



ИНСАЙДЕРСКИЕ УГРОЗЫ '08 В РОССИИ

KEEPING SECRETS SAFE



PERIMETRIX



ОБЩИЕ ВЫВОДЫ	4
ПОРТРЕТ РЕСПОНДЕНТА	5
УГРОЗЫ ИБ	8
ИНСАЙДЕРСКИЕ УГРОЗЫ	9
СРЕДСТВА ЗАЩИТЫ	13
КЛАССИФИКАЦИЯ ДАННЫХ	18
НАПРАВЛЕНИЕ ДВИЖЕНИЯ РЫНКА	21
ЗАКЛЮЧЕНИЕ	22
О КОМПАНИИ PERIMETRIX	23



Уважаемые дамы и господа!

Аналитический центр компании Perimetrix представляет результаты нового исследования в области внутренней информационной безопасности (ИБ) в России. Этой теме неспроста уделено столь пристальное внимание. Как станет ясно дальше, именно внутренние нарушители являются самой опасной угрозой ИБ. Практика показывает, что ущерб от утечек и искажения конфиденциальной информации исчисляется десятками миллионов и даже миллиардами долларов. В то же время потери от вирусов, хакеров и других внешних атак на порядки ниже.

Нашим проектом заинтересовалось множество организаций, от небольших фирм, до государственных ведомств и гигантских по размеру и обороту компаний. В результате, в исследовании приняли участие специалисты 472 учреждений из различных сфер деятельности.

Сотрудники департаментов ИТ и ИБ уже осведомлены о рисках и убытках, которые несут инсайдеры. И специалисты не сидят, сложа руки. Многие организации расширяют возможности своих систем безопасности, устраняя имеющиеся бреши. Мы отмечаем значительный рост оснащенности компаний комплексными решениями по защите от внутренних нарушителей. Такие компании исчисляются уже не единицами процентов как в прошлые годы, а десятками процентов.

Тем не менее, проблем хватает. Устаревшие системы, внедрившиеся в начале века, уже не достаточно эффективно противостоят нарушителям. Потому что изменился сам характер угроз. К примеру, раньше инсайдеры чаще всего использовали сетевые службы (электронную почту, Интернет и пр.), а сейчас просто копируют нужные документы на USB-носители и уносят их в кармане. Помимо этого, участились и случаи халатных утечек. Лояльные работники выносят с работы те же USB-накопители или ноутбуки, а затем теряют технику и всю конфиденциальную информацию вместе с ней. Кроме того, подразделениям ИБ не хватает квалифицированных кадров, особенно для борьбы с внутренними нарушителями. Также имеются определенные трудности с внедрением новых продуктов безопасности в существующие информационные системы.

Мы рассчитываем, что итоги исследования позволят российским организациям еще раз оценить собственные системы ИБ, обратить внимание на современные угрозы и новые методы борьбы с ними. Именно в этом заключается миссия аналитического центра компании Perimetrix.

Евгений Преображенский
Генеральный директор



PERIMETRIX

ОБЩИЕ ВЫВОДЫ

- Внутренние факторы заметно опережают внешние в рейтинге угроз ИБ. Наибольшие опасения специалистов вызывают утечки данных (76%) и халатность сотрудников (67%).
- Внутренние угрозы лидируют вполне закономерно, ведь всего 5% организаций не пострадали от утечек за прошедший год.
- 100% организаций оснащено антивирусным программным обеспечением и межсетевыми экранами, но лишь 24% имеют защиту от утечек, поэтому данные утекают с угрожающей регулярностью.
- Чаще всего инсайдеры крадут из компаний персональные данные (57%), детали конкретных сделок (47%) и финансовые отчеты (38%).
- Широко распространенные мобильные накопители (74%), а также электронная почта (58%) являются самыми популярными каналами утечек.
- В ближайшее время специалисты собираются исправлять критическую ситуацию с внутренней безопасностью. 34% компаний планируют принять на вооружение системы защиты от утечек, а 22% организаций собираются внедрить у себя шифрование данных при хранении.

ПОРТРЕТ РЕСПОНДЕНТА

Компания Perimetrix с 10 января по 10 февраля 2008 года провела опрос сотрудников 472 российских организаций. Респонденты отвечали на вопросы по электронной почте, в телефонных беседах, при

личном интервью в своем офисе, а также заполняли online-анкеты на сайте SecurityLab. Выборка респондентов (см. рис. 1) имеет уклон в сторону крупных и средних компаний.

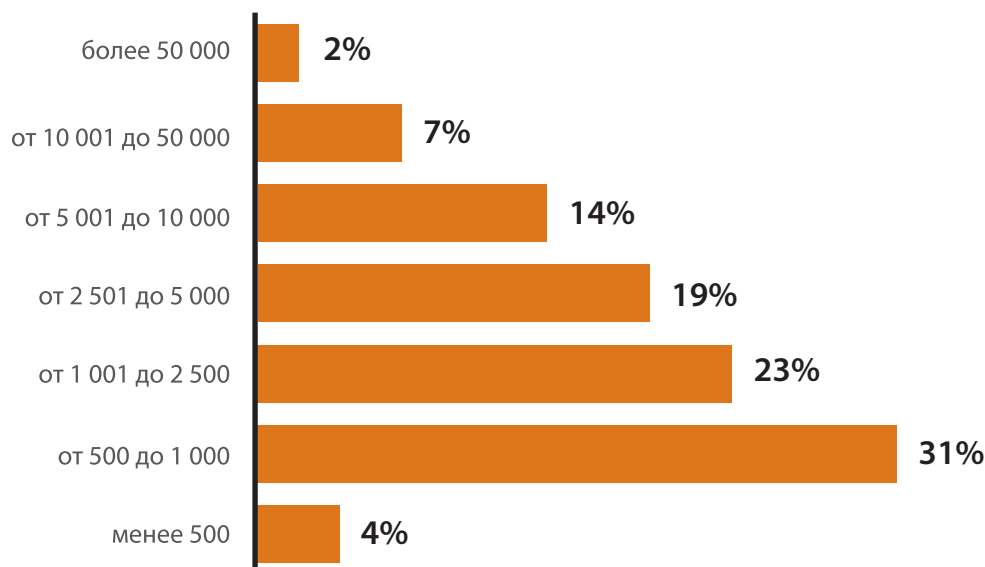


Рис.1 Количество сотрудников

Предприятия малого бизнеса (менее 500 работников) малочисленны и составляют всего 4% респондентов. Чем крупнее организация, тем больший урон наносят утечки. Ведь крупные участники рынка в большей степени страдают от ухудшения репутации, когда становится известно об инциденте. Поэтому и в исследовании преобладают компании среднего (от 500 до 2,5 тыс. работников, 54% участников) и крупного (свыше 2,5 тыс. работников, 42%) бизнеса.

Уровень компьютеризации участвовавших в опросе организаций очень высок. Это видно из ответов респондентов на следующий вопрос (см. рис. 2). Компании до 500 рабочих станций составляют те же 4%, что и участники малого бизнеса. Доля фирм от 500 до 1 тыс. компьютеров значительно больше и равняется 40%. Почти столько же (37%) приходится на организации и учреждения от 1 тыс. до 5 тыс. рабочих станций.

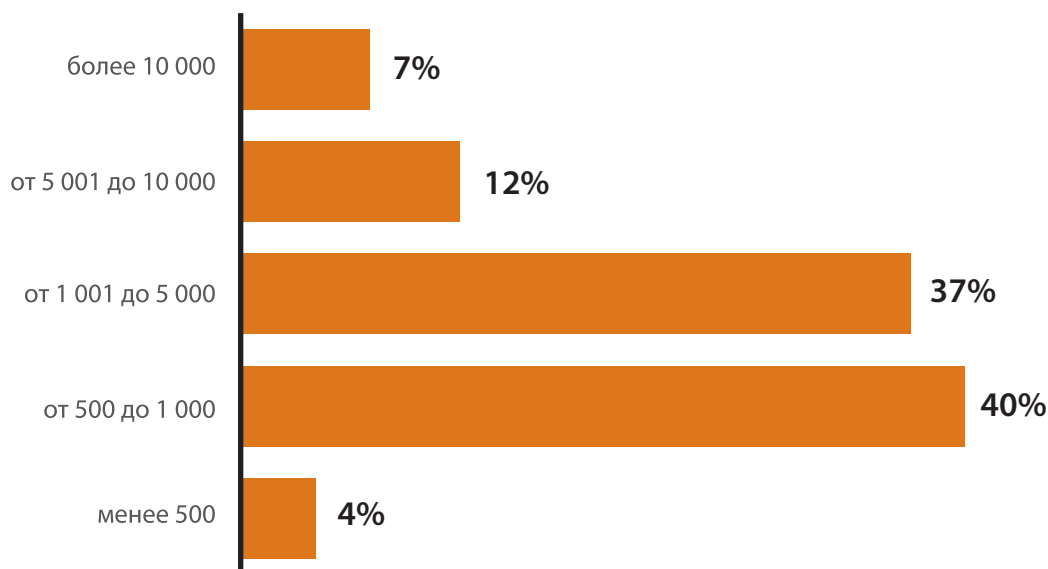


Рис.2 Количество рабочих станций

Что касается сферы деятельности компаний (см. рис. 3), лидерами являются сектор финансовых услуг (26%), ИТ и телекоммуникации (21%), а также ТЭК (19%). Немного меньше (14%) приходится на различные государственные учреждения, министерства и ведомства. Фирмы-производители, предприятия торговли и страховые компании имеют долю от 7% до 4%, всего 2% - образовательные учреждения. 1% фирм не относится ни к одной из перечисленных сфер.

Среди респондентов исследования работники ИТ и ИБ составляют примерно равные группы с преобладанием руководящего состава (см. рис. 4). 53% сотрудников ИТ включают 48% начальников отделов и 5% служащих. В свою очередь 47% работников подразделений ИБ составляют 36% руководителей отделов и 11% специалистов. Таким образом, результаты исследования строятся с учетом мнений людей, которые определяют развитие систем ИБ в организациях.

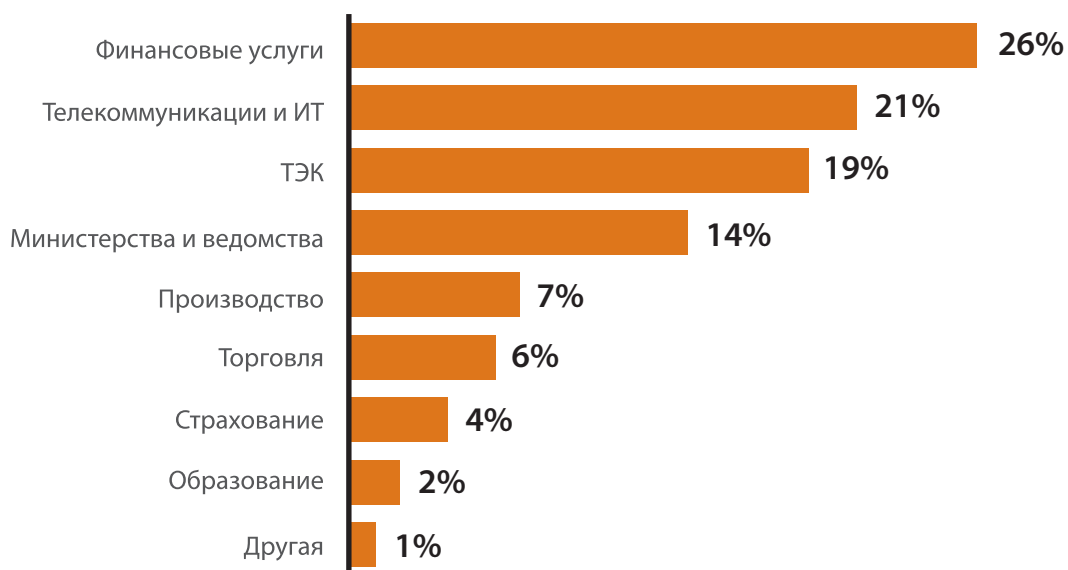


Рис.3 Сфера деятельности

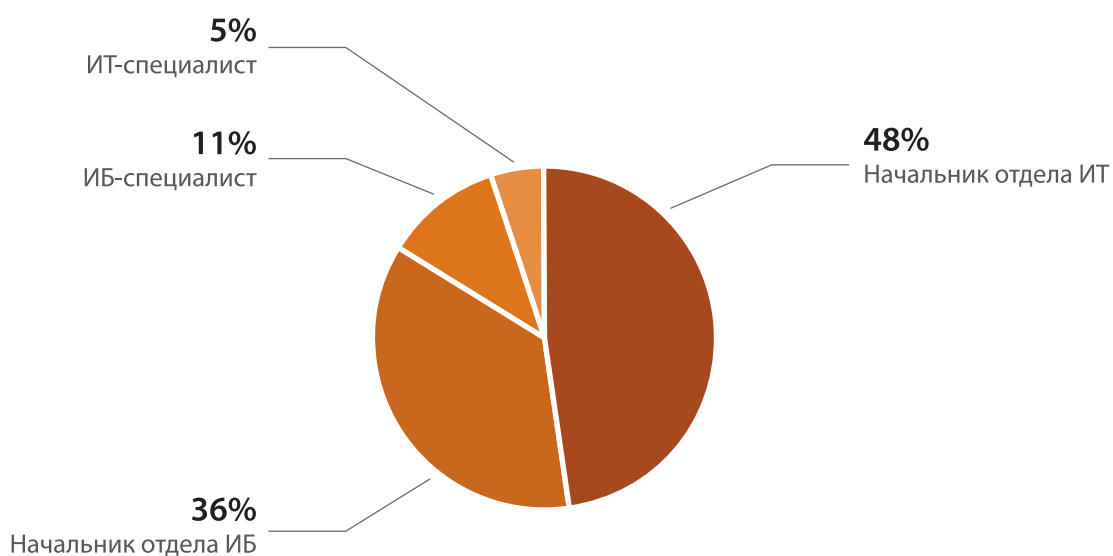


Рис.4 Респонденты по должности



УГРОЗЫ ИБ

Один из основных вопросов, заданных респондентам, касается угроз ИБ. Участники исследования могли выбрать четыре различных фактора риска. Наибольшие опасения специалистов (см. рис. 5) вызывают утечки данных (76%) и халатность пользователей (67%). Оба пункта достаточно тесно связаны.

Ведь большое количество информации утекает не только по злому умыслу работников, но и из-за обычной невнимательности или халатности служащих. Нередко конфиденциальные данные пропадают вместе с забытыми ноутбуками, потерянными USB-накопителями и прочими мобильными носителями.

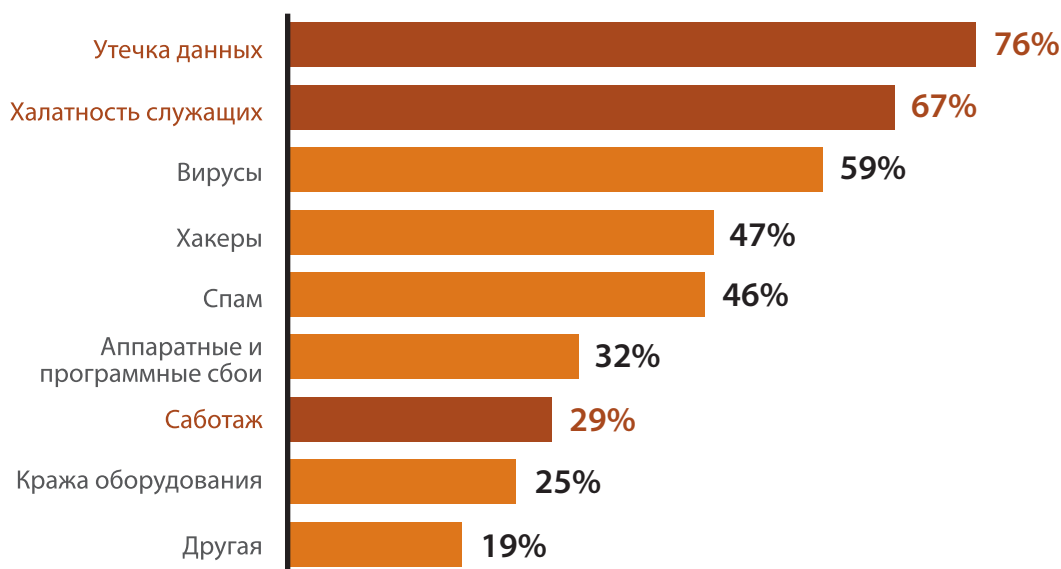


Рис.5 Наиболее опасные угрозы ИБ (возможно выбрать до четырех вариантов)

Следующие угрозы по уровню озабоченности – это вирусы (59%) и хакеры (47%). Как видим, внутренние угрозы значительно опережают внешние. Это вызвано несколькими причинами. Во-первых, средний ущерб от 1 утечки по статистике оказывается заметно выше, чем урон, причиненный атакой извне. Во-вторых, проблемы внешних атак стали актуальными еще в середине девяностых. За прошедшее с тех пор время, компании научились бороться и с хакерами, и с вирусами. Участники исследования подтвердят далее, что сегодня большинство организаций имеют достаточно эффективные барьеры для противодействия внешним угрозам. Инсайдеры же – явление относительно новое, изученное не всеми специалистами ИБ, а потому опасное вдвойне.

Далее в рейтинге угроз ИБ с 46% следует нежелательная корреспонденция, отравляющая жизнь не только компаниям всех рангов, но и обычным пользователям Интернета. Большой процент респондентов (32%), высказавшихся за программные и аппаратные сбои, говорит о том, что требование непрерывности бизнеса является одним из ключевых в современном деловом мире. Остановка операций на долгий срок (а в некоторых областях и несколько часов – целая вечность) может повлечь огромные убытки.

Саботажники получили 29% голосов, а кража оборудования набрала всего 25% процентов. Очевидно, обеспечить физическую безопасность оборудования значительно легче, чем уберечь от кражи нематериальный ресурс – информацию.

ИНСАЙДЕРСКИЕ УГРОЗЫ

Следующий набор вопросов касается внутренних угроз ИБ. На каждый вопрос респонденты могли указать по 2 ответа. Наиболее опасную внутреннюю угрозу (см. рис. 6) представляет опять же утечка данных (корпоративных секретов, интеллектуальной собственности и пр.). Этот фактор выбрала почти половина специалистов (46%). Близкие по смыслу угрозы, искажение документации и утрата информации, набрали соответственно 37% и 31%. Чуть

менее опасны, по мнению ИБ- и ИТ-специалистов, сбои в работе информационных систем (ИС, 26%) и саботаж (22%). 20% в пункте кража оборудования говорит о том, что собственные сотрудники воруют технические устройства значительно меньше, чем информацию. Вынести электронный файл легче и прибыльнее, чем, к примеру, сетевое оборудование. Внутренние угрозы, не перечисленные выше, набрали в сумме 18%.

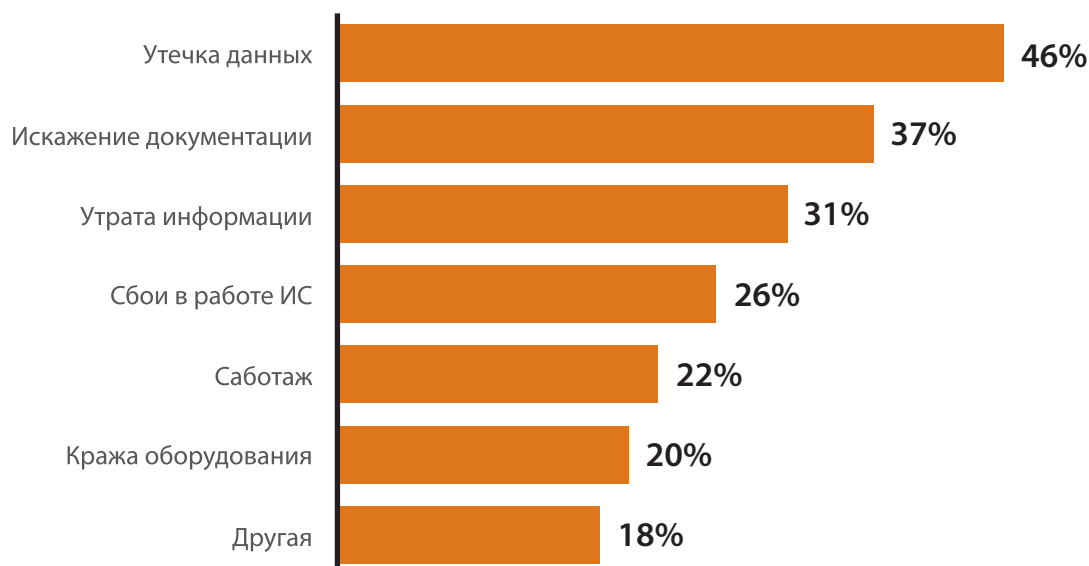


Рис.6 Самые опасные угрозы внутренней ИБ (возможно выбрать до двух вариантов)

Что же чаще всего утекает из организаций? Можно предположить, что интеллектуальная собственность и корпоративные секреты. Оказывается, не совсем так (см. рис. 7). Еще чаще (57%) крадут персональные данные. Это тоже не удивительно. В последние годы известно немало случаев, когда крупные утечки персональных данных клиентов случались в отечественных банках. В скандальных

новостях оказались замешаны даже гиганты кредитной сферы, а также известные игроки на рынке телекоммуникационных услуг. Вслед за персональными данными действительно идут детали конкретных сделок (47%), финансовые отчеты (38%) и интеллектуальная собственность (25%). Бизнес-планы набрали 19%, а прочие информационные ресурсы – 14%.

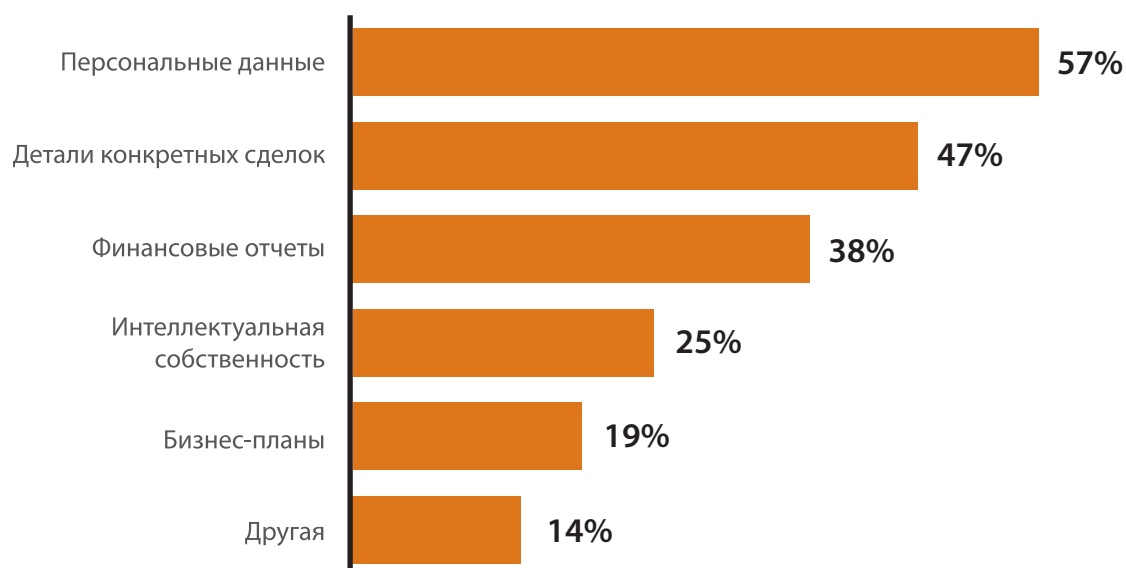


Рис.7 Информация наиболее подверженная утечке (возможно выбрать до двух вариантов)

Мобильные накопители (74%) – безусловный лидер среди других способов украсть информацию (см. рис. 8). Действительно, с развитием данной области, миниатюрные накопители большой емкости на основе флеш-памяти или магнитных пластинах стали буквально общедоступными. За цену менее 100 долларов в компьютерном магазине легко приобрести гаджет, которым еще несколько лет назад мог обладать только Джеймс Бонд. Легкое подключение к компьютеру, большая пропускная способность интерфейса, высокая емкость, размер со спичечный коробок – современные носители обладают всеми необходимыми для инсайдера качествами.

Еще один популярный канал утечек – это электронная почта. Электронная почта (58%) широко распространена, а потому пользуется спросом среди инсайдеров. Доступ к электронной почте имеет практически каждый сотрудник, работающий на компьютере с выходом в Интернет (а иногда и без выхода в Глобальную сеть). Кроме того, пользо-

ваться почтой удобно, а информация доставляется практически мгновенно. В то же время далеко не все фирмы фильтруют почтовый трафик на предмет конфиденциальных данных, а те компании, которые все же используют контентную фильтрацию, страдают от ее низкого уровня эффективности.

Заметно ниже распространенность веб-почты, онлайн-форумов и других Интернет-ресурсов (26%). Это объясняется ограничениями на доступ в Сеть, которые имеются в большинстве организаций. Даже если руководители компаний не беспокоятся об утечках, немногие позволяют сотрудникам свободную навигацию в Интернете. Только для того, чтобы работники не проводили время в непрофильных конференциях и на развлекательных сайтах. Аналогичная ситуация с интернет-пейджерами (17%). Примерно столько же (18%) взяли печатающие устройства. Фото-принадлежности набрали всего 2%. Конечно, ведь инсайдерам не слишком удобно работать с фотоаппаратами.



Рис.8 Самые популярные каналы утечки (возможно выбрать до двух вариантов)

В вопросе о количестве утечек в организациях за год, среди респондентов единства не было (см. рис. 9). 26% специалистов затрудняются сказать, сколько внутренних инцидентов произошло в их компаниях. Тем не менее, 3/4 респондентов сумели определиться с количеством утечек. Наибольший процент (43%) набрал вариант ответа от 1 до 5 инцидентов. И хотя утечки можно сосчитать по пальцам, даже

3-4 кражи данных это действительно много. Ведь всего один инцидент приносит огромный ущерб. Так же многочисленной (19%) получилась группа компаний, допустивших от 6 до 25 утечек в 2007 году. Отметим, что более 25 утечек допустили 7% компаний. Ни одного инцидента не зарегистрировали лишь 5% фирм.

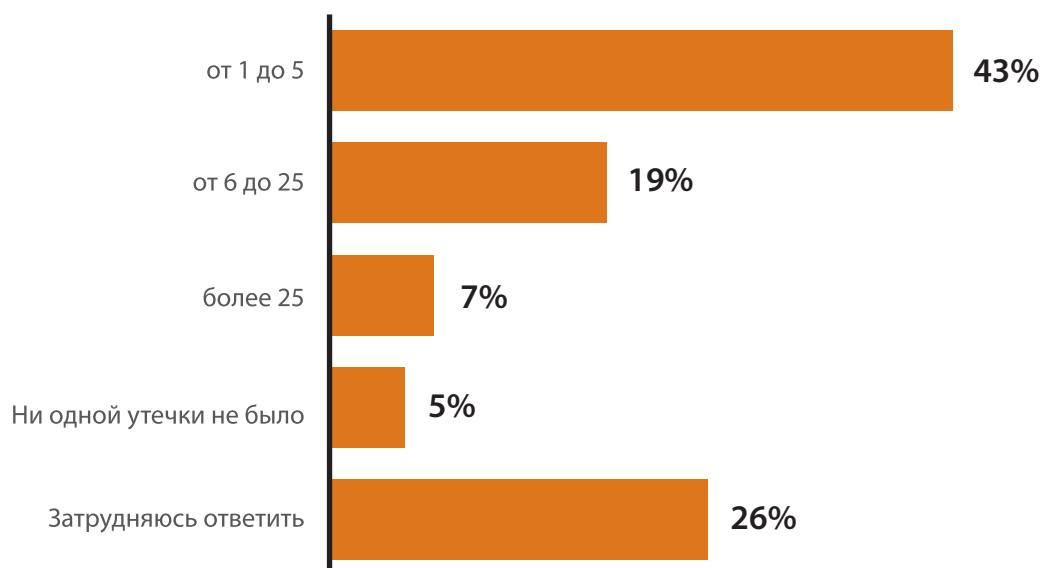


Рис.9 Количество утечек в 2007 году

СРЕДСТВА ЗАЩИТЫ

Отвечая на вопрос о наиболее опасных угрозах ИБ, респонденты данного исследования поставили на первое место утечки и халатность служащих. При этом атаки хакеров и вирусная активность заметно отстали. Анализируя ответы на вопрос о средствах ИБ (см. рис. 10), можно найти следующее объяснение сложившейся ситуации. Все опрошенные организации используют антивирусы и межсетевые экраны. Значит, в большей или меньшей степени все защищены и от вирусов, и от хакеров. Отличия заключаются лишь в реализации программных средств. Кроме того, 98% компаний применяют

контроль доступа, 74% - системы обнаружения/предотвращения вторжений (IDS/IPS) и 53% - VPN-соединения. Данные меры также снижают шансы хакеров и вредоносного кода на успех. Получается, от внешних угроз защищают сразу несколько различных технологий. И в то же время организации оказываются беззащитными перед столь актуальными внутренними угрозами. Ведь только 36% компаний шифрует данные при хранении, а системами защиты от утечек оснащены и того меньше, 24% фирм. Впору говорить о халатности работников подразделений ИБ!

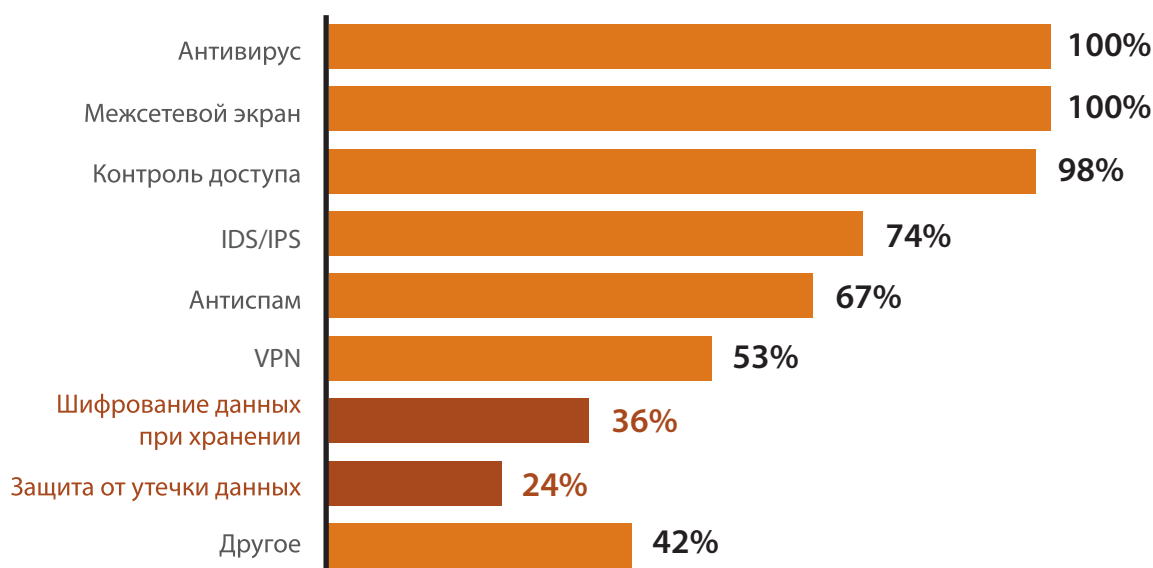


Рис.10 Самые популярные средства ИБ (возможно выбрать неограниченное число вариантов)

Интересно было узнать, какие же средства (см. рис. 11) используют те 24% компаний, которые позаботились о защите от внутренних нарушителей, и как они сами оценивают эффективность принятых мер (см. рис. 12). Естественно, база респондентов сокра-

тилась примерно в 4 раза и составила 113 организаций. Эффективность используемых средств защиты специалисты оценивали по 3-уровневой шкале (низкие результаты, средние или высокие).

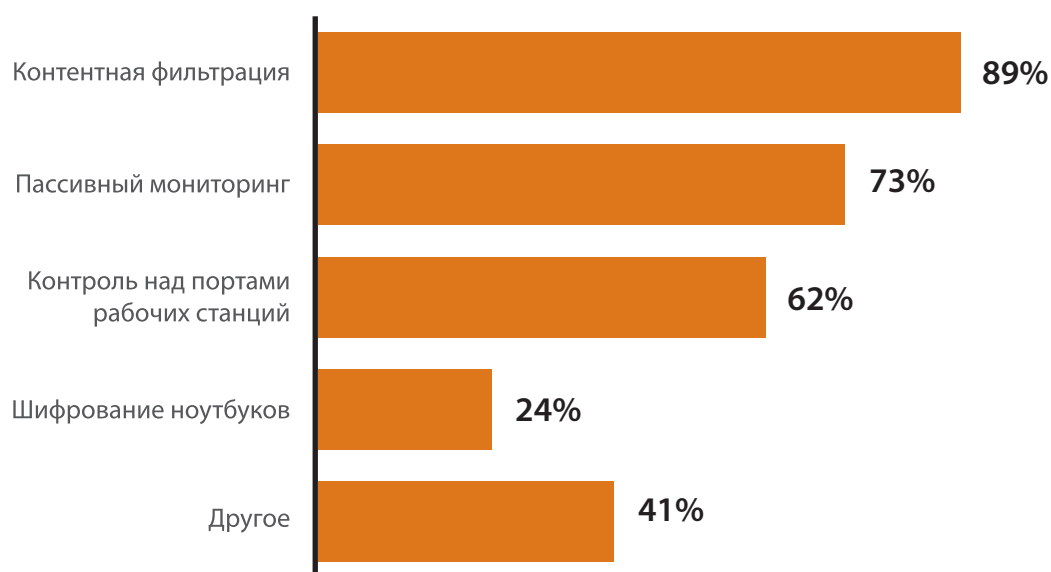


Рис.11 Самые популярные средства защиты от утечек (возможно выбрать неограниченное число вариантов)

Самым популярным (89%), при этом и самым неэффективным средством стала контентная фильтрация. Действительно, один из самых старых методов достаточно легко реализовать. Но никуда не деться

и от недостатков. Машина элементарно не сможет распознать не только зашифрованный текст, но и написанный на смеси русских, латинских букв и специальных символов.

Но и это не самая главная проблема. В целом, эффективность систем контентной фильтрации составляет не более 80%. Это означает, что в 20% случаев утечка произойдет незамеченной. А, кроме того, каждое пятое предупреждение об инциденте будет ложным.

Далее, система контентной фильтрации, установленная на каком-либо шлюзе будет сканировать лишь проходящий трафик. Данные же на рабочей станции остаются беззащитными. Достаточно воткнуть USB-носитель и скачать все нужные документы. Ну и, наконец, контентная фильтрация никак не поможет сохранить конфиденциальные сведения, которые остались на потерянном ноутбуке или резервном носителе. А такие происшествия случаются сплошь и рядом.

Пассивный мониторинг (73%) и контроль над портами рабочих станций (62%) также распространены, а их эффективность респонденты оценивают на среднем уровне. Впрочем, именно мобильные носители, прежде всего USB-устройства, являются любимыми инструментами инсайдеров. Поэтому и контроль над портами компьютеров можно признать недостаточно используемым. Единственное средство, которое специалисты назвали высокоэффективным – шифрование ноутбуков, распространено слабо, всего в 24% компаний текущей выборки. Другими словами, примерно в 6% организаций, принявших участие в исследовании.

Необходимо отметить, что участники исследования не были ограничены в количестве ответов на вопросы о мерах защиты, т.е. были перечислены все имеющиеся в компаниях средства.

ВЫСОКАЯ	Шифрование ноутбуков
СРЕДНЯЯ	Контроль над портами рабочих станций Пассивный мониторинг
НИЗКАЯ	Контентная фильтрация

Рис.12 Эффективность используемых средств защиты от утечки

Почему же уровень использования средств защиты от утечек столь низок? Специалисты называют множество причин (см. рис. 13). Самый популярный

ответ - неэффективность предлагаемых технологий (49%). Далее идут «традиционные» бюджетные ограничения (26%) и трудности с внедрением (11%).

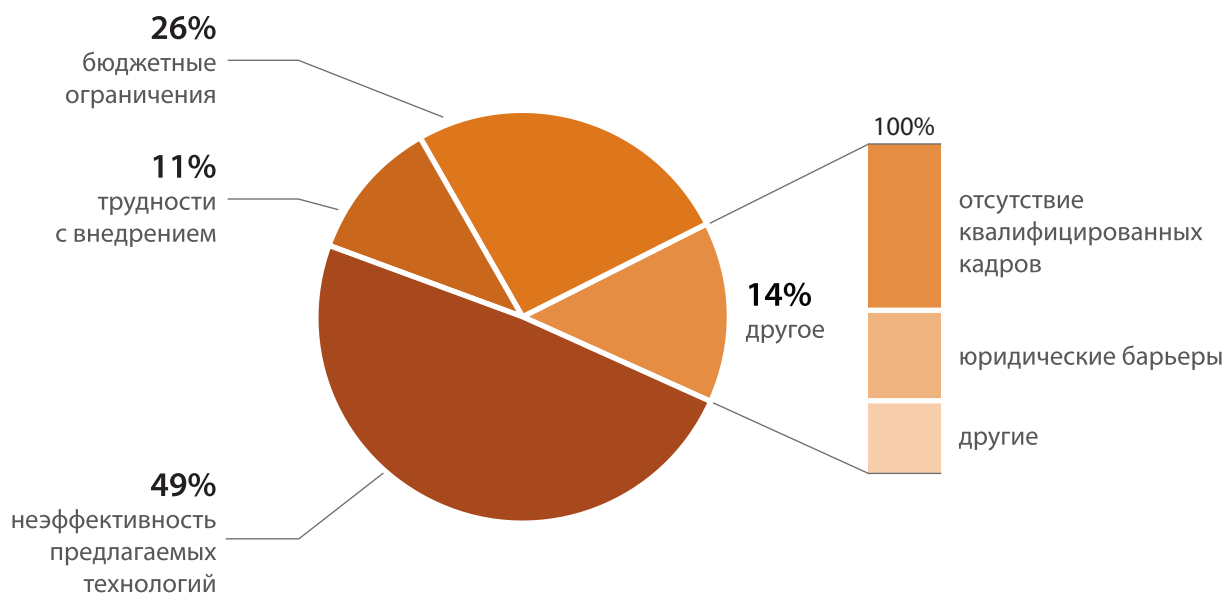


Рис.13 Препятствия на пути внедрения защиты от утечки данных

Однако вернемся к вопросам эффективности используемых средств защиты. Шифрование ноутбуков было признано эффективной мерой. Но тогда не понятно, почему криптографию используют так редко (лишь 24% респондентов)? Вряд ли это бюджетные ограничения, поскольку программы для шифрования содержимого жестких дисков не так уж и дороги, и достаточно широко представлены на рынке. Трудности внедрения также не должны пугать, ведь установить программу шифрования

после настройки операционной системы займет минимум времени ИТ-сотрудника даже невысокой квалификации. Вариант отсутствия квалифицированных кадров тоже назывался респондентами и набрал 7%. Еще меньше (4%) получили юридические барьеры. Вероятно, специалисты опасаются, что защита от утечек потребует вмешательства в личную жизнь работников, ведь контролироваться будет вся деятельность сотрудников, в том числе и частная переписка.

Представляется, что почти половина респондентов, упомянувшая неэффективность, говорила об устаревших технологиях – контентной фильтрации или электронных метках. Действительно, методы лингвистического анализа уже не отвечают современным требованиям. Ведь с появлением карманных накопителей утечки непосредственно с рабочей станции обогнали сетевые угрозы. А электронные метки в чистом виде не предоставляют никакой гибкости. Все возможные действия системы заранее предопределены. В результате ухудшается производительность труда служащих, разрастается бюрократия, нарушается баланс между бизнесом и безопасностью.

Тем не менее, сегодня существуют и более прогрессивные технологии. Например, концепция Secret Documents Lifecycle™ (SDL) подразумевает объединение лучших черт разработанных ранее методик. Электронные метки используются для защиты уже классифицированных файлов, а контентная фильтрация для входящих или новых документов. Кроме того, вся информация хранится не в открытом, а в зашифрованном виде в специальном хранилище. Таким образом, SDL предлагает исключительно высокую эффективность: 100% при защите классифицированных данных.

КЛАССИФИКАЦИЯ ДАННЫХ

Ряд вопросов, адресованных специалистам, касается классификации данных. Классификация – одна из ключевых технологий на пути создания эффективной защиты от утечек. И 42% опрошенных утверждают, что данная методика очень помогает в деле за-

щиты конфиденциальной информации (см. рис. 14). 35% думают, что скорее помогает. Таким образом, 77% экспертов положительно оценивают классификацию. Негативно настроено всего 23%, из которых лишь 4% считают, что технология бесполезна.

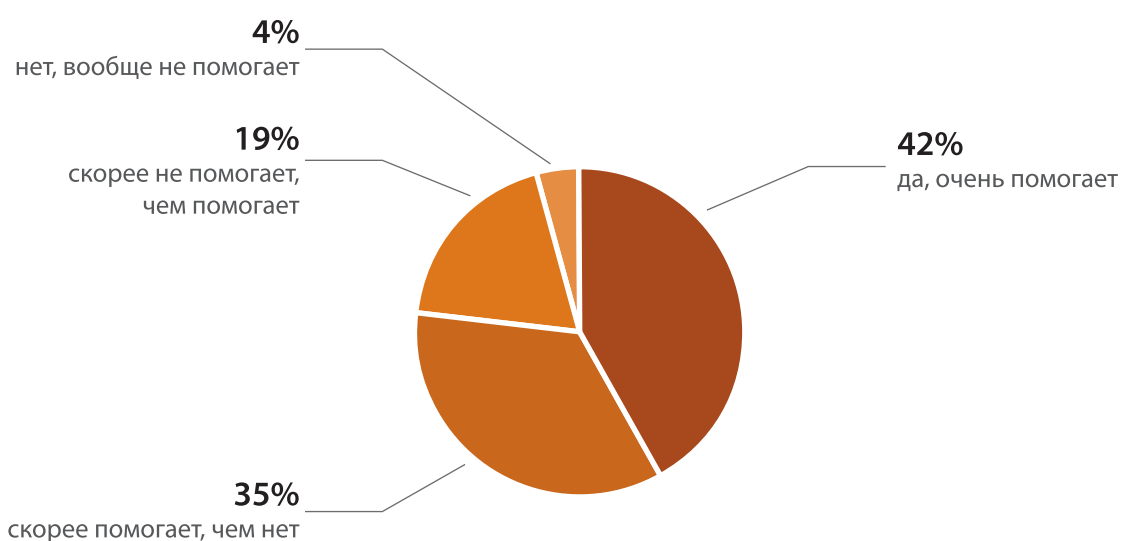


Рис.16 Помогает ли проведение классификации поднять эффективность защиты от утечки данных

Тем не менее, использовать классификацию непросто (см. рис. 15). Основных сложностей три. Большинство респондентов (52%) говорит о том, что актуальность классификации сложно поддерживать

по прошествии некоторого времени. 23% считают трудным сам процесс классификации. Еще 19% испытывают сомнения из-за высокой стоимости классификации.

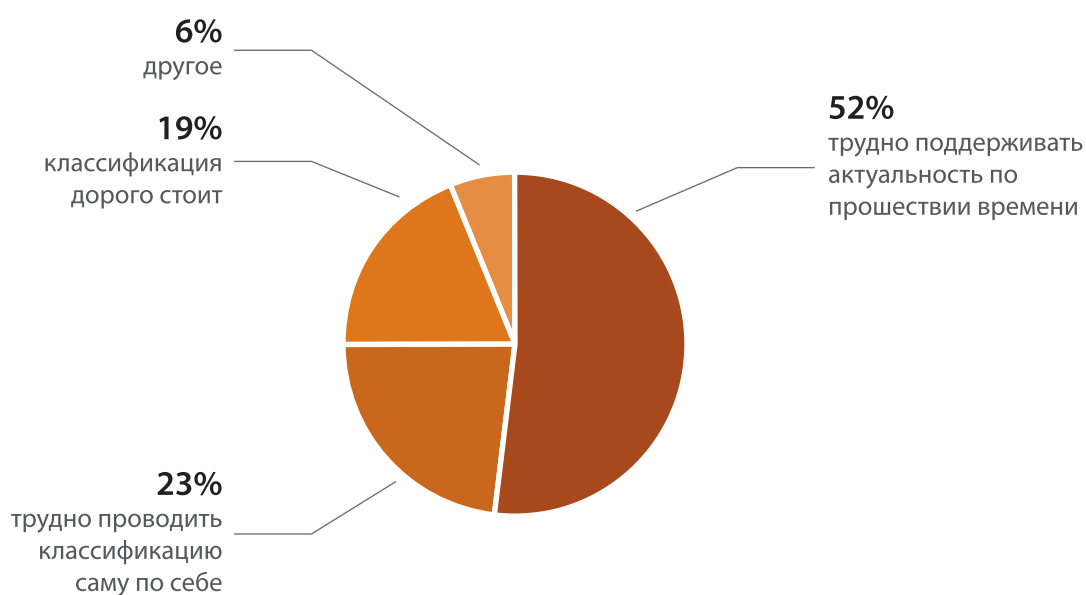


Рис.15 Причина непопулярности классификации данных

Помимо перечисленных на рис. 15, есть еще одна причина, почему классификация остается несколько недооцененной в подразделениях ИБ. Технология очень требовательна к актуальности данных. Классификация требует регулярного обновления

сведений о степени секретности документов. Однако на практике собственно разделение по классам производится достаточно редко, что подтверждают ответы респондентов (см. рис. 16).

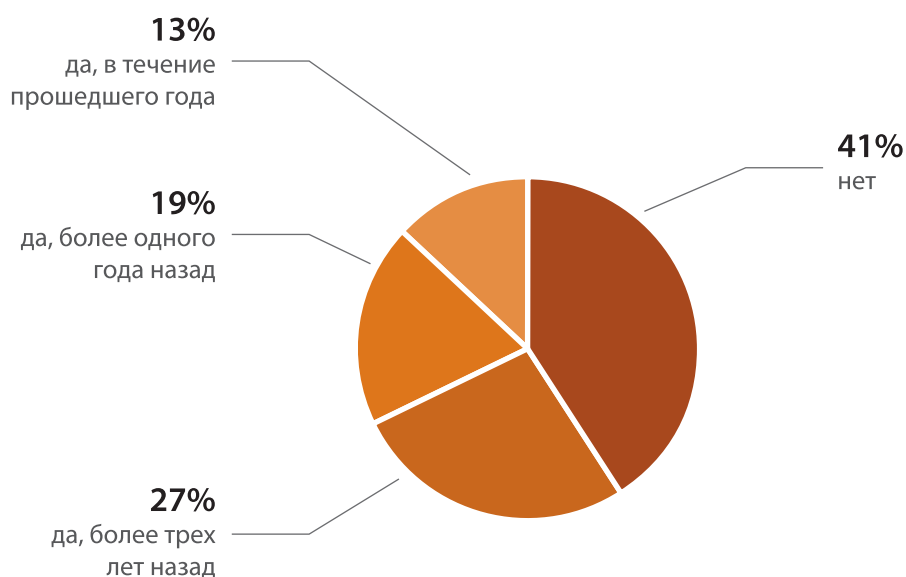


Рис.16 Проводилась ли классификация данных

41% организаций не проводил классификацию вообще. 27% компаний классифицировали данные более 3 лет назад, 19% - более года назад. И лишь 13% фирм проводили классификацию в течение

последнего года. Только в 1 компании из 8 данные классифицированы более или менее точно. Об актуальности сведений годовой и более давности не приходится и говорить.

НАПРАВЛЕНИЕ ДВИЖЕНИЯ РЫНКА

Если проанализировать ответы специалистов, принявших участие в исследовании, станет ясно, ситуация в сфере ИБ неудовлетворительная. Особенно в части утечек данных. Тем не менее, респонденты решительно настроены укреплять электронную безопасность, но каждый по-своему. Ответы на последний вопрос (см. рис. 17) нагляд-

но демонстрируют, в каком направлении организации собираются развивать отрасль ИБ в ближайшее время. Сотрудники отделов ИТ и ИБ могли бы перечислить многие мероприятия. Поэтому, чтобы выявить наиболее важные направления, количество вариантов ответа было ограничено всего одним.

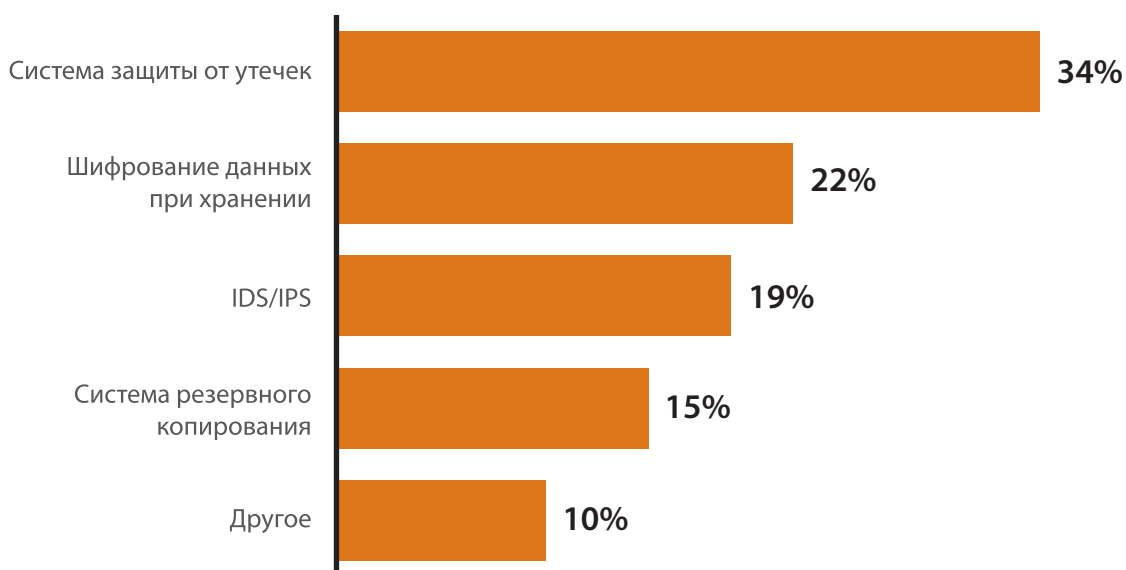


Рис.17 Планы по наращиванию системы ИБ в ближайшие 3 года

Нет ничего удивительного, что большая часть специалистов (34%) рассчитывает укрепить защиту от утечек. Это просто необходимо, ведь инсайдеры представляют наиболее опасную угрозу. На втором месте с 22% идет шифрование данных – тоже весь-

ма эффективное мероприятие от потери информации. Чуть меньше (19%) набрали комплексные инструменты ИБ - IDS/IPS. В 15% компаний планируют улучшить системы резервного копирования. А 10% респондентов назвали другие компоненты.

ЗАКЛЮЧЕНИЕ

Исследование показало, что ситуация с внутренней безопасностью в российских компаниях и учреждениях близка к критической. Лишь считанные проценты организаций избежали утечек в прошедшем году. Свыше четверти фирм зарегистрировали 6 и более внутренних инцидентов. А между тем, даже одна утечка может принести многомиллионные убытки. Согласно подсчетам аналитического центра Perimetrix, финансовый ущерб от потери персональных данных всего 1 человека обходится примерно в 200 долларов. А крупные компании теряют базы данных клиентов по несколько миллионов записей. Тогда счет убытками идет уже на миллиарды. Неудивительно, что специалисты и руководители отделов ИТ и ИБ называют утечки самой большой (76%) угрозой электронной безопасности.

Причина такого положения дел заключается в том, что лишь немногие организации (24%) используют системы защиты от утечек. А те, что используют, применяют, в основном, устаревшие малоэффективные комплексы, которые основываются на методах контентной фильтрации. Недооцененными остаются

такие технологии как шифрование хранимых данных и классификация. Шифрование является эффективным, недорогим и доступным средством для предупреждения утечек. Классификация значительно сложнее, но без нее не построить качественной системы безопасности. Кроме того, классификация требует усилий по поддержанию своей актуальности. Ведь если классифицирование проводится достаточно редко, то эффективность использующих ее технологий значительно снижается.

Следует отметить положительную тенденцию. Организации знают о существующих брешах в системах безопасности и намерены решительно с ними бороться. Уже в ближайшее время около трети компаний (34%) планируют внедрить у себя прогрессивные комплексы защиты от утечек. Примерно четверть компаний (22%) также собирается использовать шифрование данных. Эти меры вкпе с уже используемыми компонентами систем ИБ должны вывести безопасность на новый уровень и обеспечить всестороннюю защиту конфиденциальных данных, как от внешних нарушителей, так и от внутренних.

О КОМПАНИИ PERIMETRIX

Компания Perimetrix разрабатывает системы защиты корпоративных секретов третьего поколения. Благодаря реализации революционной концепции Secret Documents Lifecycle™ наши решения обеспечивают гарантированную 100% защиту секретных документов, полный контроль над каналами коммуникаций и полноценный аудит электронных операций.

В отличие от конкурентов Perimetrix концентрирует весь свой потенциал, инновационный подход и уникальный опыт на решении важнейшей задачи заказчиков – сохранении корпоративных секретов для повышения конкурентоспособности, установления плодотворных отношений с инвесторами и партнерами, соответствия государственным требованиям.

Компания основана в 2007 году инновационной командой профессионалов, стоявших у истоков создания современных систем защиты от внутренних IT-угроз. Perimetrix входит в группу компаний «КомпьюЛинк» – лидирующий альянс на российском рынке информационных технологий. Устойчивое финансовое положение группы, ее уникальный опыт и знания, внушительная база заказчиков служат надежным фундаментом развития Perimetrix. Благодаря мощной поддержке «КомпьюЛинка» компания имеет возможность выполнять комплексные проекты по внутренней IT-безопасности, выйти в лидеры российского рынка и создать основу для международной экспансии.



Штаб-квартира Perimetrix

Российская федерация,
119607, Москва,
Мичуринский проспект, д. 45

Телефон: +7 495 737 99 91
Факс: +7 495 737 99 92

info@perimetrix.com
www.perimetrix.com

KEEPING SECRETS SAFE

