об инциденте

0%

сделали официальное заявление в СМИ

* можно было выбрать несколько вариантов ответов

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

42%

Попытки откатов

39%

Промышленный шпионаж/ работа в пользу конкурентов

31%

Саботаж

19%

Создание фирмы-боковика

3%

Другое

* можно было выбрать несколько вариантов ответов

УЩЕРБ ОТ ИНЦИДЕНТОВ

67% Мелкий финансовый ущерб

26% Имиджевый ущерб

26% Ущерба не было

21% Крупный финансовый ущерб

8% Compliance-риск (угроза или факт наказания от регулятора)

* можно было выбрать несколько вариантов ответов

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО:

SEARCHINFORM
INFORMATION SECURITY

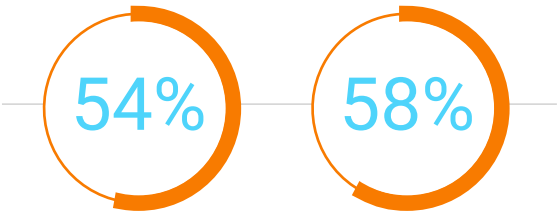
СФЕРА IT

Главный капитал IT-сферы – люди и интеллектуальная собственность, поэтому вопросы информационной безопасности и защищенности данных здесь стоят остро.

Опрошенные признают, что внутренние инциденты опасны и дорого обходятся компаниям.

Подавляющее большинство респондентов (86%) считает, что внутренние инциденты опаснее внешних и 84% фиксировали их в 2019 году.

Причем чаще, чем в других отраслях на кону стоит репутация – 54% опрошенных фиксировали имиджевый ущерб в результате инцидентов в 2019 году, еще 58% – финансовые потери.

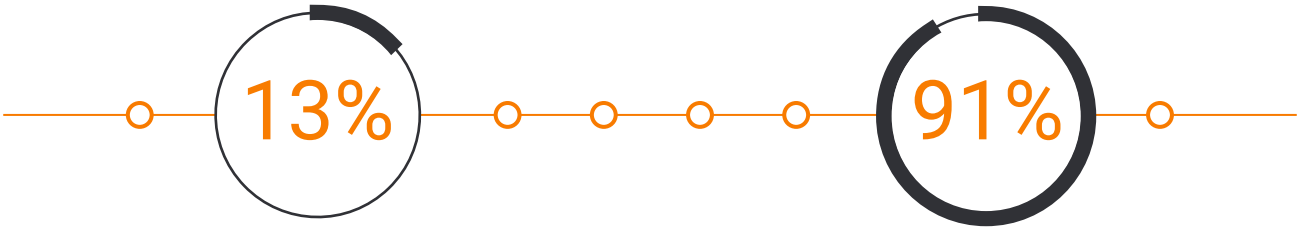


Но если взглянуть на картину обеспеченности техническими средствами, видно, что от сторонних злоумышленников IT-компании защищают периметр очень хорошо. Внутренним угрозам уделяют меньше внимания.

SEARCHINFORM
INFORMATION SECURITY

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:



Руководители

Рядовые сотрудники

* можно было выбрать несколько вариантов ответов

* можно было выбрать несколько вариантов ответов

ДИНАМИКА

16%

компаний отметили рост числа внутренних инцидентов

54%

компаний не смогли ответить на вопрос об изменении числа инцидентов

59%

компаний сообщили, что число внутренних инцидентов не изменилось

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

БЮДЖЕТ НА БЕЗОПАСНОСТЬ

25%
компаний заявили о росте бюджета на безопасность

8%
компаний сократили бюджет на безопасность

67%
компаний сообщили об отсутствии динамики в изменении бюджета в 2019 году

* можно было выбрать несколько вариантов ответов

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа	92%	Контроль целостности	25%
Средства администрирования Windows	82%	DLP-система	20%
NGFW (Firewall и Proxy)	70%	SIEM-система	15%
Шифрование (криптошлюз, ПО)	54%	DCAP	0%
IDS/IPS/EPS	25%	Другое	9%

* можно было выбрать несколько вариантов ответов

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

77%
Корпоративная почта

44%
Внешние носители

43%
Телефония

41%
ПО для администрирования (TeamViewer и т.п.)

38%
Документы, отправляемые на печать

25%
Мессенджеры корпоративные

25%
Общедоступная почта

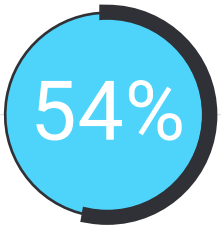
25%
Облачные хранилища

14%
Мессенджеры общедоступные

8%
Другое

* можно было выбрать несколько вариантов ответов

УТЕЧКИ ИНФОРМАЦИИ



IT-компаний столкнулись
со сливом данных

ЧТО УТЕКАЛО?

38%

Информация
о клиентах и сделках

27%

Техническая
информация

22%

Персональные
данные

15%

Финансовая информация

5%

Другое

* можно было выбрать несколько вариантов ответов

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

75%

опрошенных компаний скрыли инцидент и не делали никаких оповещений

38%

сообщили пострадавшим об инциденте и принесли извинения

7%

сообщили регулятору об инциденте

0%

сделали официальное заявление в СМИ

* можно было выбрать несколько вариантов ответов

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

30%

Попытки откатов

26%

Промышленный шпионаж/ работа в пользу конкурентов

11%

Саботаж

8%

Создание фирмы-боковика

18%

Другое

* можно было выбрать несколько вариантов ответов

УЩЕРБ ОТ ИНЦИДЕНТОВ

54% Имиджевый ущерб

50% Мелкий финансовый ущерб

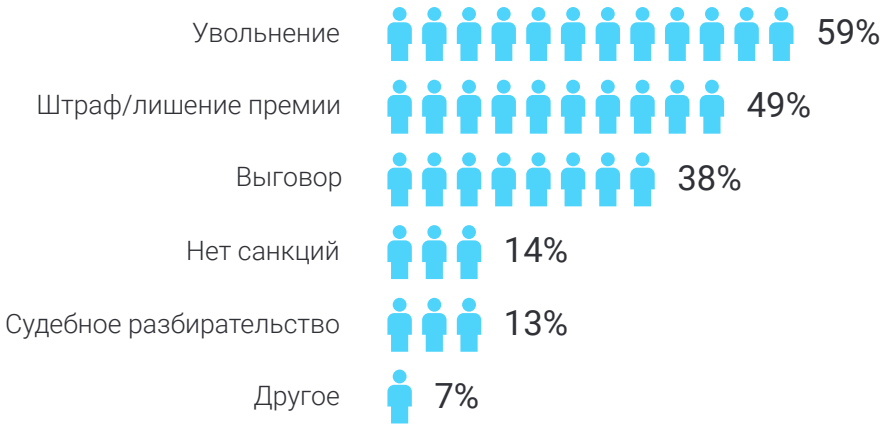
32% Ущерба не было

13% Compliance-риск (угроза или факт наказания от регулятора)

8% Крупный финансовый ущерб

* можно было выбрать несколько вариантов ответов

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО:



Увольнение 59%

Штраф/лишение премии 49%

Выговор 38%

Нет санкций 14%

Судебное разбирательство 13%

Другое 7%

SEARCHINFORM
INFORMATION SECURITY

СТРОИТЕЛЬСТВО

Оснащенность IT-средствами для защиты внешнего периметра в строительстве достаточная. Антивирусные программы стоят в 94% компаний, средства администрирования Windows – в 84%, межсетевые экраны – в половине организаций.

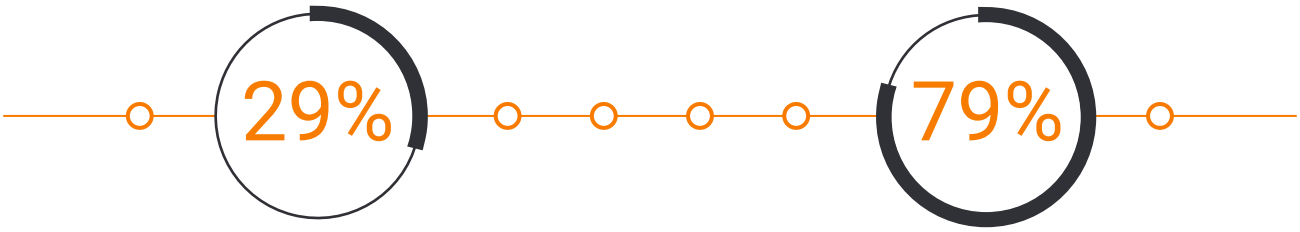
Но обеспеченность системами контроля действий сотрудников на рабочем месте хуже, чем в среднем по другим отраслям. Они установлены в трети компаний. Ситуацию усугубляет то, что строительные компании активнее остальных сокращают бюджет на ИБ.

16%
компаний сократили бюджет на безопасность

Несмотря на объемы закупок в строительстве, менеджеры снабжения – не самые частые виновники инцидентов в отрасли. С махинациями финансистов и бухгалтеров компании сталкивались чаще – в 31% случаев.

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

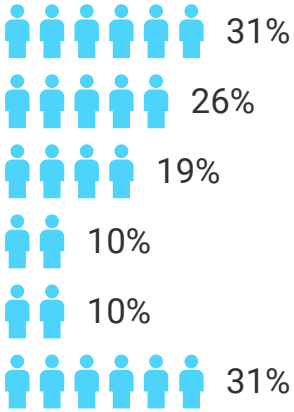
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:



Руководители

Рядовые сотрудники

* можно было выбрать несколько вариантов ответов



* можно было выбрать несколько вариантов ответов

ДИНАМИКА

14%

компаний отметили рост числа внутренних инцидентов

23%

компаний не смогли ответить на вопрос об изменении числа инцидентов

63%

компаний сообщили, что число внутренних инцидентов не изменилось

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

БЮДЖЕТ НА БЕЗОПАСНОСТЬ

18%
компаний заявили о росте бюджета на безопасность

16%
компаний сократили бюджет на безопасность

68%
компаний сообщили об отсутствии динамики в изменении бюджета в 2019 году

* можно было выбрать несколько вариантов ответов

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа	94%	Контроль целостности	13%
Средства администрирования Windows	84%	SIEM-система	4%
NGFW (Firewall и Proxy)	50%	IDS/IPS/EPS	2%
DLP-система	29%	DCAP	2%
Шифрование (криптошлюз, ПО)	23%	Другое	6%

* можно было выбрать несколько вариантов ответов

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

86%
Корпоративная почта

54%
Внешние носители

54%
ПО для администрирования (TeamViewer и т.п.)

44%
Мессенджеры корпоративные

36%
Телефония

34%
Общедоступная почта

32%
Документы, отправляемые на печать

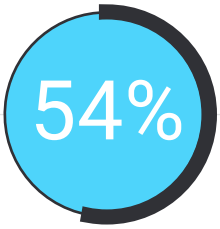
30%
Облачные хранилища

26%
Мессенджеры общедоступные

4%
Другое

* можно было выбрать несколько вариантов ответов

УТЕЧКИ ИНФОРМАЦИИ



строительных компаний
столкнулись со сливом данных

ЧТО УТЕКАЛО?

37%
Информация о клиентах и сделках

35%
Техническая информация

30%
Финансовая информация

12%
Персональные данные

9%
Другое

* можно было выбрать несколько вариантов ответов

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

69%
опрошенных компаний скрыли инцидент и не делали никаких оповещений

17%
сообщили пострадавшим об инциденте и принесли извинения

11%
сообщили регулятору об инциденте

3%
сделали официальное заявление в СМИ

* можно было выбрать несколько вариантов ответов

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

43%

Промышленный шпионаж/ работа в пользу конкурентов

38%

Попытки откатов

16%

Саботаж

16%

Создание фирмы-боковика

14%

Другое

* можно было выбрать несколько вариантов ответов

УЩЕРБ ОТ ИНЦИДЕНТОВ

35% Имиджевый ущерб

35% Мелкий финансовый ущерб

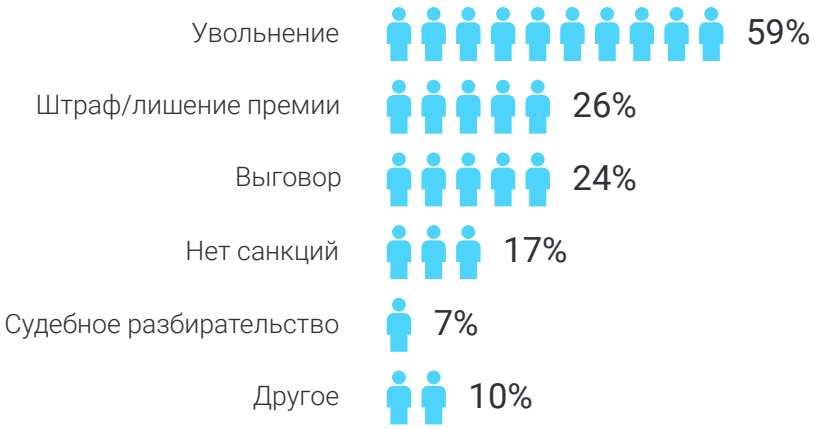
35% Ущерба не было

19% Крупный финансовый ущерб

11% Compliance-риск (угроза или факт наказания от регулятора)

* можно было выбрать несколько вариантов ответов

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО:



Увольнение 59%

Штраф/лишение премии 26%

Выговор 24%

Нет санкций 17%

Судебное разбирательство 7%

Другое 10%

SEARCHINFORM
INFORMATION SECURITY

ЛОГИСТИЧЕСКАЯ СФЕРА

В логистике угрозы внутренней безопасности приносят бизнесу прямые финансовые убытки. Это воровство, связанное с большим количеством закупок, и мошенничество.

Виновниками первого вида корпоративных преступлений, как правило, оказываются менеджеры снабжения, второго – логисты, что и отражается в цифрах опроса.

компаний фиксировали крупный финансовый ущерб

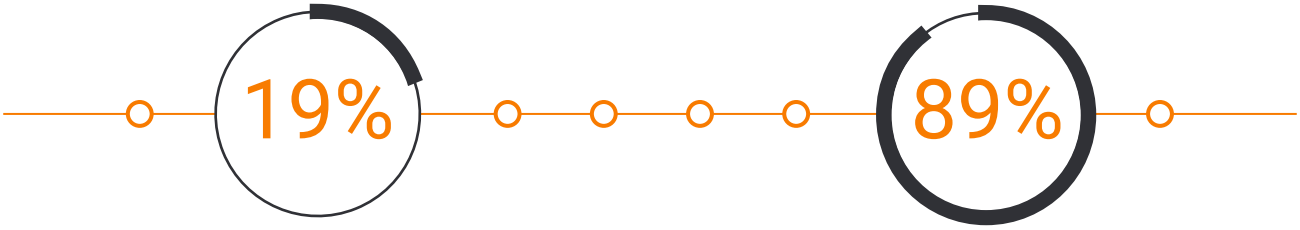
Чаще, чем в других отраслях, в логистике сталкиваются с откатами (41% заявили, что фиксировали попытки или факты в 2019 году) и боковыми схемами (22%).

Риски, связанные с потерей информации, в отрасли тоже высоки. 28% компаний сообщили, что столкнулись с промышленным шпионажем, а 63% – со сливом данных. В более чем 50% случаев утекали данные о клиентах и сделках.

В итоге не было ни одной организации, которую бы обошли инциденты внутренней безопасности. Каждая логистическая компания столкнулась с тем или иным фактом корпоративного мошенничества и утечки. Такой пессимистичной оценки ситуации не встречается больше ни в одной другой отрасли.

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

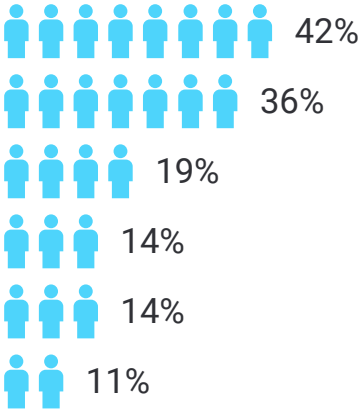
ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:



Руководители

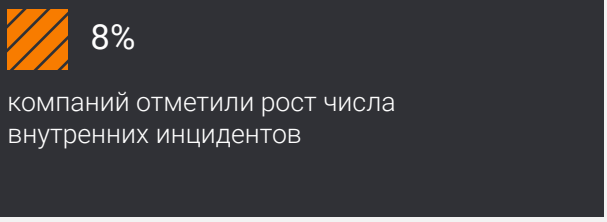
Рядовые сотрудники

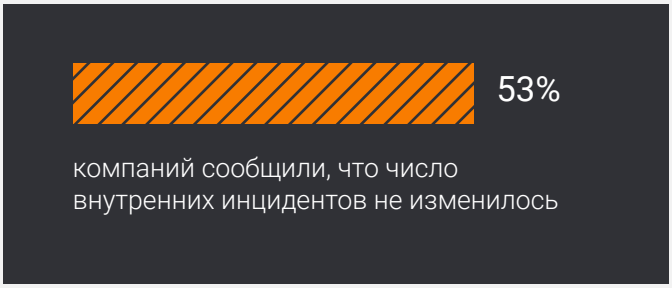
* можно было выбрать несколько вариантов ответов



* можно было выбрать несколько вариантов ответов

ДИНАМИКА





СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

БЮДЖЕТ НА БЕЗОПАСНОСТЬ

25%
компаний заявили о росте бюджета на безопасность

15%
компаний сократили бюджет на безопасность

60%
компаний сообщили об отсутствии динамики в изменении бюджета в 2019 году

* можно было выбрать несколько вариантов ответов

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа	98%	Контроль целостности	18%
Средства администрирования Windows	78%	SIEM-система	10%
NGFW (Firewall и Proxy)	50%	IDS/IPS/EPS	8%
Шифрование (криптошлюз, ПО)	28%	DCAP	0%
DLP-система	23%	Другое	0%

* можно было выбрать несколько вариантов ответов

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

79%
Корпоративная почта

41%
Внешние носители

41%
Документы, отправляемые на печать

38%
Мессенджеры корпоративные

36%
Телефония

36%
ПО для администрирования (TeamViewer и т.п.)

31%
Общедоступная почта

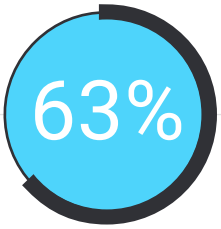
23%
Облачные хранилища

23%
Мессенджеры общедоступные

0%
Другое

* можно было выбрать несколько вариантов ответов

УТЕЧКИ ИНФОРМАЦИИ



логистических компаний
столкнулись со сливом данных

ЧТО УТЕКАЛО?

51%

Информация
о клиентах и сделках

23%

Финансовая
информация

14%

Персональные
данные

9%

Техническая
информация

9%

Другое

* можно было выбрать несколько вариантов ответов

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

51%

опрошенных компаний скрыли инцидент и не делали никаких оповещений

29%

сообщили пострадавшим об инциденте и принесли извинения

16%

сообщили регулятору об инциденте

0%

сделали официальное заявление в СМИ

* можно было выбрать несколько вариантов ответов

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

41%

Попытки откатов

28%

Промышленный шпионаж/ работа в пользу конкурентов

22%

Создание фирмы-боковика

16%

Саботаж

3%

Другое

* можно было выбрать несколько вариантов ответов

УЩЕРБ ОТ ИНЦИДЕНТОВ

38% Мелкий финансовый ущерб

38% Ущерба не было

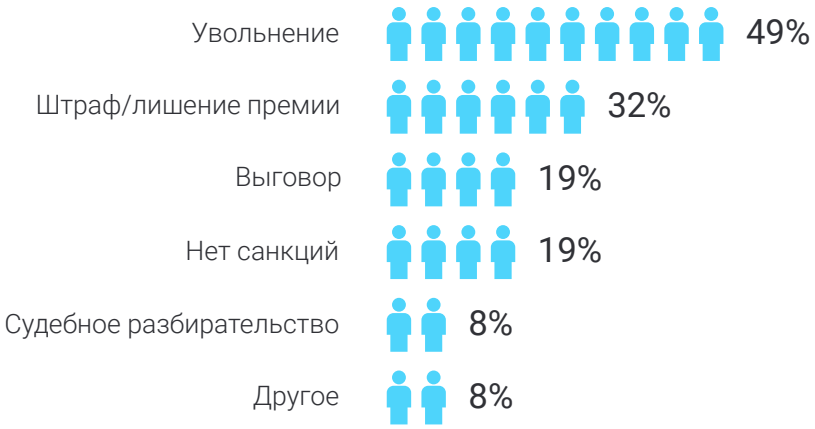
35% Имиджевый ущерб

21% Крупный финансовый ущерб

6% Compliance-риск (угроза или факт наказания от регулятора)

* можно было выбрать несколько вариантов ответов

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО:



Увольнение 49%

Штраф/лишение премии 32%

Выговор 19%

Нет санкций 19%

Судебное разбирательство 8%

Другое 8%

SEARCHINFORM
INFORMATION SECURITY

ЗДРАВООХРАНЕНИЕ

В 2019 году 69% медицинских компаний столкнулись со сливами и утечками информации, это на 10% выше, чем в среднем по другим отраслям. Тревожно, что в 42% случаев это утечки персональных данных.

Медицинская информация относится к особой категории, и на нее действуют более строгие регламенты безопасности. Обеспечить ее сохранность – важная задача, поскольку любые утечки данных имеют последствия.

42%

Утечки персональных данных

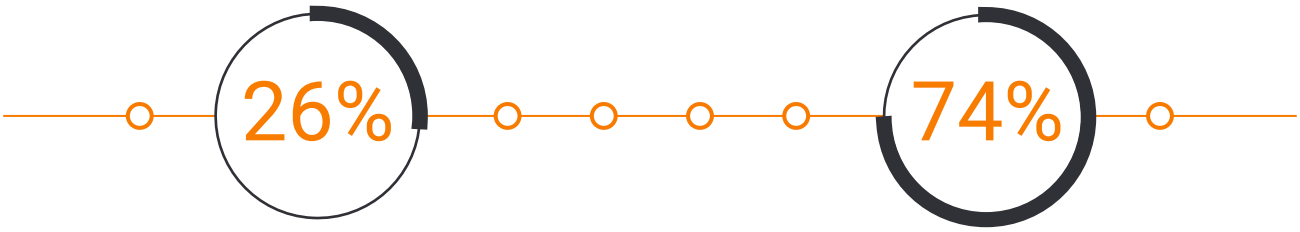
Круг внешних злоумышленников, которым интересны персданные из медицинских компаний, очень широк – от маркетологов до страховых мошенников. Поэтому оповещение о фактах утечек очень важно, тем не менее половина опрошенных сообщают, что скрывают факт инцидента. Таким образом, пациенты остаются в неведении о вероятной атаке мошенников.

64% компаний признает внутренние инциденты опаснее внешних

Число тех, кто считает внешних нарушителей опаснее внутренних, выше, чем по другим отраслям. На это есть объективные причины: больницы и поликлиники – легкая мишень для хакеров и часто оказываются под прицелом. Причем происходит это не из-за плохой технической оснащенности – как видим из цифр, необходимый минимум в компаниях часто обеспечен. Главная проблема – кадровая. Эксплуатируют сложное техническое ПО как правило не ИБ-, а IT-специалисты, а штат их недоукомплектован.

ПРИРОДА И ДИНАМИКА ИНЦИДЕНТОВ

ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:



Руководители

Рядовые сотрудники

* можно было выбрать несколько вариантов ответов

* можно было выбрать несколько вариантов ответов

ДИНАМИКА

14%

компаний отметили рост числа внутренних инцидентов

41%

компаний не смогли ответить на вопрос об изменении числа инцидентов

45%

компаний сообщили, что число внутренних инцидентов не изменилось

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

БЮДЖЕТ НА БЕЗОПАСНОСТЬ

22%
компаний заявили о росте бюджета на безопасность

11%
компаний сократили бюджет на безопасность

67%
компаний сообщили об отсутствии динамики в изменении бюджета в 2019 году

* можно было выбрать несколько вариантов ответов

ИСПОЛЬЗУЕМЫЕ СРЕДСТВА ЗАЩИТЫ:

Антивирусная программа	96%	DLP-система	21%
Средства администрирования Windows	93%	IDS/IPS/EPS	18%
Шифрование (криптошлюз, ПО)	71%	DCAP	4%
NGFW (Firewall и Proxy)	64%	SIEM-система	0%
Контроль целостности	36%	Другое	0%

* можно было выбрать несколько вариантов ответов

ПОД КОНТРОЛЕМ ЧАЩЕ ВСЕГО НАХОДЯТСЯ:

84%
Корпоративная почта

60%
ПО для администрирования (TeamViewer и т.п.)

52%
Внешние носители

52%
Телефония

52%
Документы, отправляемые на печать

32%
Общедоступная почта

24%
Мессенджеры корпоративные

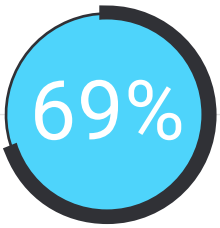
20%
Облачные хранилища

20%
Мессенджеры общедоступные

12%
Другое

* можно было выбрать несколько вариантов ответов

УТЕЧКИ ИНФОРМАЦИИ



компаний столкнулись со сливом данных

ЧТО УТЕКАЛО?

42%

Персональные данные

26%

Техническая информация

16%

Информация о клиентах и сделках

11%

Финансовая информация

16%

Другое

* можно было выбрать несколько вариантов ответов

ПРИ УТЕЧКЕ ИНФОРМАЦИИ

50%

опрошенных компаний скрыли инцидент и не делали никаких оповещений

29%

сообщили пострадавшим об инциденте и принесли извинения

21%

сообщили регулятору об инциденте

0%

сделали официальное заявление в СМИ

* можно было выбрать несколько вариантов ответов

ДРУГИЕ ИНЦИДЕНТЫ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

44%

Попытки откатов

25%

Саботаж

13%

Промышленный шпионаж/ работа в пользу конкурентов

13%

Создание фирмы-боковика

13%

Другое

* можно было выбрать несколько вариантов ответов

УЩЕРБ ОТ ИНЦИДЕНТОВ

53% Ущерба не было

37% Имиджевый ущерб

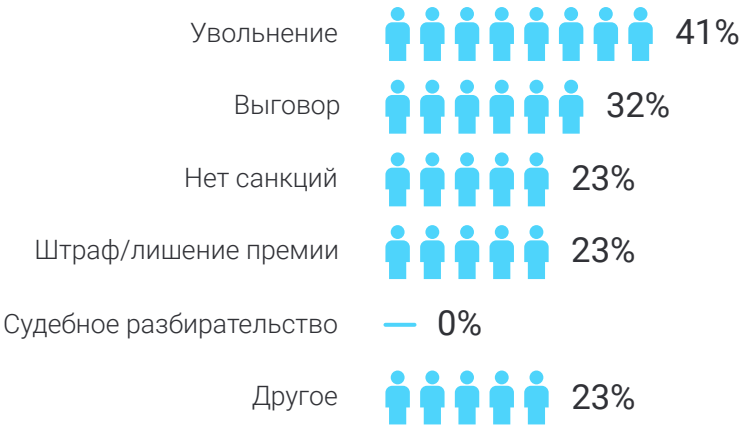
37% Мелкий финансовый ущерб

16% Compliance-риск (угроза или факт наказания от регулятора)

5% Крупный финансовый ущерб

* можно было выбрать несколько вариантов ответов

НАКАЗАНИЯ, ПРИМЕНЯЕМЫЕ К СОТРУДНИКАМ-НАРУШИТЕЛЯМ ЧАЩЕ ВСЕГО:



Увольнение 41%

Выговор 32%

Нет санкций 23%

Штраф/лишение премии 23%

Судебное разбирательство 0%

Другое 23%

SEARCHINFORM
INFORMATION SECURITY

SEARCHINFORM
INFORMATION SECURITY

«СёрчИнформ» – российский разработчик средств информационной безопасности. Компания – резидент Инновационного центра «Сколково», входит в АРПП «Отечественный софт» и НП «Руссофт». Работает во всех федеральных округах России, ее клиенты – 3000 компаний в 17 странах мира. С 2010 года в компании действует собственный учебный центр. Деятельность «СёрчИнформ» лицензирована ФСБ и ФСТЭК. В настоящее время «СёрчИнформ» разрабатывает продукты для комплексного контроля источников угроз:

«СёрчИнформ КИБ»

система класса DLP, защищает от утечек информации, корпоративного мошенничества и других инцидентов безопасности, связанных с человеческим фактором. В 2017 году включена в «магический квадрант» лучших DLP-систем мира по версии Gartner.

«СёрчИнформ SIEM»

система сбора и анализа событий безопасности в режиме реального времени, выявления ИБ-инцидентов и реагирования на них.

«СёрчИнформ FileAuditor»

DCAP-решение (data-centric audit and protection) проводит автоматизированный аудит хранилищ информации, находит нарушения прав доступа и отслеживает изменения в критичных данных.

«СёрчИнформ Database Monitor»

решение класса DAM (database activity monitoring), ведет автоматический мониторинг и аудит операций с базами данных и бизнес-приложениями.

«СёрчИнформ» развивает сервисное направление – услугу аутсорсинга информационной безопасности. Аутсорсинг позволяет решить проблему нехватки ИБ-кадров, минимизировать финансовые и трудозатраты заказчика.

SEARCHINFORM
INFORMATION SECURITY

Больше аналитики и новостей безопасности читайте на сайте компании **searchinform.ru** и в **телеграм-канале.**