

# СКОЛЬКО СТОИТ БЕЗОПАСНОСТЬ

АНАЛИЗ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИБ  
В РОССИЙСКИХ КОМПАНИЯХ

2017



Рынок информационной безопасности в России показывает постоянный рост: мы видим, что год от года увеличиваются бюджеты на ИБ, создаются новые подразделения, нацеленные на обеспечение кибербезопасности, видим, как в их арсенале появляются новейшие технологии, строятся центры мониторинга и реагирования на инциденты информационной безопасности (security operations centers). И при всем этом общее число инцидентов, происходящих в мире (и в России в частности), также год от года растет: они приобретают все большую массовость и все чаще оборачиваются крупномасштабными эпидемиями, ущерб от которых также становится все ощутимее (от нарушения работы отдельных сервисов до полной остановки бизнес-процессов со всеми вытекающими последствиями).

Получается, что, с одной стороны, «пациент» — среднестатистическая организация — все больше сил и средств вкладывает в «лечение» (свою информационную безопасность), а с другой — лучше ему, мягко говоря, не становится. В чем дело? Конечно же, нам как компании, активно исследующей актуальные угрозы и новые векторы атак, причины происходящего весьма интересны.

Поставить точный диагноз и назначить пациенту правильное лечение — без обследования невозможно. Именно этой идеей мы и руководствовались в подготовке данного отчета: это своего рода анамнез отечественного бизнеса с описанием основных точек приложения усилий в сфере ИБ, их анализом и, конечно же, с общими рекомендациями в итоге.

С уважением, Максим Филиппов,  
директор по развитию бизнеса Positive Technologies в России

## СОДЕРЖАНИЕ

Портрет участников.....	6
Бюджетирование.....	8
Риски.....	11
Финансовые потери от киберинцидентов.....	13
Реагирование на инциденты.....	19
Финансовые затраты на защиту.....	24
Компоненты защиты.....	31
Заключение.....	35
Источники.....	36

Мировая экономика переходит в цифровую плоскость. И пока компании перестраивают и автоматизируют бизнес-процессы, а ресурсы выводят в интернет, преступники также перемещают свою деятельность в киберпространство. Для того чтобы украсть кошелек, ограбить банк или начать войну, хакерам не нужно выходить из дома. При этом одна масштабная вредоносная кампания способна нанести ущерб, сопоставимый с доходами небольшого государства. Ярким примером может служить эпидемия WannaCry, от которой пострадали тысячи организаций по всему миру, а суммарный ущерб составил более миллиарда долларов.

В этом исследовании мы рассмотрим основные статьи расходов на обеспечение информационной безопасности и расскажем, на что нужно обратить внимание при планировании бюджета, проанализируем, способны ли компании самостоятельно оценить возможный ущерб заранее — или только после того, как сами станут жертвой хакерской атаки.

Разумное распределение ресурсов позволит не только соответствовать требованиям регуляторов, но и уверенно противостоять киберпреступникам.



## ПОРТРЕТ УЧАСТНИКОВ

В качестве респондентов выступили представители 170 российских компаний — руководители IT- и ИБ-подразделений, директора. Организации, принявшие участие в исследовании, различны по сфере экономики, числу сотрудников, количеству офисов, однако большинство из них входят в рейтинг 500 крупнейших компаний России по выручке за 2016 год или лидируют в своей отрасли.

Количество сотрудников  
в компании



Количество и территориальная  
распределенность офисов

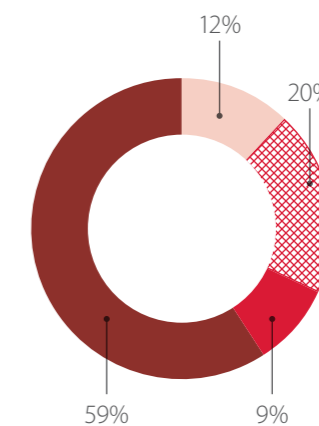
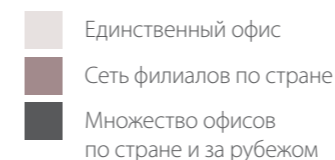


Рисунок 1. Распределение компаний-респондентов по количеству сотрудников

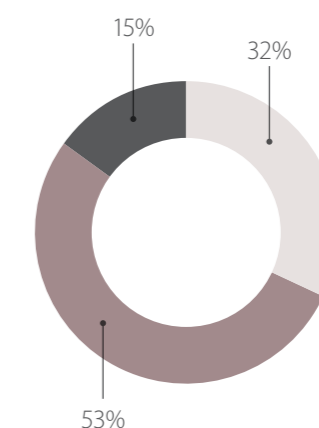


Рисунок 2. Распределение компаний-респондентов по географии офисов

## 68% компаний

обладают распределенной инфраструктурой, насчитывают множество филиалов по стране, некоторые также имеют представительства в других странах

## > 1000 сотрудников

в большинстве компаний-респондентов

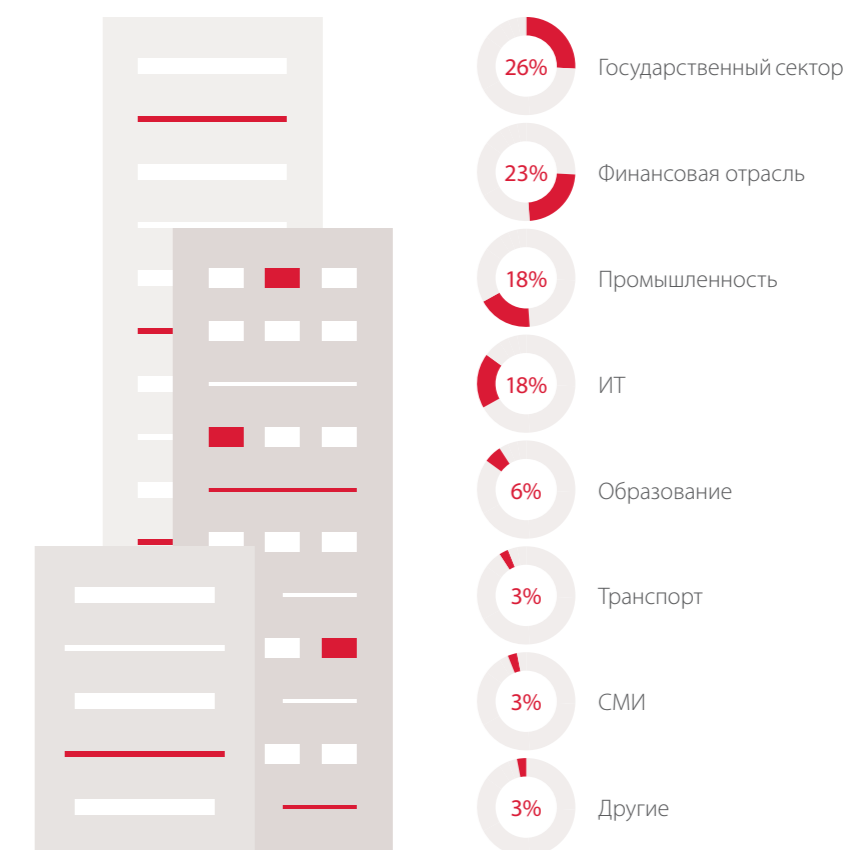



Рисунок 3. Распределение компаний-респондентов по сферам экономики





## БЮДЖЕТИРОВАНИЕ


Распределение ресурсов в условиях ограниченности бюджета осуществляется в соответствии с приоритетами компании. В части обеспечения информационной безопасности приоритеты должны расставляться в соответствии с результатом оценки рисков, присущих конкретной организации. В рамках этой публикации мы не будем углубляться в теорию оценки и обработки рисков ИБ, однако рассмотрим в деталях, как различается бюджет, выделяемый на ИБ в разных компаниях, а также на что он расходуется.


Далее по тексту используются следующие обозначения


- 


Финансовая отрасль  
(все респонденты)
- 


Образование
- 


Топ-10 финансовых организаций  
с наибольшим бюджетом на ИБ
- 


Промышленность
- 


Финансовые организации,  
не вошедшие в топ-10
- 

Транспорт
- 

Государственные организации  
(все респонденты)
- 

ИТ
- 

Топ-5 государственных организаций  
с наибольшим бюджетом на ИБ
- 

СМИ
- 

Государственные организации,  
не вошедшие в топ-5

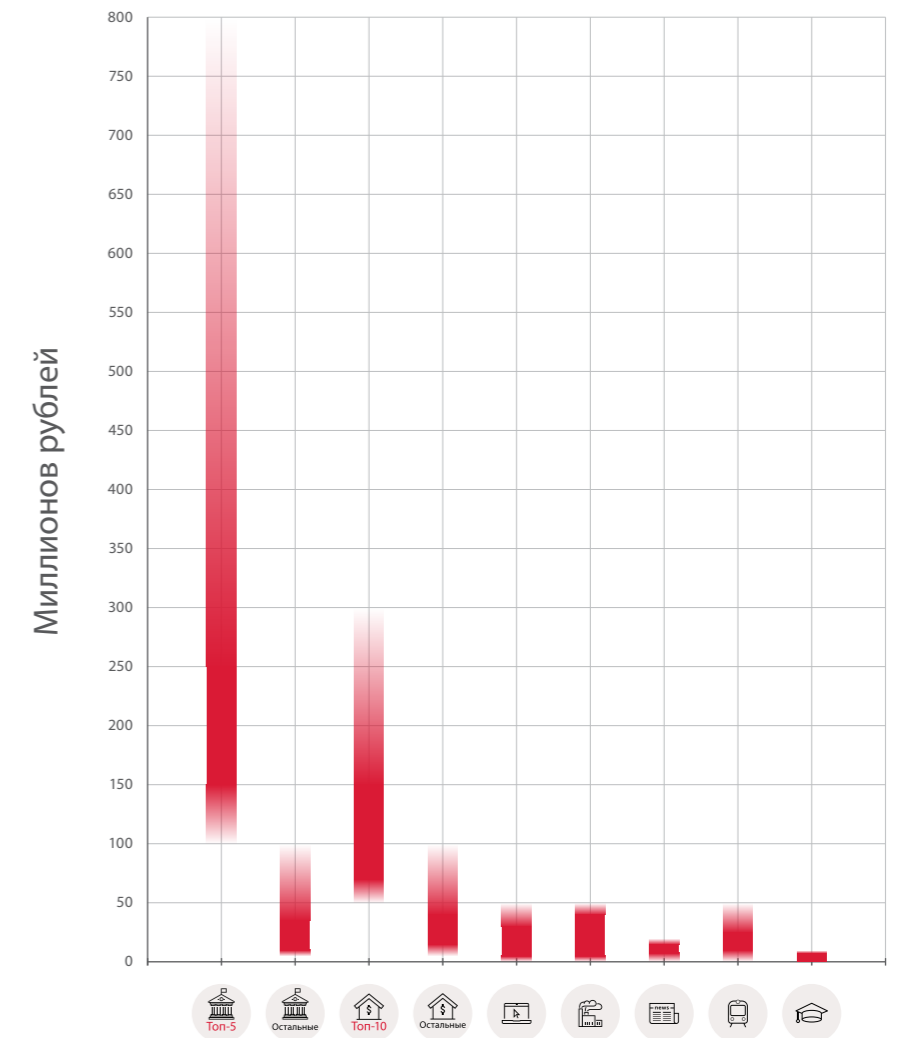


Рисунок 4. Бюджет, выделяемый ежегодно на ИБ в разных отраслях

### Компании тратят бюджет ИБ

в первую очередь на приведение инфраструктуры в соответствие требованиям регуляторов в части защиты информации

Некоторые банки и государственные организации существенно выделяются на фоне остальных компаний по объему бюджета на обеспечение ИБ. Поэтому в отдельные категории мы выделили 5 госорганизаций и 10 банков, бюджеты которых оказались крупнее бюджетов других компаний соответствующих отраслей в десятки и сотни раз.

Анализ показал, что некоторые госкомпании не скупятся, их бюджет, выделяемый на обеспечение ИБ, порой достигает 800 миллионов рублей в год, в то время как, например, образовательные учреждения ограничены совсем небольшими суммами, порой не превышающими и одного миллиона рублей. Это в первую очередь связано с общими бюджетами компаний, которые в крупных государственных учреждениях в разы больше, чем в других организациях. Более того, подразделение, отвечающее непосредственно за информационную безопасность, существует лишь в 44% компаний-респондентов, в остальных организациях необходимые функции выполняются специалистами IT-отдела. Из-за высокой сложности контроля и управления многочисленными техническими ресурсами в крупных распределенных инфраструктурах компаниям приходится внедрять специализированные средства, что также увеличивает затраты на ИБ.

Бюджет, выделяемый на ИБ  
(в рублях)

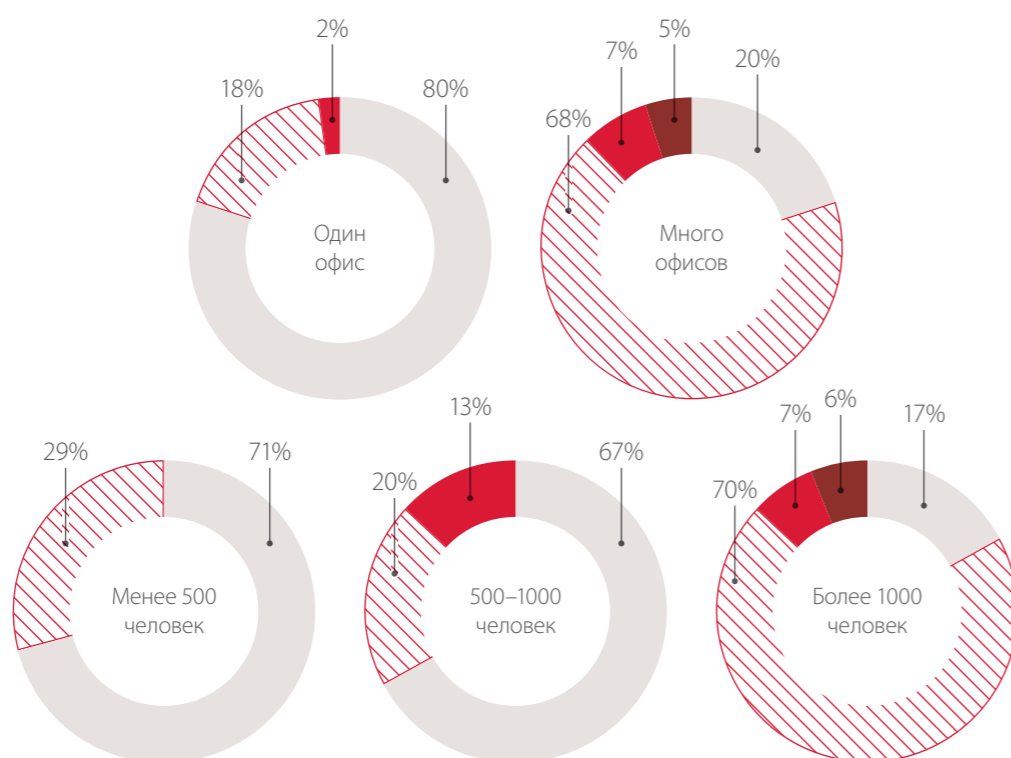
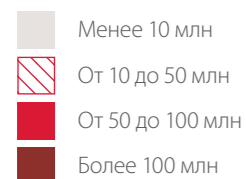


Рисунок 5. Годовой бюджет компаний на ИБ

Ряд решений по защите масштабируемы и не зависят (или зависят незначительно) от количества защищаемых ресурсов. Поэтому с ростом штата компании расходы на ИБ в перерасчете на одного сотрудника могут снижаться.

Опыт показывает, что бюджет, выделяемый на обеспечение ИБ, расходуется в первую очередь на приведение инфраструктуры в соответствие требованиям регуляторов. А это значит, что существенная часть средств уходит:

- + на разработку и адаптацию организационно-распорядительных документов;
- + на приобретение и внедрение минимально необходимых технических средств защиты, таких как антивирусы, межсетевые экраны и системы обнаружения вторжений.

И поскольку часто имеется возможность соблюдать требования без дополнительных затрат (например, администратор может ежедневно вручную проверять журналы событий безопасности вместо использования централизованной системы мониторинга), то многие организации на этом экономят и не приобретают лишние, на их взгляд, средства защиты.

Далее мы детально рассмотрим основные статьи расходов на обеспечение ИБ, на которые действительно стоит тратить бюджет, чтобы эффективно защитить компанию от современных киберугроз и избежать не только наказания от регуляторов, но и серьезных последствий от целенаправленных или массовых атак киберпреступников.

### РИСКИ

Риски информационной безопасности характеризуются комбинацией двух величин — вероятностью реализации угрозы и размером ущерба для компании. Стоит отметить, что ущерб от реализации риска не всегда связан с прямыми финансовыми потерями, также это могут быть:

- + репутационные издержки;
- + невозможность исполнения обязательств;
- + санкции регуляторов;
- + сокращение клиентской базы.

Мы попросили респондентов указать, какие угрозы они считают наиболее опасными для их компании.

«Считаем, что инвестиции в ИБ надо делать на основе анализа рисков, который должен регулярно обновляться... По результатам анализа текущей ситуации затраты на ИБ в 2017–18 году существенно повышены.»

Артем Натрусов,  
вице-президент по ИТ  
ООО «ЕвразХолдинг»

### Новые технологии — новые риски

Технологии привносят в бизнес не только новые возможности, но и новые риски, которыми необходимо эффективно управлять

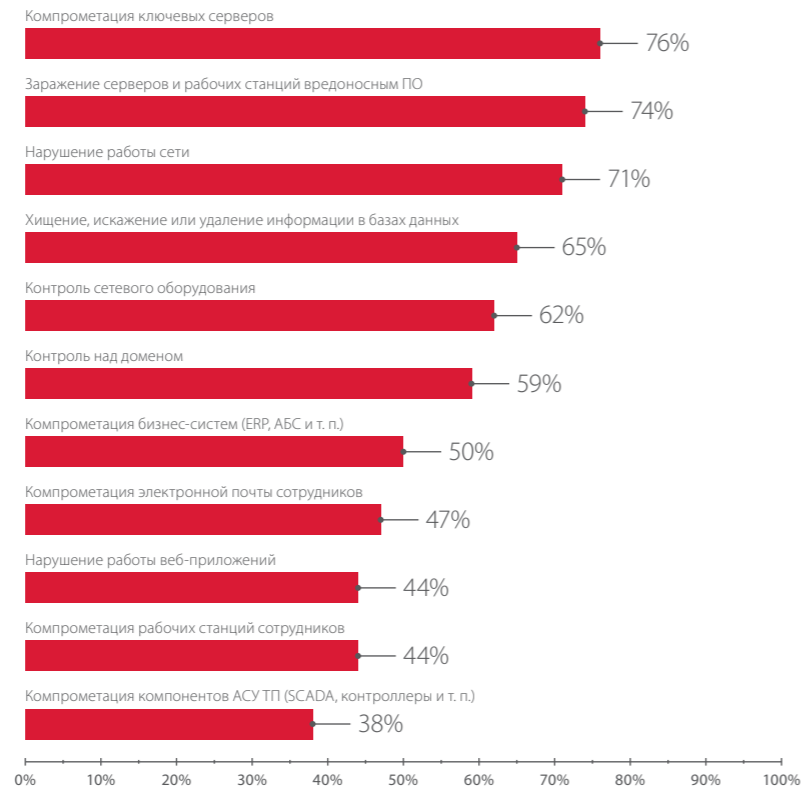


Рисунок 6. Доля компаний, для которых угроза ИБ является критически опасной

### В каждой второй компании

внешний нарушитель может получить полный контроль над всеми ресурсами

Сегодня инфраструктура практически каждой компании может быть взломана. По результатам [исследования](#) Positive Technologies, 73% компаний, проанализированных в 2016 году, были подвержены угрозе преодоления сетевого периметра. Кроме того, в половине организаций специалистам удалось получить полный контроль над инфраструктурой от лица внешнего нарушителя и во всех без исключения случаях — от лица внутреннего (например, недобросовестного сотрудника или подрядчика). Полный контроль означает не только доступ к серверам, компьютерам сотрудников, сетевому оборудованию, но и к критически важным системам, таким как системы управления финансовой отчетностью, компьютерам директоров компании, почтовым серверам, на которых доступна вся переписка сотрудников, к системам документооборота. В случае банка это могут быть АБС, процессинговый центр или система управления банкоматами. В случае промышленных предприятий — системы управления технологическими процессами, серверы, на которых хранятся данные о перспективных разработках, ноу-хау и т. п. Кроме того, сегодня зарождается новый тренд — атака на компании не с целью их компрометации, а с целью использования их инфраструктуры для атак на другие компании, что может привести к серьезным репутационным потерям, нарушению доверия со стороны партнеров и клиентов, блокированию ресурсов надзорными органами.

Для каждой современной компании сайт является визитной карточкой, которая позволяет клиентам получить всю необходимую информацию. При этом, согласно нашему [исследованию](#), атаки на веб-приложения в 25% случаев позволяют получить доступ к внутренней сети организации (если приложение находится не на внешнем хостинге) и еще в 25% — к базе данных. Кроме того, есть компании, деятельность которых выстроена на базе веб-ресурсов, например интернет-магазины, онлайн-банки, различные онлайн-сервисы. Если их сайты становятся недоступными (например, в результате DDoS-атаки), то нарушаются важные бизнес-процессы. Как правило, у клиентов это вызывает негативную реакцию, и они могут уйти к конкурентам.

В следующих разделах отчета мы остановимся подробнее на последствиях атак на инфраструктуру компаний и на веб-приложения, а также рассмотрим, как оценивают соответствующий ущерб компании-респонденты.

Далее при анализе бизнес-процессов обеспечения ИБ в компаниях мы исключили из оценки организации, попавшие в категорию «Другие», поскольку их было недостаточно для формирования выводов по отдельным отраслям.



## ФИНАНСОВЫЕ ПОТЕРИ ОТ КИБЕРИНЦИДЕНТОВ

Предлагаем сравнить оценку потерь от потенциального киберинцидента, которую предоставили компании-респонденты, с реальными последствиями аналогичных атак, расследуемых экспертами отдела мониторинга и реагирования на инциденты Positive Technologies.

Специалисты по ИБ ПАО «Росбанк» согласны с тем, что часть компаний недооценивает возможный ущерб от реализации киберугроз. Именно это обстоятельство и непринятие мер для предотвращения таких угроз и создает «питательную» среду для кибермошенников, позволяет им реализовывать свои устремления по хищению денежных средств со счетов компаний, проявляющих беспечность или самоуверенность в отношении киберугроз.

Николай Носов,  
начальник управления департамента  
информационной безопасности  
ПАО «Росбанк»

## 5 уязвимостей

достаточно внешнему нарушителю для проникновения во внутреннюю сеть компании и получения полного контроля над доменом

### Атаки на корпоративную информационную систему

Действует хакер целенаправленно или так получается случайно, но кибератака порой заканчивается для жертвы нарушением работы внутренних систем. Как правило, инфраструктура организаций строится на основе доменов Active Directory. Если нарушитель получит полный контроль над доменом и сетевым оборудованием, то он сможет парализовать работу всей сетевой инфраструктуры компании на длительное время. Практика показывает, что даже когда имеются средства защиты, они могут быть неэффективно настроены, и в этом случае получить контроль над доменом довольно просто. И если внешнему нарушителю для атаки потребуется эксплуатация в среднем 5 уязвимостей, то внутреннему нарушителю (например, сотруднику, контрагенту или любому другому человеку, получившему доступ к сетевой розетке, например уборщику) достаточно найти и использовать всего две-три уязвимости, для чего не потребуются глубоких технических знаний или дорогостоящих устройств.

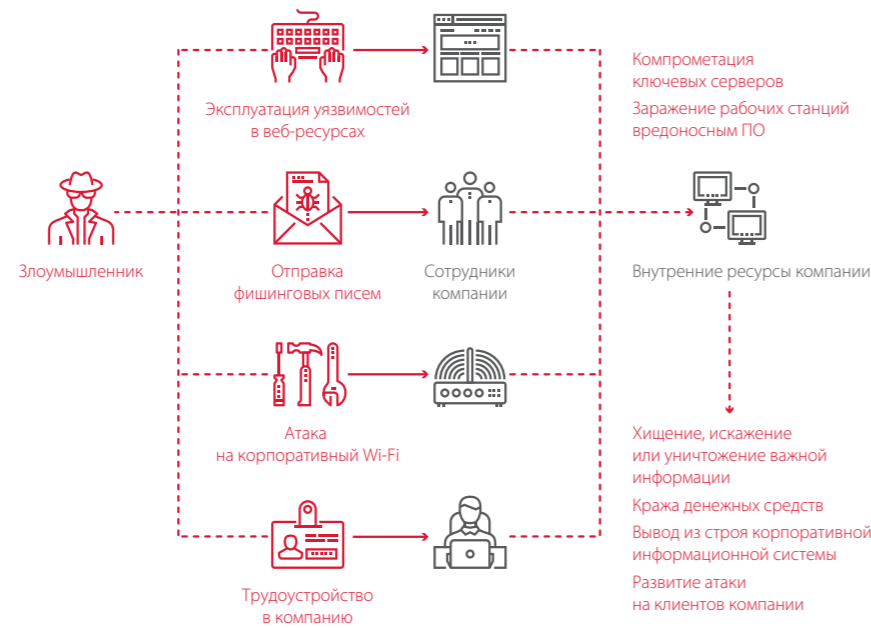


Рисунок 7. Типовой сценарий атаки на корпоративную информационную систему

Четверть компаний считают, что от остановки в работе всех систем на один день потеряют не более 500 тысяч рублей. Примечательно, что в эту категорию попали большинство IT-компаний, деятельность которых напрямую зависит от работоспособности информационных систем. На диаграмме ниже и далее мы рассматриваем разделение по категориям не только для всех компаний-респондентов, но и внутри одной отрасли.

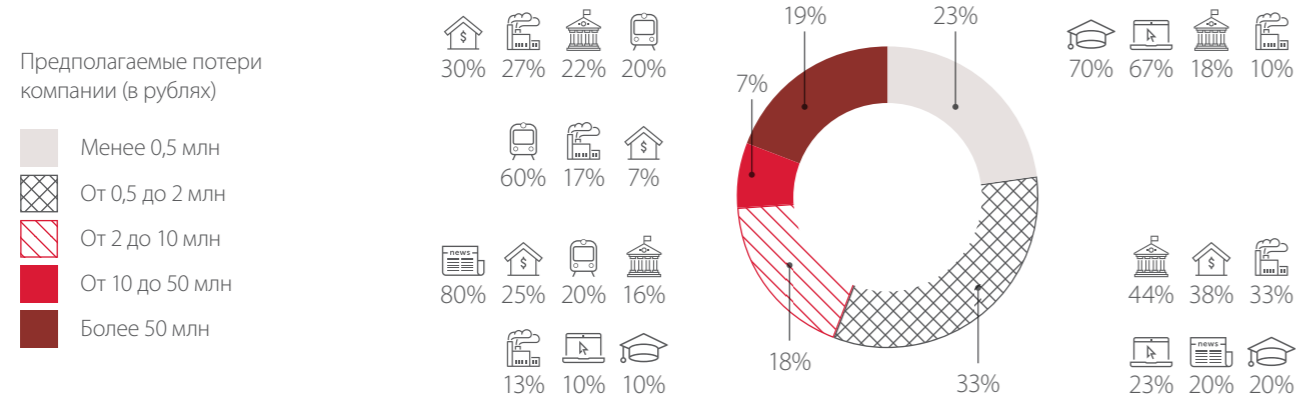


Рисунок 8. Потери от отказа всей корпоративной инфраструктуры в течение одного дня (доля компаний)

Скорее всего, некоторые респонденты недооценивают ущерб от простоя корпоративной инфраструктуры. Так, по оценке KnowBe4, предполагаемый ущерб, который нанес WannaCry по всему миру, превысил миллиард долларов США. При оценке ущерба учитывались потери компаний от простоя в работе, снижения производительности, недоступности данных, выплат шантажистам и, конечно, репутационные потери. Последствия были вызваны тем, что компании потеряли доступ только к данным. Еще один пример: троян-шифровальщик NotPetya обошелся датской логистической компании Moller-Maersk в 200–300 миллионов долларов. Эту сумму составила недополученная выручка компании за время простоя зараженных систем.

Помимо прямых финансовых потерь от киберинцидента (например, когда с корреспондентских счетов банка уводят деньги) и упущенной выгоды, связанной с простоем инфраструктуры и оттоком клиентов, существенные затраты могут быть вызваны дальнейшим восстановлением бизнес-процессов.

Мы сталкивались с целевой атакой, когда злоумышленники с целью шпионажа скомпрометировали контролеры доменов, серверы управления инфраструктурой, лок-серверы, рабочие станции сотрудников, в том числе высокопоставленных лиц компании. Организации для устранения всех последствий той атаки пришлось заново выстраивать всю корпоративную информационную систему буквально с нуля, что заняло более двух месяцев.

Затраты на восстановление (в рублях)

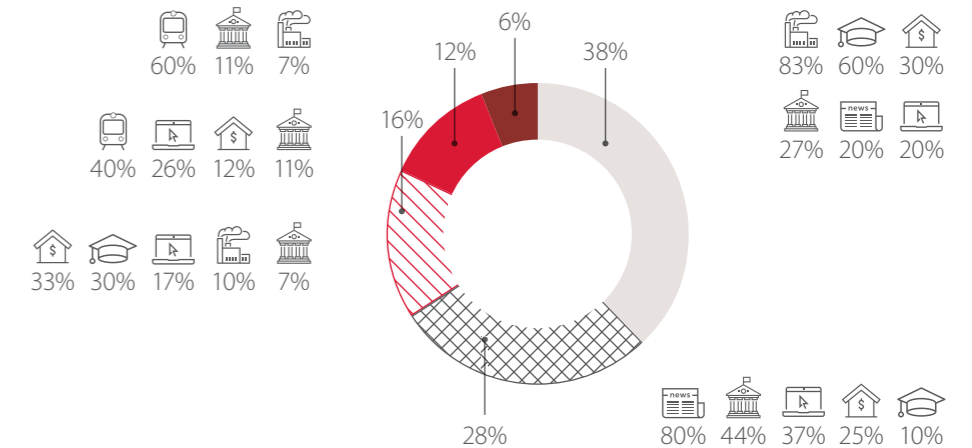
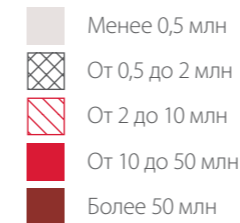


Рисунок 9. Затраты на восстановление корпоративной инфраструктуры после вывода из строя всех ресурсов домена (доля компаний)

## 100% респондентов

уверены, что восстановят работу корпоративных систем в случае выхода из строя всех ресурсов домена менее чем за месяц

Наибольшую оценку стоимости восстановления инфраструктуры дали 60% транспортных компаний, а также 11% государственных организаций (как вы понимаете, данную оценку дали все анализируемые госкомпании из топ-5 по выделяемому бюджету). По их подсчетам, в случае вывода из строя всех ресурсов домена потребуется более 50 миллионов рублей для возобновления работоспособности корпоративных информационных систем. Большинство же компаний полагает траты на восстановление незначительными. Большинство промышленных компаний, а также 30% банков готовы восстановить всю инфраструктуру, не потратив и 500 тысяч рублей. В случае некоторых банков это может объясняться относительно небольшими размерами инфраструктуры, в случае же промышленных компаний данная оценка кажется заниженной.

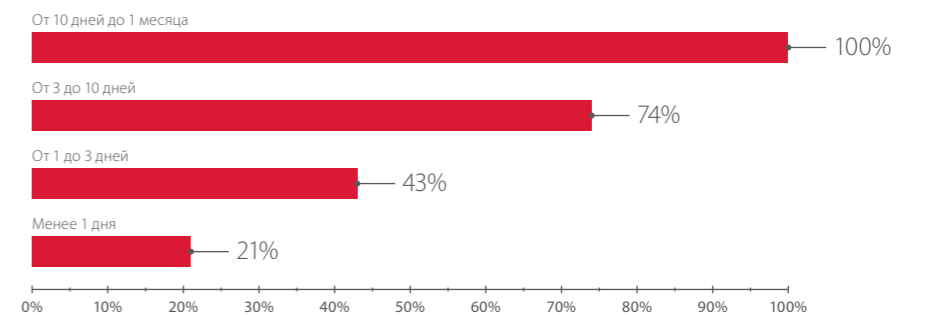


Рисунок 10. Срок, за который компании готовы восстановить корпоративную инфраструктуру в случае вывода из строя всех ресурсов домена (доля респондентов)



Компании выгодны долгосрочные отношения с покупателями, поэтому мы стараемся, чтобы люди в нашем интернет-магазине чувствовали себя комфортно и безопасно. Потенциальную атаку на посетителя сайта мы рассматриваем как удар по репутации компании, грозящий потерей лояльности наших клиентов. И мы непрерывно занимаемся анализом и реализацией мер, направленных на минимизацию таких рисков.

Артем Кроликов,  
руководитель департамента  
информационной безопасности  
ООО «М.Видео Менеджмент»

### Атаки на веб-приложения

Не стоит недооценивать важность защиты сайтов, даже если это всего лишь информационные страницы с контактами компании. Опираясь на наши ежеквартальные исследования атак на веб-приложения, мы определили, что ежедневно происходит в среднем 926 атак на веб-ресурсы. Практика показывает, что наибольший интерес злоумышленники проявляют к сайтам государственных и финансовых организаций. При этом атаки на веб-приложения потенциально могут приводить к утечке персональных данных. Так, например, 20% проанализированных в 2016 году веб-приложений, в которых обрабатывались персональные данные, включая сайты банков и государственных учреждений, были подвержены данной угрозе. Кроме того, как показывает опыт проведения тестирований на проникновение, в 77% всех выявленных векторов проникновения во внутреннюю сеть организаций сетевой периметр удалось преодолеть благодаря использованию именно уязвимостей веб-приложений.

Угрозе отказа в обслуживании веб-ресурсов подвержены компании из любой отрасли. В 2016 году при исследовании атак на веб-приложения мы отмечали, что каждый третий сайт подвергался данной атаке. Преимущественно атаки типа «Отказ в обслуживании» были направлены на промышленные предприятия и интернет-магазины. Во втором квартале 2017 года четверть атак на сайты медицинских учреждений составили именно попытки вызвать отказ в обслуживании.

Интересно то, что стоимость атаки на веб-ресурсы в течение часа в даркнете оценивается приблизительно в 5 долл. США, в течение суток — 300 долл. США, а вот ущерб для компании, которая в это время не могла выполнять основные свои функции, будет в сотни и тысячи раз больше.

Однако веб-ресурсы могут оказаться недоступны по разным причинам. Несмотря на то, что в этом в первую очередь винят DDoS-атаки хакеров, недостатки в конфигурации веб-сервера также могут нарушить работу веб-приложений. Так, в ходе расследования DDoS-атаки на сайт одного банка мы выяснили, что недостаток памяти в журналах ошибок стал причиной недоступности веб-ресурсов. Из-за недостатков в конфигурации сервера злоумышленникам было достаточно создать относительно небольшой поток запросов к ресурсоемким разделам сайта, чтобы нарушить его функционирование.

К нарушению работы веб-сервисов могут привести и другие атаки, в том числе удаление БД или дефейс.

Наибольшие потери от отказа в обслуживании сайтов, составляющие десятки миллионов рублей, понесут банки. Действительно, невозможность совершить перевод или платеж через онлайн-банк в течение одного дня вызовет недовольство среди клиентов, которые усомнятся в надежности банка, а возможно — понесут финансовые потери из-за невозможности завершить сделку.

### Миллионы рублей

составляет потенциальный ущерб от нарушения работы критически важных сайтов

Предполагаемые потери компании (в рублях)

- Менее 0,5 млн
- От 0,5 до 2 млн
- От 2 до 10 млн
- От 10 до 50 млн
- Данная оценка не применима к компании

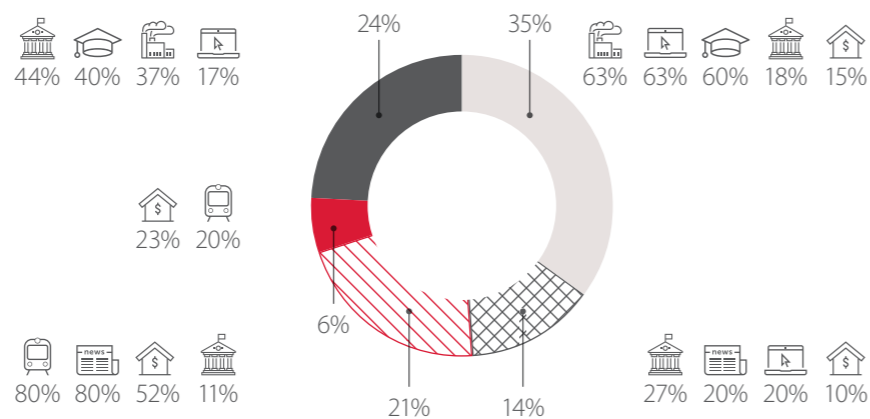


Рисунок 11. Оценка потерь от недоступности критически важных веб-приложений в течение одного дня (доля респондентов)

Веб-приложения являются одним из связующих звеньев, которое позволяет организовать подготовку и доставку информационного контента до конечного пользователя, а также обеспечить оперативное взаимодействие между собой работников, участвующих в повседневных производственных процессах.

Закономерно, что компании, являющейся круглосуточным информационным телеканалом, осуществляющим вещание в более чем 100 странах мира, необходимо принимать во внимание существующие риски.

Исходя из вышесказанного, защита веб-приложений является одним из приоритетных направлений в реализации стратегии обеспечения информационной безопасности телеканала.

Евгений Макаревич,  
руководитель отдела информационной безопасности  
дирекции информационных технологий  
Телеканал RT (Russia Today)



## 53% атак

на веб-приложения могут привести к утечке данных

### Кража базы данных

Существует множество сценариев атак, при которых злоумышленники могут получить базу данных о клиентах организации. Это может быть и недовольный сотрудник, который из обиды «сливает» данные конкурентам, и атака на внешние веб-ресурсы компании, в результате которой среди прочих данных злоумышленник получает и клиентскую базу, и многое другое.

Значительная доля опрошенных компаний (41%) не ждет финансовых потерь в случае реализации такой угрозы. Действительно, есть такие организации, прибыль которых не зависит напрямую от количества клиентов (например, те, что финансируются из государственного бюджета — образовательные учреждения, некоторые промышленные предприятия). Но что касается банков и IT-компаний, то мы рекомендуем им пересмотреть свою оценку.

Если об инциденте станет известно клиентам компании, то пострадает репутация организации. Если же конкуренты воспользуются полученной базой данных для того, чтобы переманить клиентов к себе, то компания понесет финансовые убытки из-за упущенной выгоды.

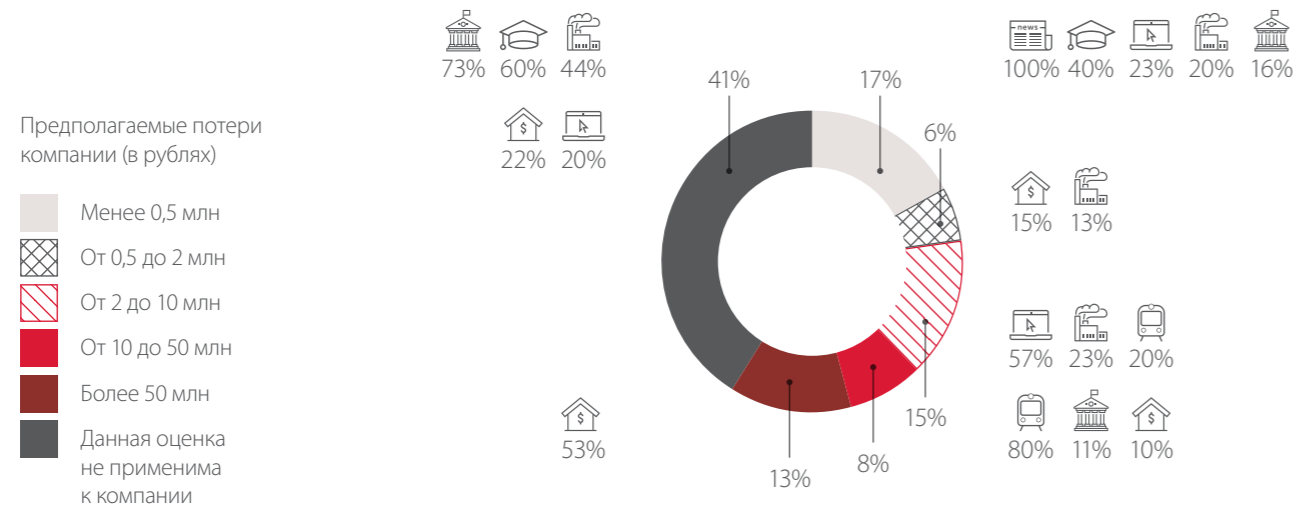


Рисунок 12. Предполагаемые потери от кражи БД клиентов конкурентом (доля респондентов)

Мы сталкивались с ситуацией, когда злоумышленники начинали шантажировать, угрожая уничтожением базы данных или ее публикацией в интернете. В результате атаки на веб-приложения компании злоумышленники якобы получили полный контроль над сервером базы данных и направили жертве письмо с требованием заплатить 10 000 долл. США. В результате расследования факты, подтверждающие возможность кражи данных, или следы присутствия нарушителя в инфраструктуре обнаружены не были. Однако компания все равно решила перестраховаться и заплатить злоумышленникам, поскольку риск публикации базы клиентов оценивался как недопустимый. Последствия реализации этого риска могли нанести серьезный удар по репутации и снизить уровень доверия к компании, а возможно, и вызвать судебные иски со стороны клиентов.

Кроме того, нельзя забывать, что законодательством Российской Федерации предусмотрена ответственность за «нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб» в виде штрафа в размере до 500 000 рублей. А персональные данные клиентов как раз относятся к охраняемой информации.



## РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

Именно от корректности действий, совершенных сотрудниками в случае возникновения инцидента ИБ, будет зависеть ущерб — сколько денег потеряет компания в результате атаки.

Превосходство на стороне хакеров, они не ограничены ни во времени, ни в методах, они на шаг впереди защитников. Универсальной защиты от киберугроз пока что не существует, однако можно минимизировать время обнаружения и реагирования на инциденты, если грамотно спланировать и регламентировать порядок действий всех вовлеченных в эту деятельность сотрудников.

Серьезный инцидент можно сравнить с пожаром. Например, троян-шифровальщик, попавший во внутреннюю сеть банка и заблокировавший все компьютеры, в том числе рабочие станции операторов в распределенных офисах, посеет хаос и панику в отделениях, которая может распространиться и на клиентов. Однако как действовать при пожаре, куда бежать и как спастись, знают все. И дважды в год проводятся тренировочные учения, чтобы все действия были отработаны до автоматизма. А что делать в случае киберинцидента? На этот вопрос ответит не каждый специалист отдела безопасности, не то что рядовой сотрудник.



■ Есть внутреннее подразделение SOC  
▨ Подразделение SOC отсутствует

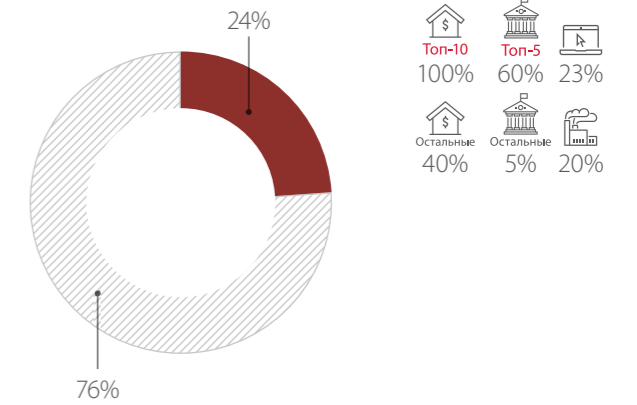


Рисунок 14. Доля компаний, имеющих внутреннее подразделение SOC

### Действия сотрудников

в случае киберинцидента должны быть так же отработаны, как эвакуация при пожаре

Как правило, когда компания сталкивается с действительно серьезным инцидентом, сотрудники IT-отдела не могут быстро справиться с ситуацией. Для противостояния современным атакам уже недостаточно знаний в области информационных технологий, нужно быть экспертом и в ИТ, и в ИБ, и в форензике, и в проведении пентестов, и в обратной разработке, разбираться в принципах проведения типовых атак и методах сокрытия следов. Практика расследования инцидентов, связанных с целевыми атаками, показывает, что многие компании не подозревают, что оказались жертвами киберпреступников. После получения доступа к инфраструктуре нарушитель может контролировать ее годами и скрывать свое присутствие. Один из подобных инцидентов был выявлен нашими экспертами спустя 5 лет после того, как произошло вторжение. Помочь в расследовании инцидента и принятии мер по устранению последствий могут как компании, специализирующиеся на вопросах безопасности, так и центры по противодействию киберугрозам соответствующей отрасли. Однако всего 17% организаций пользуются подобными услугами, в то время как больше половины пытаются справиться с угрозами своими силами.

- Иногда привлекаются специализированные сторонние компании для расследования инцидентов
- ▨ Расследования проводятся силами внутренних подразделений компании
- Отсутствует практика выявления и расследования инцидентов ИБ

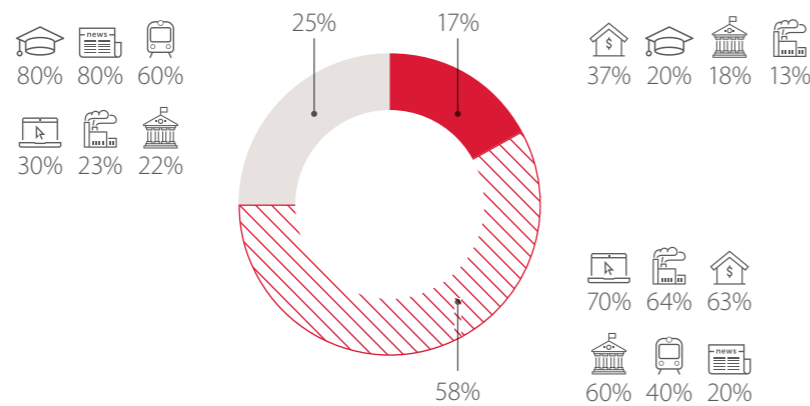


Рисунок 13. Способы расследования инцидентов (доля респондентов)

### В ¼ компаний-респондентов

отсутствует практика выявления и расследования инцидентов

Большое количество киберинцидентов, произошедших за последнее время, привлекло внимание руководителей компаний к проблемам информационной безопасности. В организациях массово стали появляться собственные ситуационные центры информационной безопасности (security operations centers, SOC). Они, в частности, функционируют в 24% компаний-респондентов, преимущественно в промышленной сфере, банках и госорганизациях.

### Стратегия расходов на ИБ

Агентство Gartner ожидает, что расширение возможностей по обнаружению и реагированию на атаки станет ключевым приоритетом компаний на период до 2020 года.

Примечательно, что большинство организаций, консультирующихся со сторонними экспертами в ходе расследования киберинцидентов, имеют собственное подразделение SOC. Этот подход считается наиболее рациональным, поскольку внутренний SOC хорошо осведомлен о процессах компании, обладает информацией обо всех инцидентах, происшедших ранее, и может, соответственно, проводить аналогии между ними. В то же время сторонние эксперты могут использовать опыт работы с другими организациями той же отрасли.

Для проникновения во внутреннюю сеть организации злоумышленники часто сканируют сетевой периметр компании, чтобы выявить веб-уязвимости, и даже не пытаются скрыть свои действия. Примечательно, что большинство атак подобного рода можно пресечь еще на стадии подготовки — до того, как нарушители получат доступ к внутренним ресурсам и важной информации. Так, например, если атакуемая организация использует систему корреляции и консолидации событий безопасности (SIEM-систему), то служба безопасности своевременно получит уведомление о событиях, связанных с началом атаки, и сможет принять необходимые меры по предотвращению инцидента. А применение межсетевых экранов уровня приложений (WAF) не позволит злоумышленникам проэксплуатировать уязвимости, выявленные на сайтах, и, соответственно, продолжить атаку на внутренние ресурсы компании.

Кроме того, компрометация веб-приложения может позволить нарушителю распространять вредоносное ПО на компьютеры пользователей сайта, что нанесет существенный ущерб репутации компании. Ярким примером является распространение трояна-шифровальщика *Bad Rabbit* через сайты популярных российских СМИ в октябре 2017 года.

Примечательно, что межсетевые экраны уровня приложений используют лишь 15% компаний-респондентов, в число которых входят государственные организации, банки, транспортные и промышленные компании.

■ Используют межсетевой экран уровня приложений (Web Application Firewall)  
▨ Не используют

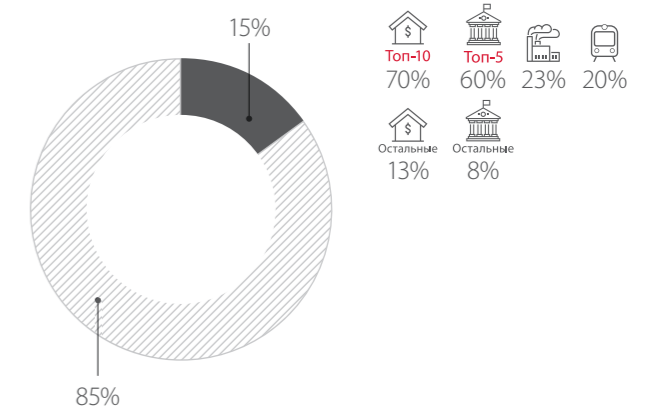


Рисунок 15. Доля компаний, использующих WAF

Если требования к степени безопасности и скорости реакции, в том числе на новые угрозы, достаточно высоки — безусловно, возникает вопрос о необходимости привлечения внешней экспертизы. Это не только позволяет расширить наблюдаемое пространство угроз, но и в кризисных ситуациях (даже при наличии достаточной компетенции) распараллелить поисковую и аналитическую работу, существенно сократить время до появления и проверки первых признаков компрометации — ключевых для принятия решения о дальнейших действиях, в том числе имеющих непосредственное влияние на бизнес организации. В нашей практике, помимо дежурной смены (группы быстрого реагирования), построенной по классической схеме L1–L2–L3, мы опираемся на экспертизу дочерней компании Сбербанка — Bi.Zone. Совместная работа наших оперативных дежурных, обогащенная глубокой экспертизой, позволяет поддерживать на высоком уровне скорость работы внутренних служб и при этом обеспечивать должную глубину проработки поступающей информации об угрозах.

Алексей Качалин  
Исполнительный директор центра киберзащиты  
ПАО «Сбербанк»

SIEM-системы применяются примерно в четверти организаций, причем преимущественно в компаниях с множеством офисов и более чем 1000 сотрудников. Ввиду специфики систем сбора и корреляции событий этот компонент необходим компаниям со зрелой разветвленной инфраструктурой. При этом правильно настроенная SIEM-система способна прийти на помощь SOC, анализируя события, происходящие в инфраструктуре, в режиме реального времени.

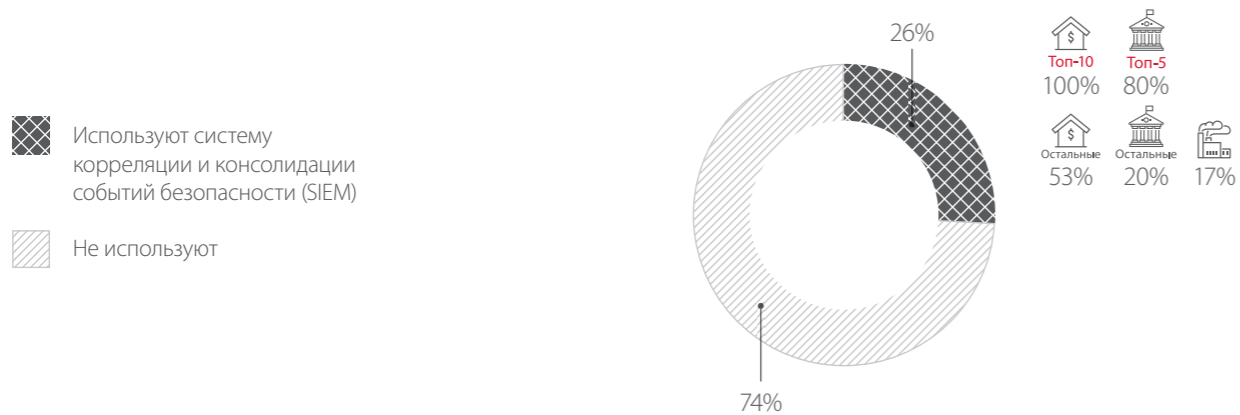


Рисунок 16. Доля компаний, использующих SIEM

Совместное применение WAF и SIEM позволит организовать комплексную защиту от киберугроз как на периметре, так и внутри корпоративной инфраструктуры, а также сэкономит время и ресурсы за счет автоматизации работ, которые специалисты по ИБ обычно выполняют вручную (например, анализ журналов событий со всех средств защиты).

## 35% компаний-респондентов,

в которых более 1000 сотрудников, применяют систему корреляции и консолидации событий безопасности (SIEM)

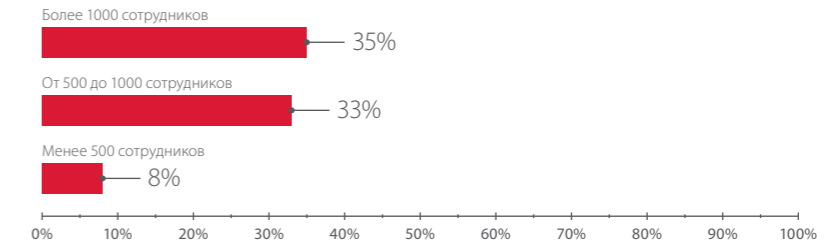


Рисунок 17. Доля компаний, использующих SIEM в зависимости от количества сотрудников

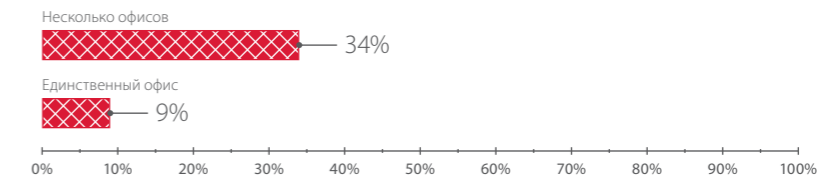


Рисунок 18. Доля компаний, использующих SIEM в зависимости от количества офисов

Сопоставив бюджет компаний, выделяемый на обеспечение ИБ, и принимаемые меры по реагированию на инцидент, мы видим, что большинство организаций, в которых на защиту информации выделяется более 50 млн рублей, создают внутренние подразделения SOC. SIEM и WAF начинают использоваться при наличии бюджета на ИБ свыше 10 млн рублей в год.

Когда у компании небольшой бюджет, а на обеспечение ИБ ежегодно выделяется всего пара миллионов рублей, то об использовании таких дорогостоящих решений, как SIEM, речи не идет. Однако этого бюджета достаточно для принятия минимально необходимых мер по защите на организационном уровне (например, для разработки процедур мониторинга и реагирования на инциденты), а также на покупку продуктов для защиты конечных точек (endpoint security), таких как антивирусное ПО.

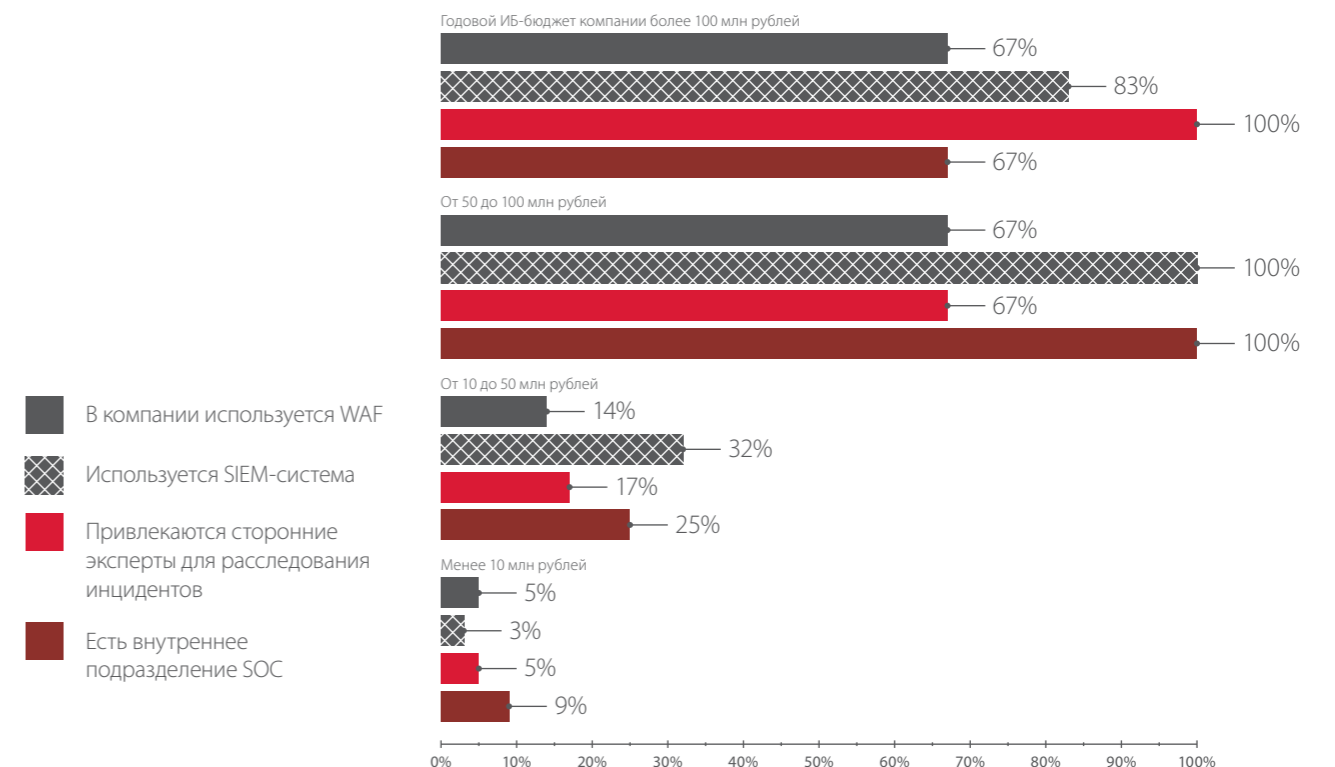


Рисунок 19. Соотношение бюджета и мер по обнаружению и реагированию на инциденты



Подчеркнем, что это — результаты опроса. Наш опыт проведения тестов на проникновение показывает, что проверку эффективности принятых мер по устранению уязвимостей проводят лишь порядка 35–40% организаций. В то же время при проведении последующих пентестов у некоторых компаний мы встречаем недостатки, которые не были устранены, либо принятых мер было недостаточно и уязвимости можно эксплуатировать повторно. Возможно, впрочем, что ряд организаций проводит проверку устранения уязвимостей, выявленных нашими экспертами, — самостоятельно или с привлечением других специалистов.

## Тестирование на проникновение

Для того чтобы обеспечить защиту корпоративной инфраструктуры, рекомендуется регулярно (не реже одного раза в год, а также при внесении существенных изменений в инфраструктуру) проводить тестирование на проникновение и (или) комплексный аудит информационной безопасности. Эти работы позволяют выявить уязвимости и недостатки безопасности и, соответственно, определить актуальные для организации угрозы ИБ и учесть их при оценке рисков. Только часть банков, государственных и промышленных организаций следуют рекомендациям и регулярно проводят тестирование на проникновение. Большинство компаний инициируют проверки, аудит ИБ, тесты на проникновение лишь в случае необходимости, например по факту выявления конкретного инцидента.

Примечательно, что несмотря на требование стандарта [PCI DSS 3.2](#) (относится ко всем организациям, которые обрабатывают данные владельцев платежных карт) о проведении ежегодного тестирования на проникновение, а также вопреки рекомендации Банка России по проведению комплексной оценки защищенности автоматизированной банковской системы, включающей тестирование на проникновение ([РС БС ИББС 2.6-2014](#)) — 10% финансовых организаций никогда не проводили подобных работ.

Важно отметить, что существенную роль в построении системы защиты играет не столько выявление уязвимостей, сколько принятие своевременных мер по их нейтрализации. Поэтому после устранения всех выявленных уязвимостей рекомендуется проводить проверку эффективности принятых мер. И этой рекомендации придерживаются 86% компаний-респондентов из числа тех, что проводят тестирование на проникновение и (или) аудит ИБ.

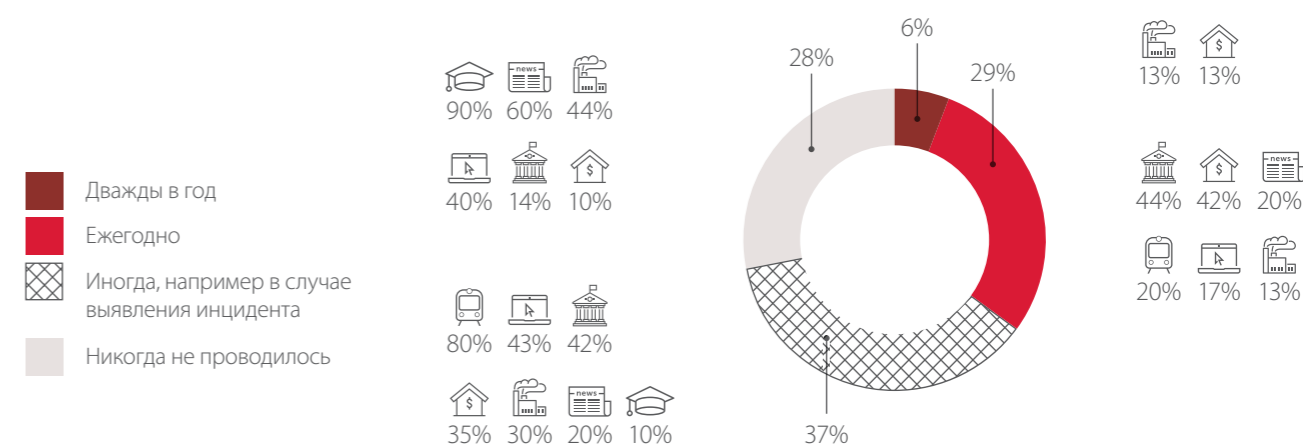


Рисунок 20. Регулярность проведения тестирования на проникновение или аудита ИБ (доля компаний)

## ФИНАНСОВЫЕ ЗАТРАТЫ НА ЗАЩИТУ

Законодательство Российской Федерации устанавливает необходимость использования ряда технических средств для обеспечения информационной безопасности. Средства антивирусной защиты, межсетевое экранирование, резервирования, управления доступом, системы обнаружения вторжений — затраты на внедрение, поддержание и модернизация этих компонентов в той или иной мере закладываются в бюджет всех компаний. Однако технологии развиваются намного быстрее требований регуляторов, законов и политик безопасности. Далее мы рассмотрим важные статьи расходов бюджета, выделяемого на защиту, о которых нельзя забывать — но не потому, что их отсутствие может привести к санкциям регуляторов, а потому что без них инфраструктура компании будет уязвима.

Среди компаний, которые проводят тестирование на проникновение и (или) аудит ИБ

- Проверяют эффективность принятых мер по устранению уязвимостей
- Не проверяют

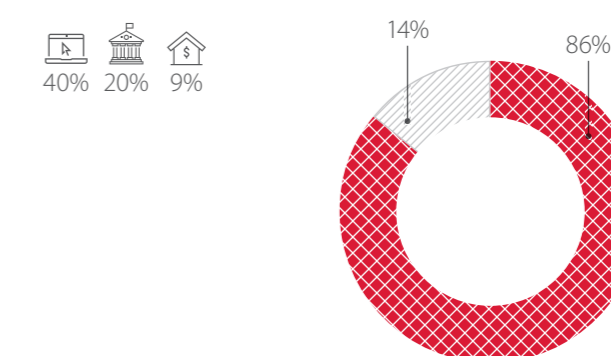





Рисунок 21. Доля компаний, проверяющих эффективность принятых мер по устранению уязвимостей

## 72% компаний

могут не заметить случайное появление новых ресурсов, доступных из сети Интернет

-  Проводится инвентаризация и контроль за появлением небезопасных ресурсов на периметре сети
-  Инвентаризация проводится для получения информации о ресурсах
-  Инвентаризация не проводится

### Инвентаризация ресурсов сетевого периметра

Невозможно защищать ресурсы, о наличии которых не знаешь. Пятая часть компаний не могут с уверенностью сказать — сколько и каких ресурсов доступно на периметре их сети. При этом в 91% организаций в ходе работ по анализу защищенности были выявлены интерфейсы удаленного доступа, управления оборудованием и подключения к СУБД. Причем большинство компаний, у которых такие интерфейсы были обнаружены, не ожидали увидеть на периметре сети столько уязвимых узлов и ресурсов, которые, по их мнению, не должны были быть доступны из сети Интернет.

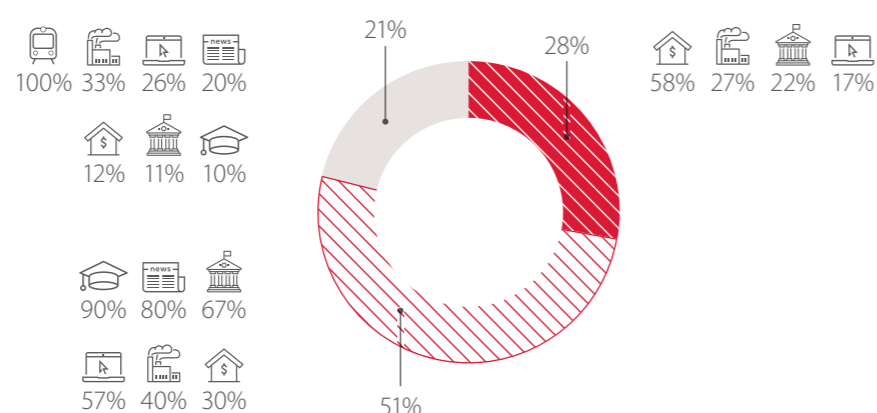


Рисунок 22. Доля компаний-респондентов, в которых проводится инвентаризация ресурсов сетевого периметра




Исследование сетевого периметра финансовых организаций показало, что чем крупнее банк, тем сложнее его инфраструктура и, соответственно, больше сервисов размещено на сетевом периметре. А с ростом числа сервисов увеличивается вероятность ошибки конфигурации. Для 100 анализируемых банков был выявлен 2781 доступный адрес, из которых 326 содержали потенциально опасные сервисы.

Информационные системы в крупных компаниях развиваются стремительно: даже в пределах одной недели может появиться несколько десятков новых узлов и столько же могут перестать функционировать. И вероятность того, что некоторые из узлов будут доступны из сети Интернет, очень велика. Уследить за тем, чтобы на всех рабочих станциях и серверах не были доступны опасные сервисы или везде были установлены актуальные обновления, — крайне сложная задача. Именно по этой причине периодический контроль состояния периметра в режиме, максимально приближенному к реальному времени, очень важен для обеспечения безопасности.

### Анализ защищенности беспроводных сетей

Беспроводные сети являются неотъемлемой частью корпоративной инфраструктуры большинства современных компаний. Однако успешный взлом Wi-Fi позволяет не только перехватывать чувствительную информацию, атаковать пользователей беспроводной сети, но и развивать атаку для получения доступа к ресурсам внутренних сетей организаций. Поэтому наряду с выявлением уязвимостей в корпоративных информационных системах важно также проверять и защищенность беспроводных сетей, используемых в компании.

Регулярно анализ защищенности беспроводных сетей проводит лишь четверть банков, а еще четверть — никогда не проводили данные работы. В 6% компаний-респондентов отсутствуют беспроводные сети. В общем-то, это можно считать мерой защиты, ведь если нет Wi-Fi, то нет и риска, что хакеры им воспользуются для проведения атак :)

-  Проводится регулярно
-  Проводится периодически (после инцидента)
-  Никогда не проводился

### Ежеквартально

необходимо проверять наличие авторизованных и неавторизованных точек Wi-Fi (согласно стандарту PCI DSS). Требование актуально преимущественно для сферы розничной торговли, где часто используются беспроводные терминалы оплаты

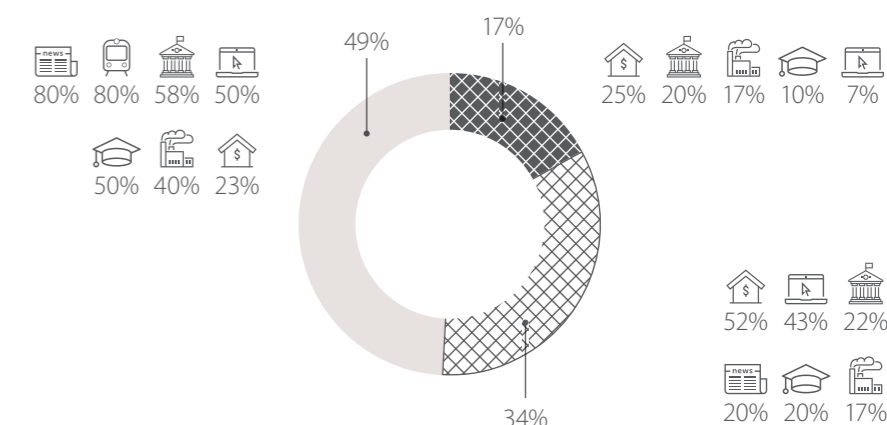




Рисунок 23. Анализ защищенности беспроводных сетей (доля компаний, использующих корпоративный Wi-Fi)

### Контроль обновлений

Примечательно, что хотя большинство компаний контролируют установку обновлений, в ходе тестов на проникновение наши специалисты регулярно выявляют использование устаревших версий программного обеспечения или отсутствие необходимых обновлений безопасности. Так, 82% исследованных в 2016 году корпоративных информационных систем использовали уязвимые версии прикладного ПО, 64% — уязвимые версии веб-серверов, а 18% — уязвимые версии поставляемых вендорами веб-приложений. А значит, нарушитель мог использовать известные уязвимости, характерные для этих версий ПО, в реализации различных атак.

-  Выполняется регулярно
-  Отсутствует

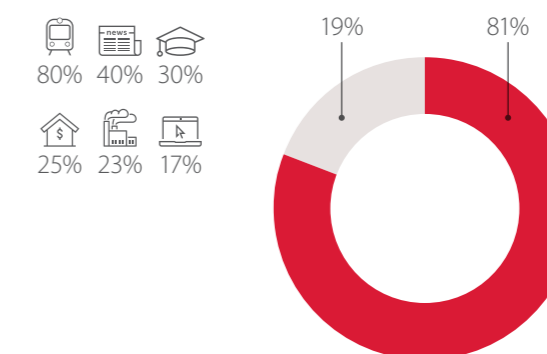


Рисунок 24. Контроль установки обновлений ПО (доля компаний)

Например, про небезопасность использования протокола SMBv1 известно достаточно давно, патч для устранения уязвимости MS17-010 появился в марте 2017 года. Практически в то же время был опубликован известный на весь мир эксплоит ETERNALBLUE. В 71% проектов по тестированию на проникновение, проведенных нашими специалистами в течение 7 месяцев с момента появления обновления, была продемонстрирована возможность получения полного контроля над ресурсами компаний с использованием именно этого инструмента.

В некоторых случаях технические специалисты аргументируют отказ от установки актуальных обновлений тем, что внесение изменений в систему может повлиять на корректность функционирования компонентов, не совместимых с новой версией ПО. Однако в случаях, когда риск нарушения работоспособности действительно велик, необходимо принимать дополнительные меры по защите, например выделяя такие компоненты в отдельные сетевые сегменты, доступ к которым из пользовательской сети будет закрыт.

### Выявление и устранение уязвимостей нулевого дня

Исследователи по всему миру периодически находят и публикуют информацию об уязвимостях нулевого дня. Против таких уязвимостей не действуют существующие защитные механизмы, однако производитель программного обеспечения, в котором была выявлена такая уязвимость, как правило, дает рекомендации для решения проблемы на время, пока не появится соответствующий патч, устраняющий уязвимость.

-  Информация о новых уязвимостях оперативно анализируется и принимаются меры по устранению
-  Данные принимаются во внимание, но принятие мер откладывается на неопределенный срок
-  Отсутствует практика поиска новых уязвимостей

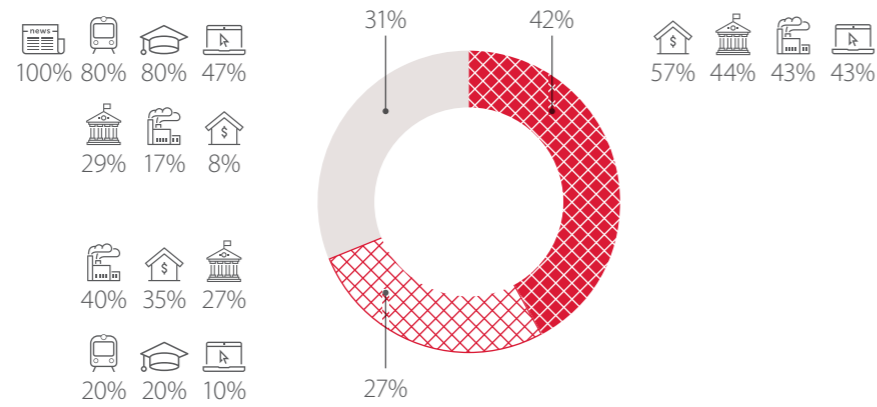


Рисунок 25. Доля компаний, обладающих практикой мониторинга публикаций с информацией о новых уязвимостях (0-day)

Надо ли говорить, что злоумышленники стараются воспользоваться такими уязвимостями, чтобы атаковать компании, которые не приняли необходимые меры для защиты. Менее половины компаний-респондентов отслеживает появление информации о новых уязвимостях и оперативно принимает меры по их устранению или превентивные меры защиты, остальные либо не следят за новостями в этой области, либо откладывают принятие мер на неопределенный срок.




### Обучение сотрудников

Слабым местом в обеспечении ИБ любой компании являются сотрудники — по причине их недостаточной осведомленности в вопросах информационной безопасности. Примечательно то, что несмотря на сложность и продуманность системы защиты в организации, всего один работник, перешедший по вредоносной ссылке из письма или загрузивший файл с вредоносным ПО, может привести к компрометации всех ресурсов компании.

Практика расследования целевых атак показывает, что именно рассылка фишинговых писем — наиболее частый и при этом эффективный начальный вектор атак, позволяющий злоумышленникам проникнуть во внутреннюю сеть компании.

#### Фишинг

сегодня является самым распространенным методом проникновения в корпоративную сеть при реализации АРТ-атаки

-  Проводится регулярно с последующей проверкой эффективности
-  Проводится формально без проверки эффективности
-  Не проводится

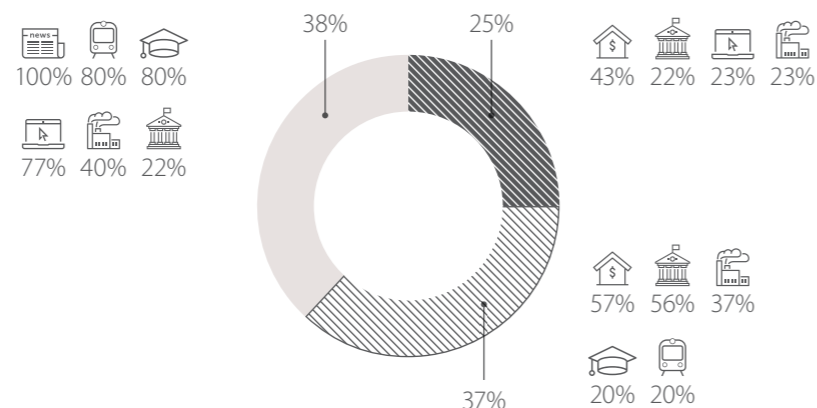


Рисунок 26. Доля компаний, которые проводят тренинги для сотрудников по вопросам ИБ

Несмотря на регулярные оповещения и тренинги всегда остается вероятность того, что работник не распознает угрозу. Как показывает практика, на хорошо подготовленные целенаправленные фишинговые письма попадают даже квалифицированные и опытные IT- и ИБ-специалисты. Поэтому мы учим не только на открытие и возниконовения малейших сомнений на счет отправителя и содержимого письма.

Александр Евтеев,  
директор по информационной безопасности  
ООО «РТ-ИНФОРМ»



Исследование показало, что банковская отрасль — единственная, в которой 100% компаний принимают меры по обучению сотрудников основам ИБ. В этом основная заслуга требований Банка России и международного стандарта PCI DSS, обязывающих проводить работу с персоналом по обучению и повышению осведомленности в вопросах информационной безопасности.

Больше трети организаций (38%) не уделяют внимания обучению сотрудников основным правилам ИБ. Заметим, что помимо скучных методических документов сегодня существует множество нестандартных способов повышения осведомленности — от красочных плакатов до мультфильмов, освещающих различные киберугрозы и порядок действий в той или иной ситуации.





### Бюджет и организационные меры по защите

Оценив соотношение бюджета, выделяемого на обеспечение ИБ, и принимаемых организационных мер защиты, мы видим, что значительный бюджет в 10, 50 и даже более чем в 100 миллионов рублей, выделяемый на обеспечение ИБ, не гарантирует, что в организации применяются все необходимые и достаточные меры для защиты от киберугроз. В компаниях, обладающих колоссальными средствами (это 5 госкомпаний и 10 банков с наибольшим ИБ-бюджетом), основные рекомендации преимущественно выполняются.

Большие вопросы вызывает целесообразность расходов в организациях с бюджетом свыше 10 миллионов. Возможно, что значительная часть ресурсов уходит на разработку организационно-методических документов, удовлетворяющих требования регуляторов. Однако сложно внедрять в компании руководящие документы по защите информации и описывать существующие процессы без актуальных результатов проведенного аудита. Также мы видим, что защита беспроводных сетей и контроль периметра осуществляются в этих компаниях в меньшей мере; возможно, они пока сосредоточены на закупке дорогостоящих аппаратных средств защиты и не успели уделить данным вопросам достаточно внимания.

Ежегодные расходы на ИБ для нашего вуза это продление лицензий антивирусных средств, ОС и прикладного ПО, а также повышение квалификации IT-специалистов в вопросах безопасности. Среди приоритетов на 2018 год отмечу программно-аппаратный комплекс для создания внутренней защищенной сети и организацию безопасного соединения с филиалами в других городах. Кроме того, на 2018 год запланированы аттестация ИС, в которых обрабатываются персональные данные, и тренинги для сотрудников на базе симулятора вирусных атак.

Алексей Гузев,  
директор департамента  
информационных систем  
и технологий МТУСИ

-  В компании регулярно проводится обучение сотрудников
-  Регулярно проводится анализ защищенности беспроводных сетей
-  Контролируют появление небезопасных ресурсов на периметре сети
-  Регулярно проводится тестирование на проникновение или аудит ИБ

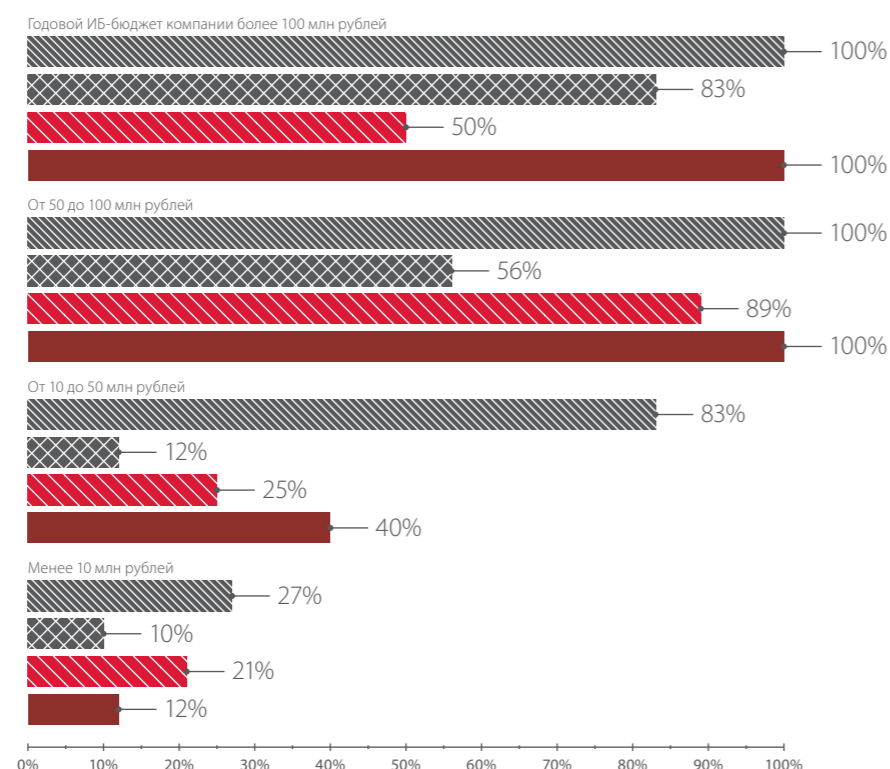


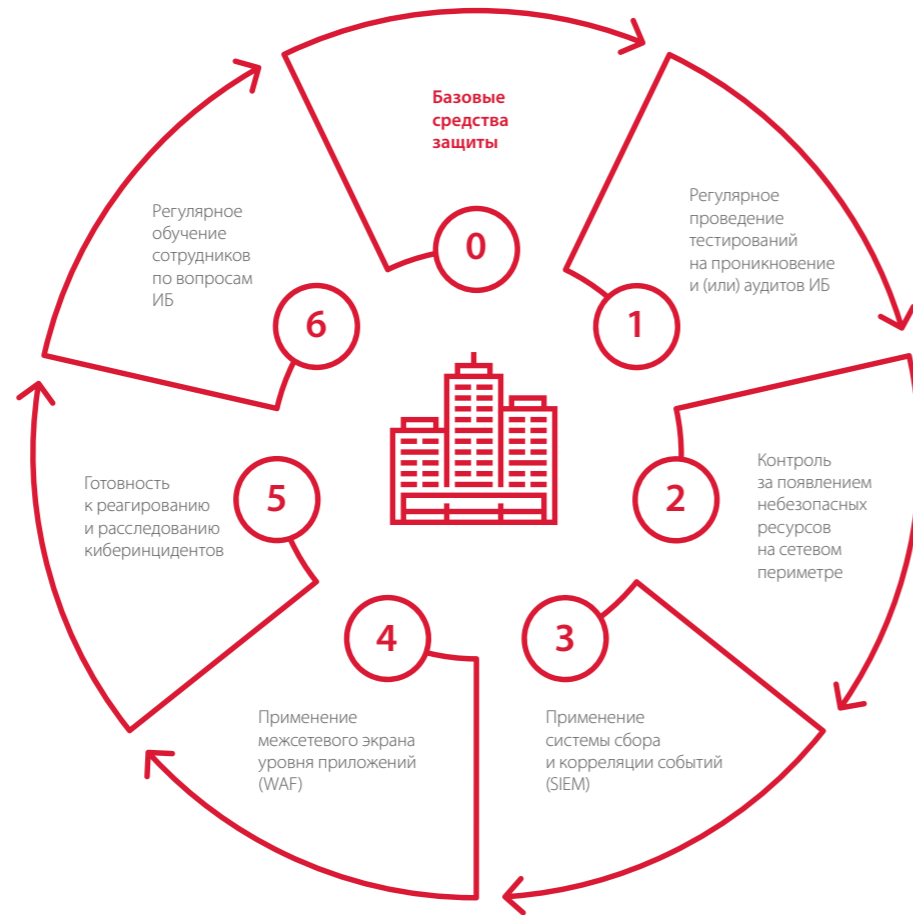
Рисунок 27. Соотношение бюджета и применяемых организационных мер по защите от киберинцидентов

## КОМПОНЕНТЫ ЗАЩИТЫ

Средства антивирусной защиты, межсетевое экранирование и виртуальные частные сети, демилитаризованные зоны, IPS/IDS, средства резервирования — эти компоненты в той или иной мере присутствуют в каждой организации, поскольку необходимость их использования закреплена на законодательном уровне в части требований по защите информации. Кроме того, необходимость обучения сотрудников основным правилам информационной безопасности сегодня также не требует доказательств.

Однако тенденции кибератак показывают, что стандартные средства защиты перестали быть серьезной преградой для целевой атаки на организацию, а значит — пора совершенствовать систему защиты. Причем для разумного распределения бюджета мы рекомендуем выделить шесть основных компонентов защиты от киберугроз.





## 01

### Регулярное (не реже 1 раза в год) проведение тестирования на проникновение и (или) аудита ИБ

Это первый и обязательный для всех компаний шаг, позволяющий выявить актуальные угрозы. Причем помимо заключения договора с опытными компаниями существуют и другие способы решения этого вопроса. Например, некоторые небольшие организации, ограниченные в бюджете, берут в штат одного сотрудника, обладающего необходимым опытом по анализу защищенности систем.

## 02

### Контроль за появлением небезопасных ресурсов на сетевом периметре

Когда в компании всего десяток компьютеров, то все открытые на них сетевые интерфейсы, доступные из сети Интернет, можно контролировать. Однако когда у организации большая инфраструктура и тем более распределенная (например, несколько офисов в разных городах, а часть сотрудников работают из дома), то уже сложно не только сказать, какие порты доступны из сети Интернет, но и вообще точно подсчитать, сколько и каких ресурсов используются и каков уровень их защищенности. В таком случае необходимо применять специализированные сканеры для анализа защищенности сетевого периметра или поручать эту работу специализированным организациям.

## 03

### Применение системы сбора и корреляции событий (SIEM)

Ввиду специфики систем сбора и корреляции событий этот компонент необходим компаниям со зрелой разветвленной инфраструктурой. При этом правильно настроенная SIEM-система способна прийти на помощь SOC, анализируя события, происходящие в инфраструктуре, в режиме реального времени.

## 04

### Применение межсетевого экрана уровня приложений (WAF)

Этот компонент значим для всех компаний, у которых есть сайт, поскольку позволяет своевременно выявить и предотвратить веб-атаки. Наиболее актуально применение WAF в организациях, которые размещают серверную часть веб-ресурсов внутри корпоративной инфраструктуры, а не на стороннем хостинге, поскольку в такой ситуации в случае успешной атаки помимо риска проведения атак на пользователей и нарушения работы сайта (например, в результате DDoS или дефейса) также возможно проникновение злоумышленника во внутреннюю сеть. Данный компонент необходим не только в тех сферах деятельности, которые построены на основе возможностей веб-ресурсов (например, системы дистанционного обслуживания в банковской отрасли или интернет-магазины), но и компаниям, которые не хотят оказаться промежуточным звеном целенаправленной атаки. В последнее время злоумышленники стали использовать уязвимые сайты для размещения на них вредоносного ПО, а владельцы этих веб-ресурсов становятся невольными соучастниками атаки.

## 05

### Готовность к реагированию и расследованию киберинцидентов

Речь идет не только о создании внутреннего подразделения SOC, которое в режиме 24/7 выявляет и анализирует инциденты ИБ и кибератаки, но и о предварительных договоренностях со сторонними специалистами, которые в случае инцидента смогут быстро прибыть на место и помочь с принятием необходимых мер для блокировки атаки и нейтрализации последствий. Кроме того, внешний SOC может полностью взять на себя функции по мониторингу событий в системах защиты компании, сообщать в случае выявления инцидента и самостоятельно принимать меры по нейтрализации угроз.

## 06

### Регулярное обучение и повышение осведомленности сотрудников в вопросах ИБ

Всего один работник, перешедший по вредоносной ссылке из письма или загрузивший файл с вредоносным ПО, может стать причиной компрометации всех ресурсов компании. Поэтому необходимо обучать сотрудников компании основным правилам информационной безопасности: это позволит снизить риски, связанные с неумышленными действиями персонала при работе в корпоративной информационной системе.

Ниже представлена сводная таблица, которая показывает доли компаний, применяющих те или иные компоненты в совокупности.

Доля компаний-респондентов							Среди всех	Регулярно проводят пентесты	Контролируют периметр	Есть SIEM	Есть WAF	Есть SOC и (или) привлекают экспертов для расследований	Проводят обучение сотрудников
Внутри одной отрасли													
	13%						3%	+	+	+	+	+	+
	5%						1%	+	+	+	-	+	+
4%							1%	+	+	+	+	-	+
9%	5%		3%				4%	+	+	-	-	+	+
7%	5%		3%				4%	+	-	+	-	+	+
4%							1%	+	-	+	+	-	+
	2%						1%	+	-	-	+	+	+
7%	13%						5%	+	+	+	-	-	+
	8%						2%	+	-	-	+	+	+
	18%		7%				5%	-	+	+	-	+	+
	2%	3%					1%	+	-	-	-	+	+
2%			3%				1%	+	-	-	+	+	-
	10%						2%	-	-	+	-	+	+
		13%					2%	-	+	-	-	+	+
	5%						1%	-	+	-	+	-	+
2%			7%				2%	-	-	-	+	+	+
11%	2%		13%				6%	+	-	-	-	-	+
		7%	3%				2%	+	-	-	-	+	-
4%	2%						2%	-	-	+	-	-	+
2%		3%	11%				3%	-	+	-	-	-	+
			13%		20%		3%	-	-	-	+	-	+
				20%			1%	-	-	-	-	+	+
			7%				1%	-	+	+	-	-	-
27%	10%	3%	3%				11%	-	-	-	-	-	+
		7%			20%	20%	2%	+	-	-	-	-	-
21%		64%	27%	80%	60%	80%	31%	-	-	-	-	-	-

Таблица 1. Доля компаний, применяющих основные компоненты защиты одновременно

## ЗАКЛЮЧЕНИЕ

Технологии привносят в бизнес не только новые возможности, но и новые риски, которыми необходимо эффективно управлять. К сожалению, всего в 3% компаний мы увидели комплексный подход к защите от киберугроз (в их числе оказались только финансовые учреждения, 13% опрошенных банков). Риск-ориентированный подход к решению задач информационной безопасности используется в компаниях редко и не в полном объеме. О страховании рисков кибератак большинство российских компаний либо не слышали, либо только начинают задумываться (за исключением банковской сферы, где страхование в принципе широко распространено). Хотя на Западе страхование является стандартным способом обработки рисков в тех ситуациях, когда компания не в силах принять меры для их снижения и не имеет возможности отказаться от деятельности, связанной с ними.

Подводя итоги исследования, мы видим, что большое количество киберинцидентов, произошедших за последнее время, привлекло внимание компаний к проблемам информационной безопасности. По данным рекрутинговых агентств, со стороны работодателей растет интерес к специалистам по информационной безопасности. Компании создают внутренние подразделения SOC, для которых требуются сотрудники. Кроме того, организации стремятся отделять специалистов, занимающихся вопросами защиты, от тех, кто выполняет функции администраторов.

Среди компаний-респондентов выделяются государственные компании, которые не скупают на нужды ИБ, однако при этом не применяют все необходимые и достаточные меры для защиты. Так, например, тестирование на проникновение в половине государственных организаций проводится только после инцидента или и вовсе ни разу не проводилось. Финансовые организации также не жалеют средств, но они при этом, как мы видим, стараются идти в ногу со временем.

Промышленным компаниям в первую очередь важна работоспособность используемых систем, а их безопасность является делом второстепенным, поэтому и бюджет, выделяемый на обеспечение ИБ, в большинстве случаев не столь значителен, как в государственных или финансовых компаниях. К тому же промышленность — это важная сфера, где любые изменения в инфраструктуре могут оказать серьезное влияние на технологический процесс, поэтому все дополнительные средства защиты применяются с осторожностью. Кроме этого, не всегда существует возможность быстро внести изменения в конфигурацию оборудования и прикладного ПО или установить обновления. И хотя организации знают о проблемах, связанных с ИБ, в настоящее время не все готовы их решать эффективно ввиду нюансов, связанных с используемыми технологиями и внутренними бизнес-процессами, а также в связи с неготовностью руководства вкладывать в безопасность значительные суммы. Стоит предположить, что введение в действие федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» внесет существенные положительные изменения в процессы обеспечения защиты промышленных объектов.

Исследование показало, что IT-компании максимально оптимизируют затраты и принимают меры лишь в случае реальных инцидентов, зачастую пренебрегая превентивными мерами защиты.

Разные сферы по-разному подходят к вопросам защиты. Главное, что никто не стоит на месте, а своим путем идет к созданию безопасного пространства для ведения бизнеса.

### О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.