POSITIVE TECHNOLOGIES

Компромисс бюджета и безопасности

Анализируем уровень защищенности организаций в регионах России

Содержание

Введение 2

Портрет участников 2

Финансирование 4

Меры и средства обеспечения ИБ 8

Готовность к реагированию на кибератаки 11

Ключевые особенности регионов 17

Выводы 21

Введение

Выступая на пленарном заседании Международного конгресса по кибербезопасности, который прошел в Москве 5 и 6 июля 2018 года, В. В. Путин отметил, что «цифровые платформы и электронный документооборот кардинально повышают открытость и эффективность работы органов власти, компаний, бизнеса, социальных и образовательных учреждений». В то же время темпы расширения преступной деятельности в киберпространстве стремительно увеличиваются с каждым годом. По данным МВД, с января по октябрь 2018 года в России было зафиксировано 141 552 преступления, совершенных с использованием компьютерных и телекоммуникационных технологий, что почти в два раза больше, чем с января по октябрь 2017 года. Рост числа киберпреступлений закономерно ведет к увеличению суммарного ущерба для экономики страны. В 2017 году Сбербанк оценил убытки российских компаний от хакерских атак в 600–650 млрд рублей, в то время как в 2018 году прогнозируемые потери составят 1,1 трлн рублей. Большинство преступных действий хакеров попадают под санкции ст. 272 УК РФ и связаны с неправомерным доступом к компьютерной информации. По данным Генпрокуратуры за 2017 год, наибольшее число киберпреступлений зафиксировано в регионах. В тройку лидеров по числу компьютерных атак вошли Удмуртия (Приволжский федеральный округ), Коми (Северо-Западный федеральный округ) и Омская область (Сибирский федеральный округ).

Цель нашего исследования — выяснить, как на самом деле обстоят дела с информационной безопасностью в регионах России и какие проблемы ИБ актуальны для регионального бизнеса. Мы проанализировали состояние защищенности российских организаций в регионах и постарались оценить достаточность их бюджета на ИБ, мер защиты и готовность к реагированию на кибератаки.

Портрет участников

В основу исследования положены результаты анкетирования, которое мы проводили в течение 2018 года. Активными участниками опроса стали организации из четырех регионов — Приволжского, Уральского, Сибирского и Дальневосточного федеральных округов. Доля респондентов из остальных федеральных округов суммарно составила 6% от общего числа, поэтому мы объединили их в категорию «Другие», однако все ответы респондентов из всех регионов проанализированы и учтены.

Участниками опроса были руководители подразделений ИТ и ИБ из 192 компаний, многие из которых входят в такие рейтинги, как:

- 500 крупнейших компаний России в 2018 году по версии РБК;
- крупнейшие компании России (RAEX-600) по итогам 2017 года;
- крупнейшие компании Урала и Западной Сибири (Эксперт-Урал-400) по итогам 2017 года.

Изучив ответы респондентов, мы выявили общие тенденции во всех округах и поэтому решили строить исследование на уровне отрасли, без детальных срезов по регионам, отразив лишь главные особенности в инфографике, которую можно найти в конце отчета.

Опрос проводился в 2018 году

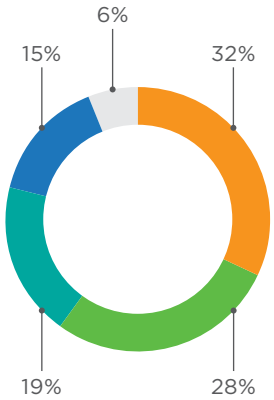
4 активных округа

192 компании

Рисунок 1. Характеристики основных регионов, принявших участие в опросе[1]

Далее по тексту используются следующие обозначения:

- Государственная организация
- Информационные технологии
- Финансовая организация
- Нефтегазовая отрасль
- Промышленность
- Образование
- Энергетика
- Иные сферы деятельности



Уральский федеральный округ	28%	43%	39%	22%	31%	–	33%	33%
Приволжский федеральный округ	33%	31%	24%	35%	31%	12%	–	–
Дальневосточный федеральный округ	18%	14%	30%	26%	8%	–	–	33%
Сибирский федеральный округ	11%	7%	3%	17%	23%	88%	50%	17%
Другие	10%	5%	4%	–	7%	–	17%	17%

Рисунок 2. Компании-респонденты по федеральным округам

1 По данным Федеральной службы государственной статистики за I полугодие 2018 года.

32%
респондентов — государственные организации

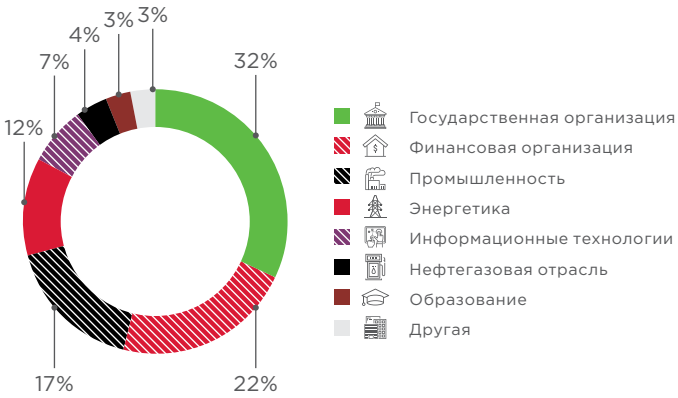
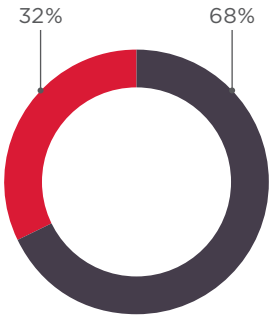


Рисунок 3. Компании-респонденты по сферам деятельности

Более 1000	41%	36%	58%	22%	23%	63%	33%	50%
От 500 до 1000	16%	10%	24%	39%	8%	13%	–	33%
От 100 до 500	18%	28%	12%	17%	46%	12%	50%	17%
Не более 100	25%	26%	6%	22%	23%	12%	17%	–

Рисунок 4. Компании-респонденты по численности штата



Самостоятельная организация	67%	62%	73%	74%	62%	88%	67%	67%
Дочерняя организация	33%	38%	27%	26%	38%	12%	33%	33%

Рисунок 5. Компании-респонденты по степени самостоятельности

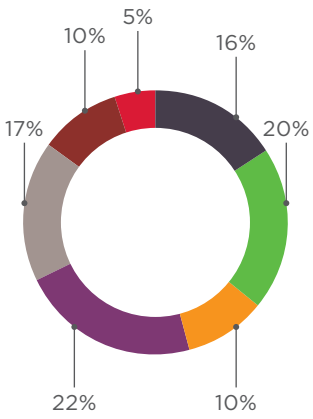
Финансирование

Руководитель ежегодно сталкивается с задачей оптимального формирования бюджета на ИБ. Мы предложили участникам нашего исследования ответить на несколько вопросов, связанных с бюджетированием в их организациях.

Общая проблема регионов — низкий бюджет на ИБ

Анализ показал, что в большинстве региональных компаний бюджет на информационную безопасность довольно низкий. Так, бюджет организаций сферы образования, принявших участие в опросе, в 2018 году не превышает 5 млн рублей. Распространено заблуждение, что образовательные учреждения не нуждаются в сложном комплексе мер защиты и дорогостоящих решениях, поскольку не представляют интереса для серьезных киберпреступников. Недавний инцидент, связанный с утечкой научных разработок в области ядерной физики, служит наглядным примером того, как уникальные исследования могут стать товаром на рынке дарквеба.

Среди участников опроса солидные суммы (более 50 млн рублей) готовы тратить на ИБ только несколько финансовых и государственных организаций. В то же время доля финансовых и государственных организаций с крайне низким бюджетом на ИБ (не более 0,5 млн рублей) достигает 14% и 20% соответственно.



Не более 0,5 млн ₽	20%	14%	6%	26%	15%	–	33%	17%
От 0,5 до 2 млн ₽	21%	10%	24%	13%	15%	38%	50%	33%
От 2 до 5 млн ₽	11%	5%	15%	4%	15%	–	17%	17%
От 5 до 10 млн ₽	16%	19%	27%	35%	31%	25%	–	17%
От 10 до 20 млн ₽	16%	21%	18%	17%	9%	25%	–	16%
От 20 до 50 млн ₽	9%	17%	10%	5%	15%	12%	–	–
Более 50 млн ₽	7%	14%	–	–	–	–	–	–

Рисунок 6. Годовой бюджет компаний-респондентов на ИБ

В прошлом году мы провели исследование, участниками которого стали компании преимущественно Центрального региона из топ-500 крупнейших компаний страны. Согласно его результатам, в 83% опрошенных организаций с численностью штата более 1000 человек бюджет на ИБ составлял не менее 10 млн рублей. Среди региональных компаний в нынешнем году этот показатель существенно ниже: только 47% крупных компаний, в которых работает более 1000 сотрудников, выделили на защиту информационных систем 10 и более млн рублей.

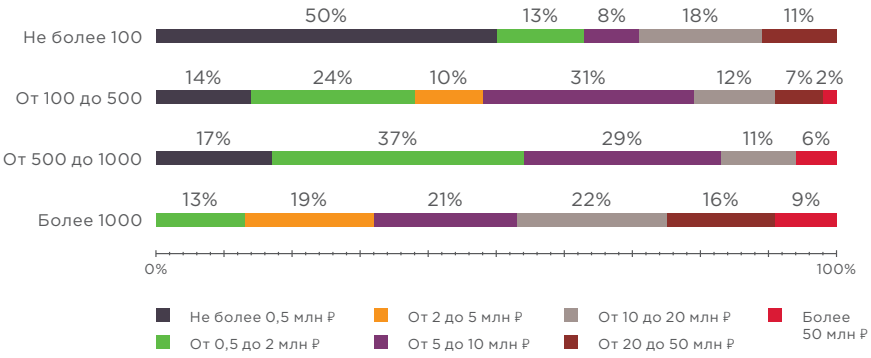


Рисунок 7. Годовой бюджет на ИБ в зависимости от штата организации

Бюджет на ИБ: стратегии планирования

Для планирования бюджета на ИБ распространен простой прием применения коэффициента к бюджету, выделяемому на поддержку IT-инфраструктуры (как правило, до 10%), но не секрет, что существует и другой подход — распределение средств на безопасность по остаточному принципу. Как следствие, не всегда можно однозначно установить, достаточно ли финансовых ресурсов выделяется для создания и поддержания требуемого уровня защиты.

Каждый пятый участник опроса отмечал, что отдельная статья расходов на обеспечение кибербезопасности не предусмотрена: средства на эти нужды выделяются из состава бюджета на информационные технологии. Интересно, что в 20% таких организаций доля бюджета ИБ выше среднего показателя. Представители этих компаний отметили, что на 2018 год запланирована замена устаревших технических средств обеспечения ИБ современными решениями. Дороговизна современных средств защиты информации объясняет значительную долю бюджета ИБ.

21%
компаний-респондентов включают бюджет ИБ в состав бюджета ИТ

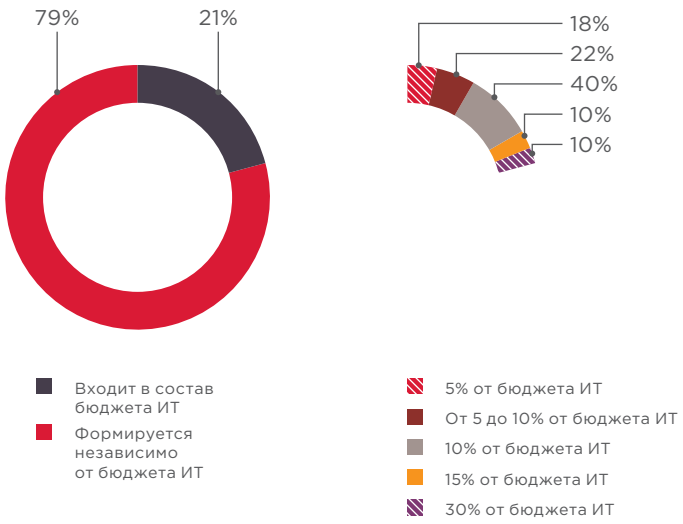


Рисунок 8. Формирование бюджета ИБ

Большинство дочерних компаний
не формируют бюджет на ИБ самостоятельно и в финансовых вопросах обеспечения ИБ зависят от головной компании

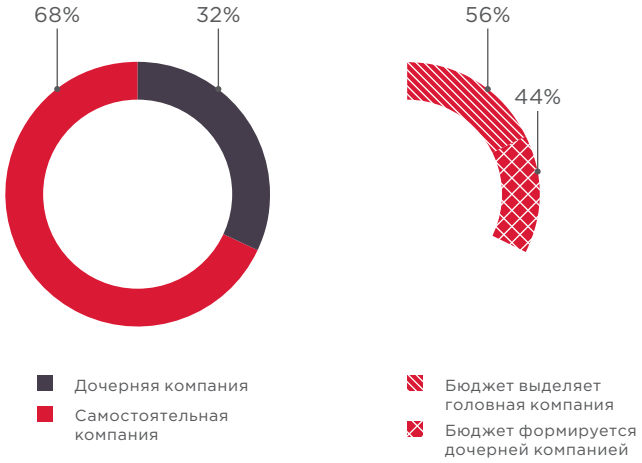
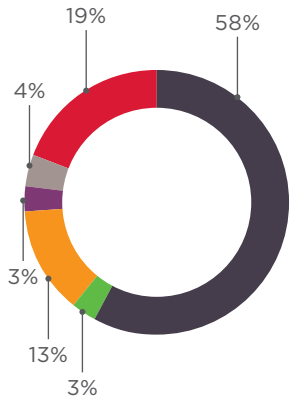


Рисунок 9. Зависимость бюджета от степени самостоятельности

16%
компаний-респондентов столкнулись с сокращением бюджета на ИБ в 2018 году

Сократить нельзя повысить

Более половины респондентов констатируют, что размер бюджета на ИБ не изменился по сравнению с 2017 годом. Рост инвестиций в обеспечение безопасности отмечен в 26% опрошенных компаний.



Остался прежним	59%	62%	58%	65%	46%	50%	50%	33%
Сократился менее чем на 15%	6%	–	–	–	–	–	17%	17%
Сократился более чем на 15%	10%	17%	15%	13%	15%	–	33%	–
Увеличился менее чем на 15%	2%	2%	9%	–	8%	–	–	–
Увеличился более чем на 15%	3%	2%	3%	–	8%	38%	–	–
Увеличился более чем на 50%	20%	17%	15%	22%	23%	12%	–	50%

Рисунок 10. Изменения в объеме бюджета на ИБ в 2018 году по сравнению с 2017 годом

На что потрачен бюджет ИБ в 2018 году

Самой популярной статьей расходов в бюджете на ИБ стала покупка систем защиты информации (и продление лицензий). Менее половины респондентов осознают важность регулярного тестирования корпоративной инфраструктуры на проникновение и готовы выделить в своем бюджете статью расходов на организацию такого тестирования. Компании с бюджетом свыше 20 млн рублей запланировали построение собственного центра оперативного реагирования на угрозы ИБ (security operations center, SOC), при этом они отмечали, что потребуются закупка дополнительного оборудования, внедрение технических средств для мониторинга и реагирования на события ИБ, а также увеличение числа специалистов по защите информации.

48%
компаний-респондентов выделили в своем бюджете средства на внедрение SIEM

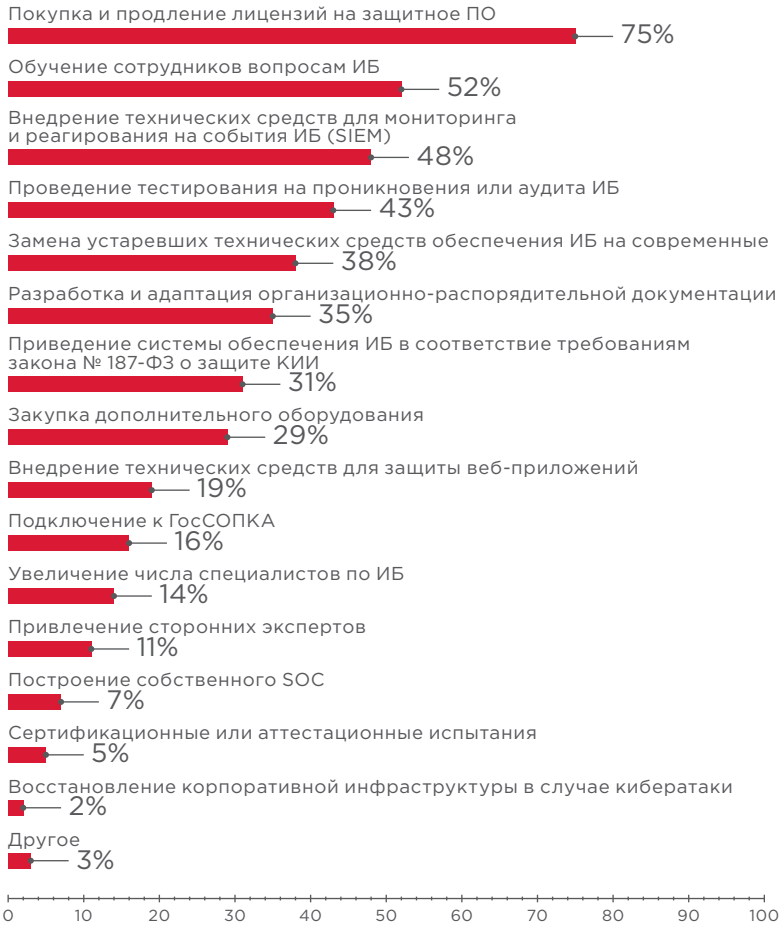
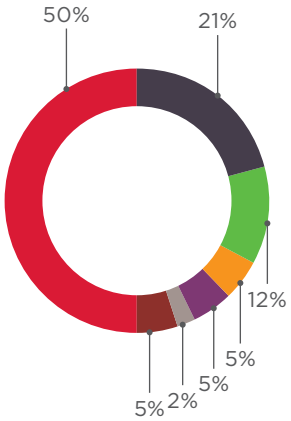


Рисунок 11. Статьи расхода в бюджете на ИБ в 2018 году (доля организаций)

50%
респондентов уверены, что требования закона № 187-ФЗ неприменимы к их организациям

Менее трети организаций запланировали в своем бюджете статью расходов на выполнение требований закона № 187-ФЗ о безопасности критической информационной инфраструктуры. Каждый второй респондент придерживается мнения, что вопросы соответствия требованиям о защите КИИ и методическим рекомендациям о создании ведомственных и корпоративных центров ГосСОПКА неактуальны для компании, которую он представляет. Заметим, что такого мнения придерживается существенная часть государственных организаций, а также более 40% компаний финансовой отрасли. По словам представителя ФСТЭК, по состоянию на конец ноября 2018 года кредитно-финансовые организации входят в число отстающих по числу представленных перечней объектов КИИ. То же можно сказать и о государственных учреждениях. Вполне вероятно, что в бюджеты большинства опрошенных нами госкомпаний не были заложены средства на вопросы защиты КИИ, поскольку многие компании, не имея четких методических рекомендаций по последовательности действий, которые они должны предпринять, боятся зря потратить деньги и занимают выжидательную позицию. Тем не менее в ноябре 2018 года ФСТЭК определила свою позицию по срокам категорирования объектов КИИ: его необходимо завершить до конца 2019 года. Кроме того, стало известно о намерениях ФСБ расширить список компаний, для которых подключение к ГосСОПКА станет обязательным. Ожидается, что требования к категорированию объектов КИИ будут доработаны в первом квартале 2019 года, будут утверждены методические документы по соответствию требованиям. Эти обстоятельства позволяют нам прогнозировать рост бюджетов ряда компаний на информационную безопасность в 2019 году.



Не более 0,5 млн ₽	18%	24%	27%	13%	31%	25%	–	17%
От 0,5 до 2 млн ₽	7%	12%	18%	17%	8%	25%	17%	–
От 2 до 5 млн ₽	–	10%	9%	5%	–	12%	–	16%
От 5 до 10 млн ₽	3%	2%	3%	4%	15%	25%	–	–
Более 10 млн ₽	2%	–	–	5%	8%	13%	–	–
Требуется предварительная оценка	5%	10%	3%	4%	7%	–	–	–
Неприменимо	65%	42%	40%	52%	31%	–	83%	67%

Рисунок 12. Размер бюджета на ИБ, который готовы выделить компании для обеспечения требований по защите КИИ

Меры и средства обеспечения ИБ

Эффективность системы информационной безопасности компании определяется множеством факторов. Ключевую роль играет рациональное распределение ресурсов. Хотя существуют нормативные документы регуляторов в области ИБ, которые определяют состав базовых мер, любая компания может выбирать среди различных инструментов те, которые подходят именной ей. Мы спросили у наших респондентов, какие меры принимаются в их организациях, а также поинтересовались их субъективным мнением по поводу достаточности этих мер.

От отдела ИБ до собственного SOC

24%
финансовых организаций
не проводят регулярных тестов на проникновение

Подразделение ИБ есть в большинстве компаний, принявших участие в опросе. Тесты на проникновение в корпоративную инфраструктуру не реже одного раза в год проводят только 30% опрошенных компаний, в их числе три четверти финансовых организаций. Согласно указанию № 4793-У Центрального банка РФ, с 1 января 2020 года ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры станут обязательными для всех операторов по переводу денежных средств и операторов услуг платежной инфраструктуры.

Чтобы правильно настроить средства защиты, специалистам по защите информации необходимо хорошо разбираться в инфраструктуре, которую они хотят защитить. Корпоративная сеть должна быть прозрачна для системных администраторов и недоступна для злоумышленников, а это требует регулярной инвентаризации сетевых ресурсов и проверки их доступности из интернета. Такие проверки проводятся только в 49% опрошенных компаний.

30%
компаний-респондентов не устанавливают актуальные обновления

Крупный киберинцидент, случившийся в «ПИР Банке»[2], в очередной раз свидетельствует о том, что несвоевременное обновление программного обеспечения может привести к огромным финансовым потерям. В ночь с 3 на 4 июля 2018 года хакеры похитили с корреспондентского счета «ПИР Банка» более 58 миллионов рублей. Преступники получили доступ к IT-системам банка через сетевое устройство, программное обеспечение которого своевременно не обновлялось.

Если подразделение ИБ есть почти в каждой организации, то собственный SOC — только в 6% компаний-респондентов. Несмотря на это мы прогнозируем, что число центров реагирования в ближайшие годы будет расти. Так, в Калининградской области уже началось создание регионального центра безопасности.

Рисунок 13. Организационные меры (доля компаний)

Все используют антивирусы

Антивирусы и межсетевые экраны используются для защиты от кибератак практически во всех компаниях, которые приняли участие в нашем опросе. Несколько менее распространенными средствами являются виртуальные частные сети и системы

2 В настоящий момент лицензия банка отозвана приказом Банка России от 12.10.2018 № ОД-2646.

обнаружения и предотвращения вторжений. Не исключено, что применение этих средств в опрошенных организациях обусловлено стремлением соответствовать государственным или отраслевым нормативам.

Индустрия средств обеспечения безопасности не стоит на месте, и сегодня в распоряжении бизнеса есть много эффективных решений для противодействия киберугрозам. В компаниях, где для выявления кибератак используется система корреляции и консолидации событий безопасности (SIEM-система), применяется не менее пяти средств защиты. Это объясняется тем, что неавтоматизированный мониторинг событий безопасности может быть успешен только до тех пор, пока в компании функционирует небольшое количество средств защиты. Однако с ростом их числа администратору безопасности становится сложно вручную сопоставлять записи системных журналов множества различных систем и делать выводы о взаимосвязи событий и потенциальных инцидентах ИБ. Как следствие, компания выделяет ресурсы на приобретение системы класса SIEM, которая позволяет выявлять инциденты безопасности автоматически. Стоит отметить, что треть всех компаний, использующих SIEM, составляют финансовые организации. Это неудивительно, поскольку хакерские атаки на финансовый сектор с каждым годом становятся все более сложными и распределенными во времени. Согласно отчету Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ), типовая схема целевой атаки на кредитную организацию с использованием ПО Cobalt Strike включает восемь последовательных этапов. Финальным этапом практически любой целевой атаки является сокрытие ее следов. Без использования специализированных средств мониторинга событий информационной безопасности стало невозможно вовремя обнаружить и предотвратить атаки, которые могут повлечь большие финансовые потери.

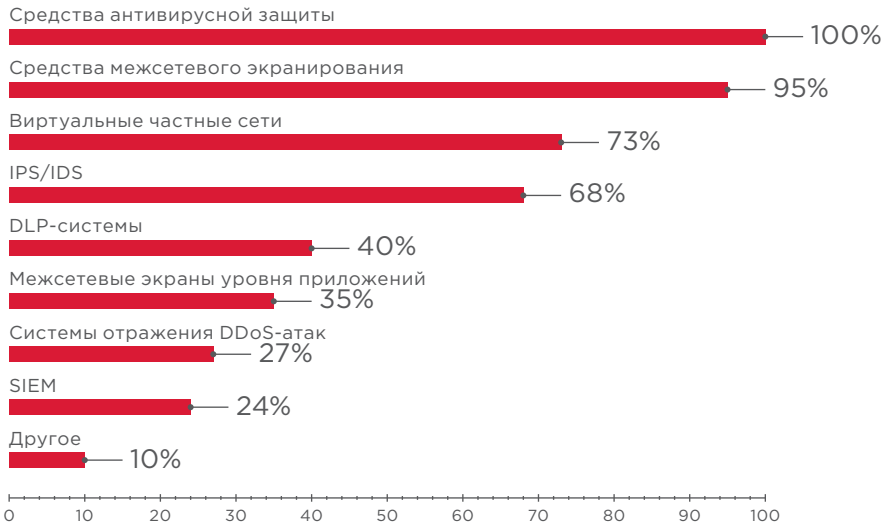
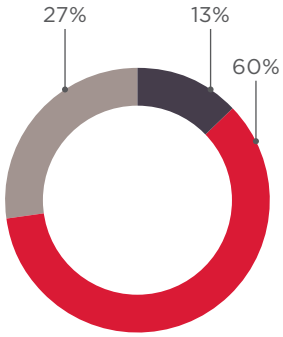


Рисунок 14. Технические средства защиты информации (доля компаний)

Достаточно ли этих мер защиты?

Кибербезопасность названа одним из приоритетных направлений национального проекта «Цифровая экономика», целью которого является внедрение информационных технологий во все сферы экономики государства. В 2018 году на реализацию первоочередных мероприятий проекта из федерального бюджета направлено более 3 млрд рублей, из которых около 364 млн — на направление «Информационная безопасность», что составляет 17% от бюджета ИТ и 12% от общего объема государственных инвестиций в проект в 2018 году. В то же время большинство участников нашего опроса были вынуждены признать, что применяемых в их организациях мер защиты недостаточно. Более того, 34% государственных организаций отмечают, что руководство не выделяет необходимые средства на кибербезопасность.



Применяемых мер достаточно	15%	10%	12%	13%	23%	12%	17%	–
Мер недостаточно, но компания выделяет бюджет	51%	71%	67%	48%	62%	63%	50%	83%
Мер недостаточно, и компания не выделяет необходимые средства	34%	19%	21%	39%	15%	25%	33%	17%

Рисунок 15. Эффективность мер защиты (по мнению респондентов)

87%
компаний-респондентов считают, что применяемых мер защиты недостаточно

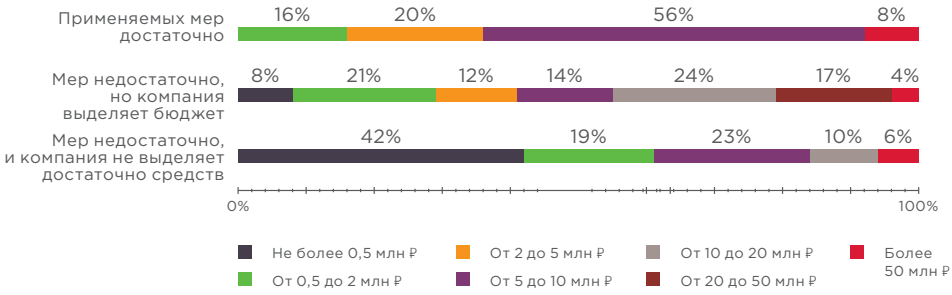


Рисунок 16. Эффективность мер защиты в зависимости от выделяемого бюджета (по мнению респондентов)

Готовность к реагированию на кибератаки

20%
компаний-респондентов не отслеживают киберинциденты

Для эффективного противодействия кибератакам чрезвычайно важно вовремя обнаружить надвигающуюся угрозу и предпринять оперативные действия по ее предотвращению. Необходимо регистрировать все события информационной безопасности, чтобы упростить задачу расследования инцидента, если он будет иметь место. К сожалению, не во всех компаниях, принявших участие в опросе, есть такая практика. Анализировать инциденты и принимать меры по реагированию на них готова только половина опрошенных компаний.

Инциденты регистрируются, классифицируются и принимаются меры по реагированию на них	47%	60%	58%	35%	54%	50%	33%	66%
Инциденты регистрируются	25%	26%	36%	35%	38%	38%	17%	17%
Инциденты не выявляются	28%	14%	6%	30%	8%	12%	50%	17%

Рисунок 17. Выявление инцидентов кибербезопасности (доля респондентов)

Каждая вторая компания становилась жертвой кибератак

Бывают ситуации, когда компании требуется провести анализ событий ИБ за определенный промежуток времени в прошлом (так называемый ретроспективный анализ), чтобы выявить пропущенные инциденты. Как показывает наш опыт, в ходе такого анализа в большинстве случаев специалистам удается обнаружить следы присутствия злоумышленника в инфраструктуре. В то же время, согласно нашей статистике, только в 2 из 100 тестов на проникновение действия специалистов по анализу

82%
компаний-респондентов подвергались кибератакам

защищенности бывают обнаружены сотрудниками подразделений ИТ и ИБ заказчика. Поэтому у нас есть все основания полагать, что 18% компаний-респондентов, которые отметили, что не столкнулись с кибератаками за последний год, просто могли вовремя их не обнаружить.

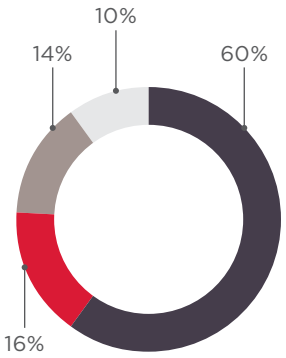
Не было выявлено атак	21%	14%	12%	18%	24%	25%	34%	17%
Не было выявлено успешных атак	33%	41%	36%	39%	38%	–	33%	33%
Были успешные атаки	46%	45%	52%	43%	38%	75%	33%	50%

Рисунок 18. Выявление атак

Только 43% предприятий сферы энергетики отметили, что столкнулись с успешными кибератаками. Однако истинное положение дел может быть иным, поскольку 30% респондентов из той же сферы энергетики признались, что практика выявления инцидентов в их компаниях отсутствует вовсе. В то же время такие компании представляют огромный интерес для злоумышленников. Летом 2018 года эксперты из Cybereason провели эксперимент, разместив в интернете приманку — поддельную электрическую подстанцию. Исследователям было интересно оценить, как скоро хакеры предпримут попытки ее взлома. В результате хакеры взломали инфраструтуру поддельной электрической станции в течение двух суток, а еще через несколько дней уже пытались продать полученную информацию в дарквебе. Возможно, компании-респонденты, не зафиксировавшие атак, имеют недостаточно технических средств для обнаружения вторжений.

88%
компаний-респондентов, не зафиксировавших атаки, не используют SIEM

К помощи сторонних специалистов для расследования инцидентов обращались только 16% организаций. Бюджет на информационную безопасность в большинстве этих организаций превышает 10 млн рублей.



Расследование проводилось своими силами	52%	66%	76%	40%	69%	37%	67%	83%
К расследованию привлекались сторонние эксперты	20%	14%	12%	17%	15%	38%	–	–
Отсутствует практика выявления и расследования инцидентов ИБ	21%	10%	6%	17%	8%	13%	33%	–
Сторонние эксперты не привлекались: компания не подвергалась кибератакам	7%	10%	6%	26%	8%	12%	–	17%

Рисунок 19. Привлечение сторонних специалистов к расследованию кибератак

Фишинг и ВПО: почему антивирус не сработал?

Что касается видов кибератак, то чаще всего организации сталкивались с попытками заражения рабочих станций сотрудников и серверов различным вредоносным программным обеспечением (шифровальщиками, майнерами и т. п.): доля таких компаний составила 60%. Более трети респондентов не смогли отразить атаки и предотвратить заражение своих ресурсов, несмотря на использование антивирусного программного обеспечения. Это неудивительно, ведь в первом полугодии 2018 года в мире появилось около 2,4 миллиона новых экземпляров вредоносного ПО.

Их разнообразие и сложность поражает. Так называемые бесфайловые, или бестелесные вирусы, которые выполняются в оперативной памяти компьютера, сделали сигнатурный анализ неэффективным в борьбе с вредоносным ПО. Все чаще традиционные средства защиты позволяют обнаружить атаку только тогда, когда уже наступили ее последствия. Поэтому необходим комплекс решений, позволяющий выявлять атаки на ранних стадиях, как только злоумышленники попытались сломать периметр защиты. Это означает, что в современном киберпространстве для защиты своего бизнеса от воздействия вредоносного ПО пришла пора использовать антивирусные решения нового поколения, которые включают сразу несколько антивирусных «движков» и способны проверять все потоки информации в инфраструктуре (в почтовом и сетевом трафике, в файловых хранилищах, на веб-порталах), а также анализировать подозрительные программы посредством их выполнения в ограниченной среде.

Фишинг занимает второе место по популярности среди атак, которым подверглись опрошенные компании, — с ним столкнулись 57% респондентов. Это неудивительно, поскольку фишинг является самым простым и в то же время эффективным способом доставки вредоносного программного обеспечения на рабочие станции и серверы. А значит, любая организация кредитно-финансового сектора может стать жертвой преступной группировки Cobalt, возобновившей свои действия в мае 2018 года. Эта волна атак отличилась особой изобретательностью: письма с вредоносными вложениями рассылались от имени антивирусной компании и Европейского центробанка.

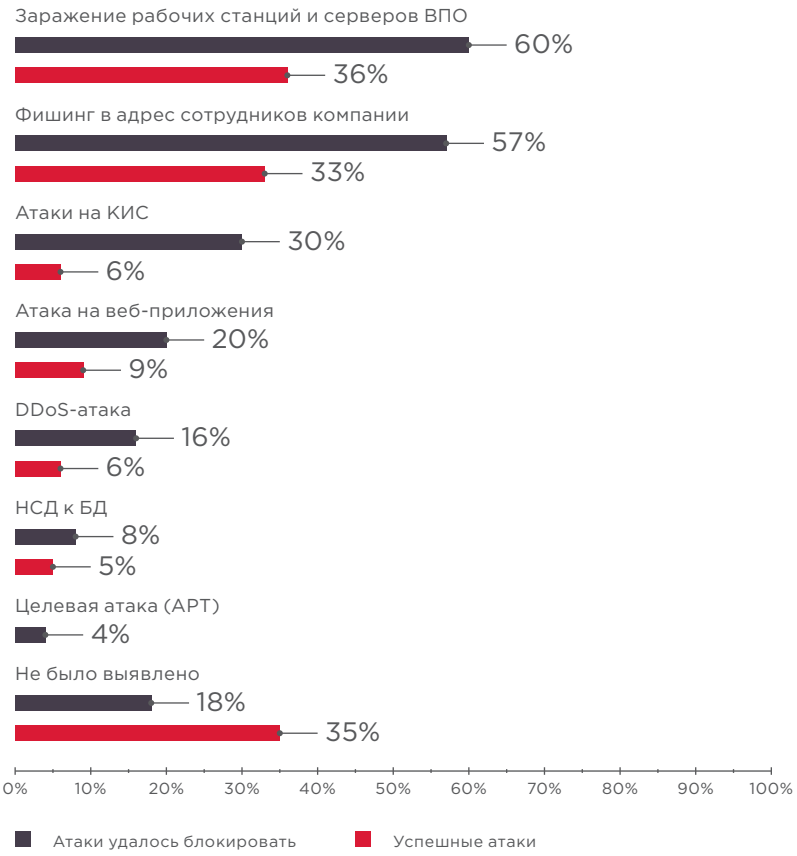


Рисунок 20. Кибератаки, с которыми столкнулись участники опроса (указана доля компаний)

Человеческий фактор всему виной

Более половины респондентов полагают, что причиной успеха кибератаки может быть неосведомленность персонала в вопросах информационной безопасности, немного меньше респондентов отметили непреднамеренные действия сотрудников. Нам остается только надеяться, что в будущем влияние человеческого

фактора на количество успешных кибератак снизится. Согласно плану мероприятий по направлению «Информационная безопасность» в рамках программы «Цифровая экономика», доля граждан, повысивших грамотность в сфере информационной безопасности, является одним из индикаторов эффективности мероприятий программы. Так, к 2024 году этот показатель должен достичь 50%. Кроме того, в 2019 году планируется рассмотреть возможность включения дисциплины по информационной безопасности в WorldSkills Russia, и это должно способствовать росту числа специалистов в области ИБ на рынке труда, что актуально для многих организаций, ведь каждый четвертый респондент отметил дефицит квалифицированных специалистов в качестве одной из возможных причин успеха кибератак.

Большая часть компаний не видит угрозы в инсайдерах. Возможно, роль инсайдера в хищении и уничтожении информации недооценена, подтверждением тому служит множество примеров. Так, летом 2018 года прокуратура Новосибирска отправила в суд уголовное дело против менеджера оператора мобильной связи, который, имея доступ к специализированному ПО, совершал мошеннические действия и воровал деньги со счетов клиентов сотовой компании. Подобные инциденты могут стать сильным ударом по репутации организации. Не стоит забывать, что зачастую инсайдерами движет не финансовая мотивация, а обида или желание отомстить. В августе 2018 года стало известно, что замдиректора одной из ульяновских школ из мести начальству на протяжении длительного периода времени удалял электронные документы, связанные с деятельностью учебного заведения, в том числе бухгалтерскую отчетность и персональные данные учащихся.

Как следствие использования преимущественно базовых средств защиты можно отметить, что 57% опрошенных компаний считают причиной успеха кибератак отсутствие или неэффективность средств защиты.

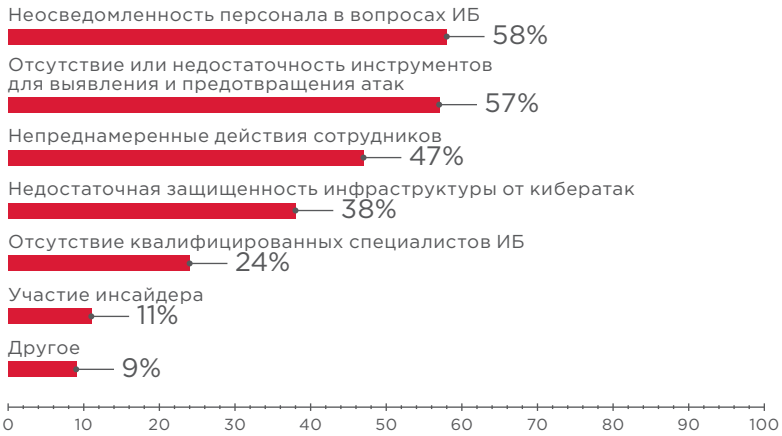
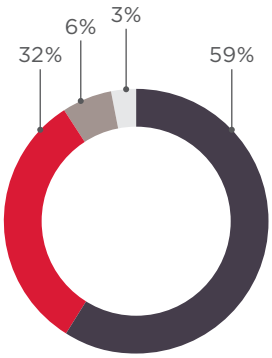


Рисунок 21. Причины успеха кибератак (по мнению той или иной доли респондентов)

59%
компаний-респондентов не раскрывают информацию о кибератаках

Легко ли учиться на чужих ошибках?

Большинство организаций, раскрывающих информацию о произошедших у них инцидентах, ограничиваются сообщениями в адрес регулятора и не сообщают об атаках своим клиентам и партнерам. Стоит отметить, что 21% финансовых организаций не раскрывают информацию о произошедших нападениях хакеров. Однако с 1 июля 2018 года операторы по переводу денежных средств и операторы платежной инфраструктуры обязаны сообщать о них в ФинЦЕРТ Банка России. Соответствующие правки внесены указанием № 4793-У в положение № 382-П. Организации, не раскрывающие информацию о киберинцидентах, скорее всего, опасаются возможных санкций со стороны регуляторов. Видимо, некоторые компании полагают, что после оглашения информации об успешных кибератаках, совершенных против них, будет подорвана их репутация и утеряно доверие клиентов.



Информация о кибератаках не раскрывается	69%	21%	73%	74%	62%	50%	66%	83%
Информация передается регулятору	25%	71%	18%	22%	15%	12%	17%	17%
Информация передается регулятору, клиентам и партнерам	5%	5%	6%	4%	–	38%	17%	–
Информация передается партнерам или клиентам компании	1%	3%	3%	–	23%	–	–	–

Рисунок 22. Раскрытие информации о кибератаках

Каждая третья компания понесла прямые финансовые потери от кибератак

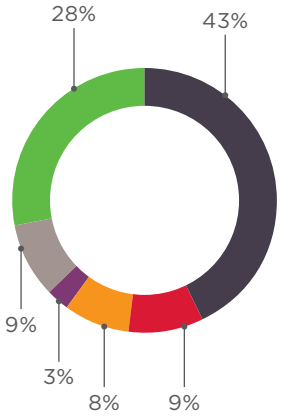
Прямые финансовые потери от кибератак понесли 32% участников опроса. Каждая четвертая компания пострадала от простоя инфраструктуры, в том числе 30% промышленных компаний. Простой инфраструктуры является, пожалуй, одним из самых опасных последствий кибератак для промышленных предприятий. Летом 2018 года разновидность вредоносного ПО WannaCry на три дня парализовала работу нескольких заводов по производству iPhone. Как отмечают эксперты, подобный инцидент может привести к задержкам поставок и росту цен.

Более 40% респондентов отметили, что не столкнулись с последствиями кибератак. Но давно не секрет, что киберпреступники зачастую организуют «пробные» атаки, после которых некоторое время не проявляют активности, или совершают взломы без кражи денег либо информации. Это может оказаться своего рода подготовкой к более серьезной атаке.

Рисунок 23. Последствия кибератак (доля респондентов)

Финансовый ущерб от кибератак для большинства организаций составил не более 500 тысяч рублей. Отметим, что это значение сравнимо со средним показателем финансовых потерь от кибератак в 2017 году. Согласно отчету Национального агентства финансовых исследований, средняя сумма убытков в одной российской компании в 2017 году составила около 300 тысяч рублей, в крупном бизнесе — почти 900 тысяч. Отдельно стоит остановиться на финансово-кредитном секторе. Треть финансовых организаций, принявших участие в опросе, не понесли потерь

от кибератак, еще треть участников опроса из финансовой отрасли отметили, что потери составили не более 500 тысяч рублей. Это довольно хорошие показатели для банков. Как отмечает ФинЦЕРТ, в 2018 году потери кредитных организаций от кибератак снизились: за восемь месяцев в 2018 году банки потеряли всего 76,5 млн рублей, в то время как за аналогичный период годом ранее — более 1 млрд рублей. Однако здесь справедливо будет отметить, что объем активов региональных банков в десятки раз отличается от объемов активов банков в Центральном регионе. Так, например, средний объем активов одного банка в Сибирском федеральном округе составляет 9 млрд рублей, в то время как для Центрального округа данный показатель составляет почти 237 миллиардов[3]. Ущерб от кибератак в 10–20 млн рублей, который понесли 3% наших респондентов из финансовой отрасли, мог стать довольно ощутимым, поскольку он сопоставим, например, со средней месячной прибылью банка в Сибирском федеральном округе[4]. Кроме того, известно множество случаев, когда финансовые потери банка от одной кибератаки превышали средний показатель в сотни и даже тысячи раз.

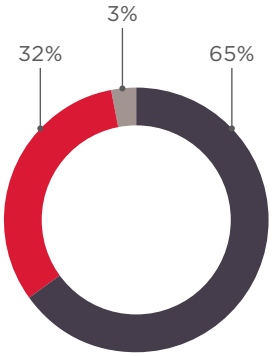


Не более 0,5 млн ₽	46%	33%	37%	39%	47%	75%	67%	66%
От 0,5 до 2 млн ₽	10%	7%	12%	5%	15%	13%	–	–
От 5 до 10 млн ₽	3%	14%	6%	4%	15%	12%	–	17%
От 10 до 20 млн ₽	2%	3%	9%	5%	–	–	–	–
Неизвестно	11%	10%	9%	4%	8%	–	–	17%
Без финансового ущерба	28%	33%	27%	43%	15%	–	33%	–

Рисунок 24. Финансовый ущерб от кибератак

Вернуться на круги своя за один день

Большинство компаний-респондентов уверены, что смогут устранить последствия кибератаки в течение суток. Однако мы склонны полагать, что эта оценка чрезмерно оптимистична. Расследование инцидента, связанного с кражей финансовых средств в банке, может занимать несколько недель. Если в результате кибератаки будут уничтожены важные данные (например, база клиентов или финансовая отчетность), то на их восстановление может потребоваться несколько дней даже при наличии резервных копий. Напомним, что в случае отсутствия резервных копий восстановить зашифрованные программой-шифровальщиком данные практически невозможно, а на восстановление репутации может потребоваться весьма длительный период.



Не более суток	72%	74%	55%	74%	54%	38%	33%	50%
От 1 до 3 дней	26%	26%	42%	26%	38%	62%	17%	50%
От 3 до 10 дней	2%	–	3%	–	8%	–	50%	–

Рисунок 25. Время на устранение последствий кибератаки

3 Рассчитано согласно данным рейтинга российских банков по объемам активов на 1 августа 2018 года (статистика ЦБ РФ).

4 Рассчитано согласно данным портала banki.ru по показателю «Чистая прибыль» за август-сентябрь 2018 года.

Ключевые особенности регионов

В этом разделе мы кратко охарактеризуем респондентов из четырех округов, которые приняли наиболее активное участие в опросе.

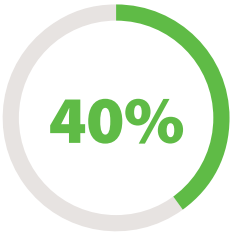
Приволжский федеральный округ

ПФО лидирует в нашем опросе по количеству государственных организаций: это 33% от общего числа респондентов и 37% от числа респондентов в округе. Средний бюджет ИБ находится в диапазоне от 5 до 10 млн рублей. Более 50 млн на вопросы кибербезопасности готовы выделять только 6% респондентов ПФО, в их число вошли в основном крупные государственные компании и организации финансовой отрасли со штатом более 1000 человек.

участников опроса полагают, что применяемых в их организациях мер защиты от кибератак недостаточно

опрошенных компаний столкнулись с кибератаками

Каждый третий респондент считает, что руководство не выделяет достаточно средств для обеспечения эффективных мер защиты



государственных организаций, принявших участие в опросе, считают причиной успеха кибератак отсутствие или недостаточность инструментов для их выявления и предотвращения

Государственные системы — излюбленная мишень киберпреступников

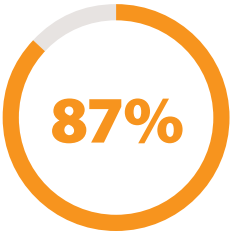
В июле 2018 года в Уфе был вынесен приговор злоумышленнику, который летом прошлого года пытался взломать сайты официальных ведомств Пермского края и Республики Татарстан.

В августе 2018 года сотрудникам УФСБ России по Кировской области удалось установить личность человека, который в ноябре 2017 года, используя ВПО, совершил кибератаку на информационные ресурсы Министерства экономического развития РФ с целью хищения информации. Им оказался 17-летний юноша.

Уральский федеральный округ

Большинство респондентов УФО (61%) — крупные организации с численностью штата более 1000 человек. Почти треть (30%) респондентов представляют финансовый сектор, высока также доля промышленных организаций — 21% от числа респондентов УФО и 39% от общего числа промышленных компаний, принявших участие в опросе. По результатам нашего исследования УФО признан округом с самыми высокими бюджетами ИБ: в 52% компаний он превысил 10 млн рублей, в основном это государственные и финансовые организации.

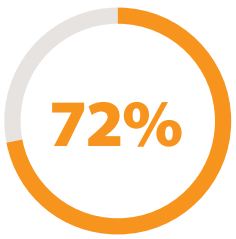
Каждая пятая компания
столкнулась с сокращением бюджета на ИБ в 2018 году



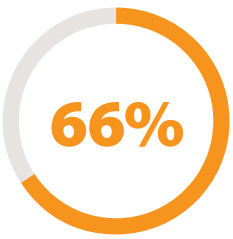
опрошенных компаний
столкнулись с кибератаками

компаний-респондентов
пострадали от простоя инфраструктуры в результате кибератак

компаний-респондентов
понесли прямые финансовые потери от кибератак



компаний-респондентов
не используют SIEM



компаний-респондентов
не используют WAF

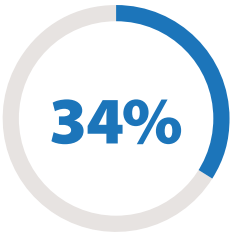
Финансовые потери от кибератак могут быть огромными

В августе 2018 года стало известно, что в Генеральной прокуратуре РФ утвердили обвинительное заключение по уголовному делу в отношении двух жителей Екатеринбурга, которые с помощью вредоносного ПО похитили со счетов клиентов различных банков в общей сложности 1,2 млрд рублей. Кроме того, используя ВПО, они получили доступ к базе данных аэропорта «Кольцово».

Сибирский федеральный округ

В СФО сосредоточены 88% нефтегазовых предприятий и половина всех образовательных учреждений, принявших участие в опросе. Большинство нефтегазовых компаний (57%) имеют более 1000 сотрудников в штате. Кроме того, крупные предприятия с численностью штата более 1000 человек есть среди государственных и промышленных организаций, а также среди IT-компаний. В то же время СФО — это регион с самыми низкими бюджетами ИБ среди участников нашего опроса. Впрочем, можно надеяться на положительную динамику, поскольку с сокращением бюджета на ИБ по сравнению с 2017 годом столкнулись только 3% всех респондентов СФО, у остальных бюджет не изменился либо увеличился. Но в 2018 году от 20 до 50 млн рублей готовы инвестировать в информационную безопасность только по одной компании из государственного сектора, нефтегазовой отрасли, энергетики и промышленности.

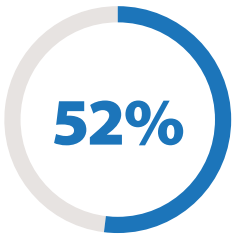
Более 500 000 ₽
составляют прямые финансовые потери от кибератак каждой четвертой организации



опрошенных компаний
имеют бюджет на ИБ менее 500 000 ₽

участников опроса
не выявляют кибератаки

опрошенных компаний
в случае кибератаки проводят расследования своими силами



компаний-респондентов
испытывают недостаток квалифицированных специалистов в области защиты информации

Кадровые вопросы по-прежнему не решены
Согласно перечню, размещенному на официальном сайте ФСТЭК, в Сибирском федеральном округе насчитывается 13 организаций, реализующих согласованные с регулятором образовательные программы в сфере ИБ. Для сравнения отметим, что в Центральном федеральном округе таких организаций 40

Дальневосточный федеральный округ

Большинство организаций ДФО — это государственные и промышленные учреждения (соответственно 31% и 28% от числа респондентов), и только в таких организациях работает более 1000 человек. Большинство компаний-респондентов ДФО — предприятия среднего бизнеса: 61% компаний имеет до 500 человек в штате. Возможно, этим объясняются довольно низкие бюджеты на ИБ: в 75% компаний-респондентов ДФО бюджет составил менее 10 млн рублей.

опрошенных компаний
не раскрывают информацию
о кибератаках

участников опроса
уверены, что устранят
последствия кибератаки
в течение суток

компаний-респондентов
не проводят регулярное обучение
сотрудников по вопросам ИБ

участников опроса,
столкнувшихся с успешными
атаками, подверглись санкциям
регуляторов в области ИБ

Боязнь санкций — одна из причин сокрытия информации о кибератаках

Первого апреля 2018 года хакерской атаке подверглось агентство продажи билетов на самолеты в Комсомольске-на-Амуре. Компьютеры сотрудников оказались заблокированы трояном-шифровальщиком, злоумышленники требовали 30 000 рублей за восстановление доступа к системе. В результате оказалась недоступной информация о лицах, приобретавших авиабилеты, в том числе по льготной стоимости, подлежащая хранению в течение трех лет. При невозможности подтверждения по запросу авиаперевозчиков в течение данного срока сведений о пассажирах, приобретавших билеты, на агентство могут быть наложены штрафные санкции.

Выводы

Результаты исследования показывают, что уровень защищенности региональных организаций в нашей стране крайне низок. Большинство компаний-респондентов (82%) стали мишенью для хакеров в 2018 году. Треть респондентов отмечает прямые финансовые потери от кибератак. Убытки особенно остро ощущаются в связи с довольно скромными бюджетами на ИБ в большинстве опрошенных организаций. Инвестиции в информационную безопасность каждой второй компании не превышают 5 млн рублей. В связи с этим многие используют только базовые средства защиты. Солидные суммы на обеспечение информационной безопасности в 2018 году выделили всего несколько предприятий, принявших участие в нашем опросе, однако и они подвергались успешным атакам. Как следствие, почти все респонденты (87%) не удовлетворены уровнем защищенности своих компаний, а 27% отмечают, что руководство не выделяет необходимых средств.

Если рассмотреть наиболее распространенные уязвимости, которые мы выявляем ежегодно в рамках тестов на проникновение, можно сделать вывод, что большинство из них могут быть устранены в случае применения базовых принципов защиты информации. Все эти принципы учтены и в требованиях регуляторов в области ИБ. Поэтому мы рекомендуем, вне зависимости от величины бюджета компании, в первую очередь убедиться, что требования нормативных документов выполняются в должном объеме.

На практике во многих региональных организациях не хватает средств на реализацию всех мер, предусмотренных нормативной базой. Что же делать руководителю бизнеса в таких обстоятельствах? В условиях ограниченности бюджета мы советуем выделить наиболее ценные активы и обеспечить их комплексную защиту. Кроме того, важно помнить, что слабым звеном в защите информации по-прежнему остается человек. Большинство респондентов признают, что причиной успеха кибератак может быть неосведомленность сотрудников в вопросах информационной безопасности. Руководителям бизнеса необходимо прививать своим сотрудникам культуру информационной безопасности.

В целом же руководителям компаний при распределении бюджета на ИБ необходимо помнить, что система защиты не может быть надежной без трех ключевых составляющих — защитных мер, технических средств и людей. Другими словами, регулярное тестирование на проникновение и инвентаризация ресурсов должны выполняться в комплексе с мониторингом инцидентов безопасности, ретроспективным анализом системных событий и непрерывной защитой веб-приложений и серверов. И конечно, необходимы квалифицированные кадры, дефицит которых в регионах ощущается в разы сильнее, чем в Центральном округе. Нехватку специалистов по защите информации отметил каждый четвертый участник опроса. Это объясняется недостатком комфортных экономических условий для жизни и работы молодых специалистов в регионах, что вынуждает их искать работу ближе к столице. Если в компании нет выделенного подразделения ИБ, стоит рассмотреть возможность делегирования части задач сторонним специалистам, имеющим соответствующие лицензии.

Противостоять преступникам крайне сложно без понимания их методов. В различных отраслях экономики уже сегодня активно развиваются центры обмена информацией и реагирования на инциденты, которые позволяют участникам своевременно узнавать о новейших трендах кибератак именно в этой отрасли, совместно вырабатывать наиболее эффективные способы противодействия. Грамотная стратегия кибербезопасности в эпоху цифровой экономики стала залогом экономической стабильности и конкурентоспособности бизнеса.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. 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.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

Regional Information Security_A4.RUS.0008.05.JAN.09.2018