КОД БЕЗОПАСНОСТИ

Защита корпоративных сетей в России – 2017

Аналитическое исследование
Ноябрь 2017 г.

Содержание

Резюме 3

Аннотация 3

Методика сбора данных и анализа 4

Респонденты 4

Характеристика сети 5

- Корпоративные сети передачи данных 5
- Организация доступа пользователей к информационным системам 6
- Пропускная способность каналов связи 6
- Использование резервного канала связи 9
- Кто отвечает за сетевую безопасность 9
- Классификация информационных систем российских компаний 11

Угрозы для корпоративных сетей 12

- Централизованная система мониторинга ИБ (SIEM) 14

Защита корпоративных сетей 15

- Бюджет на сетевую безопасность 15
- Потребность в обучении персонала, отвечающего за ИБ 15
- Приоритетные требования к средствам сетевой безопасности 16

Заключение 18

Резюме

- Приоритетными требованиями к средствам сетевой безопасности CIO и ИБ-специалисты назвали стабильность работы и качественную техническую поддержку; централизованное управление и мониторинг состояния продуктов; российское происхождение продукта (соответствие политике импортозамещения).
- ИБ-специалисты **каждой второй** компании обеспокоены атаками на рабочие станции с использованием внешнего носителя в обход внешнего периметра сети.
- В среднем российские компании используют решения **трех вендоров** для обеспечения сетевой безопасности.
- **У половины** российских компаний нет подразделения, отвечающего за сетевую безопасность.
- Удаленный доступ к информационным системам с помощью ноутбуков, планшетов и смартфонов используют **44% крупных** компаний.
- **Меньше чем у четверти** российских компаний внедрена централизованная система мониторинга ИБ (SIEM).
- На защиту корпоративных сетей компании в среднем выделяют **11% из ИТ-бюджета**.
- Для оптимизации затрат на построение системы защиты организации стремятся снизить уровень классификации информационных систем.
- **Для 76%** российских компаний важен вопрос обучения персонала, отвечающего за информационную безопасность.

АННОТАЦИЯ

Корпоративные сети являются неотъемлемой частью инфраструктуры современных компаний. Важная информация, включая конфиденциальную, передается по корпоративной сети. Темпы развития и масштабы кибератак продолжают расти. В 2017 году ландшафт угроз стал более сложным. Обеспечение безопасности информации, передаваемой по корпоративной сети, – одна из самых острых проблем, стоящих перед организациями любых отраслей и масштабов.

Аналитики компании «Код Безопасности» провели исследование, в фокусе экспертов были следующие цели:

- Дать характеристику российских корпоративных сетей в отраслевом разрезе.
- Выявить наиболее актуальные угрозы для корпоративных сетей российских компаний.
- Оценить необходимость усиления мер обеспечения безопасности корпоративных сетей.

Методика сбора данных и анализа

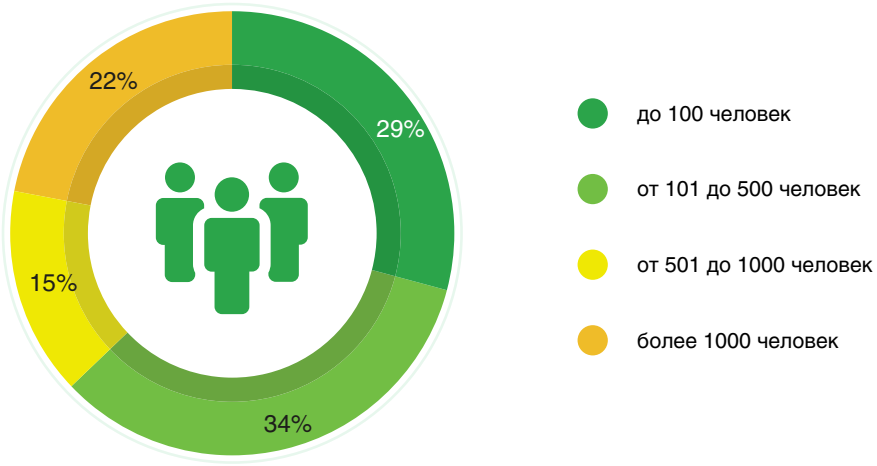
Исследование проводилось по России. Использовался количественный метод в форме онлайн-опроса на сайте компании «Код Безопасности» (www.securitycode.ru) и опросов на офлайн-мероприятиях. В исследование вошли ответы 200 специалистов по информационной безопасности 10 отраслей: госсектор; здравоохранение; ИТ; образование; промышленность; строительство; телекоммуникации; топливно-энергетический комплекс; услуги; финансы.

Для сравнительного анализа подхода к выбору средств обеспечения сетевой безопасности, помимо ответов ИБ-специалистов, в отчет вошли данные, полученные от 400 ИТ-респондентов – руководителей ИТ-служб, зарегистрированных на портале сообщества ИТ-директоров Global CIO.

При обработке полученных результатов компании были классифицированы по численности сотрудников на малые (до 100 чел.), средние (от 101–1000 чел.) и крупные (более 1000 чел.).

РЕСПОНДЕНТЫ

Распределение респондентов по размеру компании

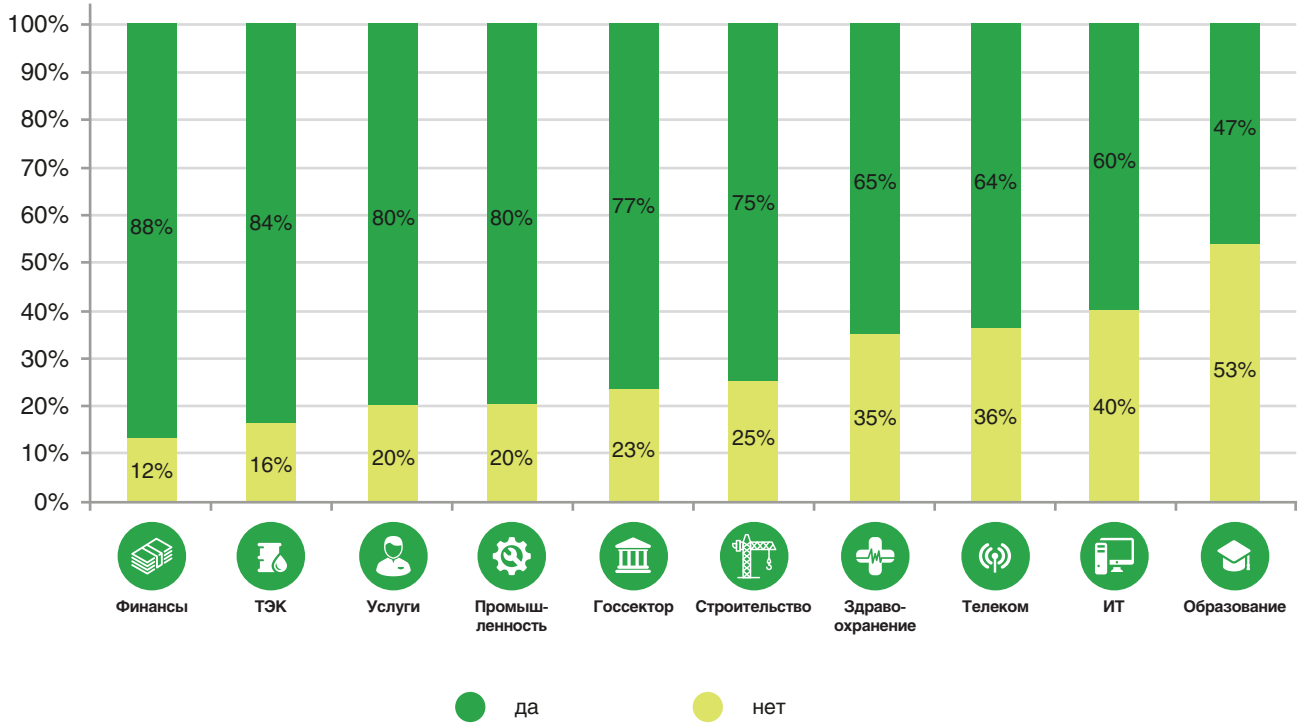


Характеристика сети

Корпоративные сети передачи данных

Для предприятия любого масштаба решение задачи быстрого и надежного обмена данными становится все более актуальным. С каждым днем объем информации, передаваемой внутри организации, увеличивается (особенно если офисы находятся на значительном расстоянии друг от друга).

Наличие филиалов, объединенных сетью передачи данных



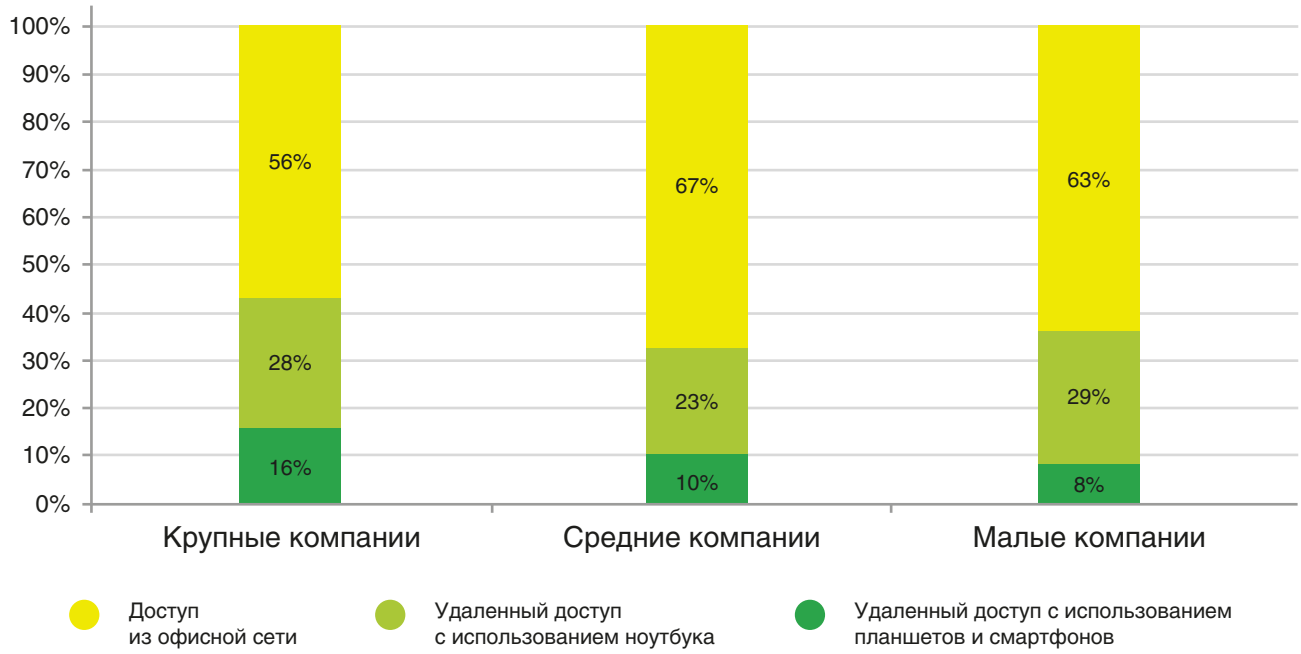
Во всех отраслях корпоративная сеть, как правило, является территориально распределенной. В среднем данный показатель составляет более 75%. Лишь образование характеризуется наименьшей долей организаций (47%), где филиалы объединены сетью передачи данных.

Организация доступа пользователей к информационным системам

Для повышения оперативности решения задач, увеличения производительности работников и эффективности процессов все больше компаний прибегают к удаленному доступу, хотя не для всех отраслей это одинаково актуально. Как показывают результаты исследования, чем крупнее организация, тем чаще ее сотрудники используют устройства удаленного доступа (планшеты, ноутбуки, смартфоны).

Характеристика сети

Организация доступа к ИС



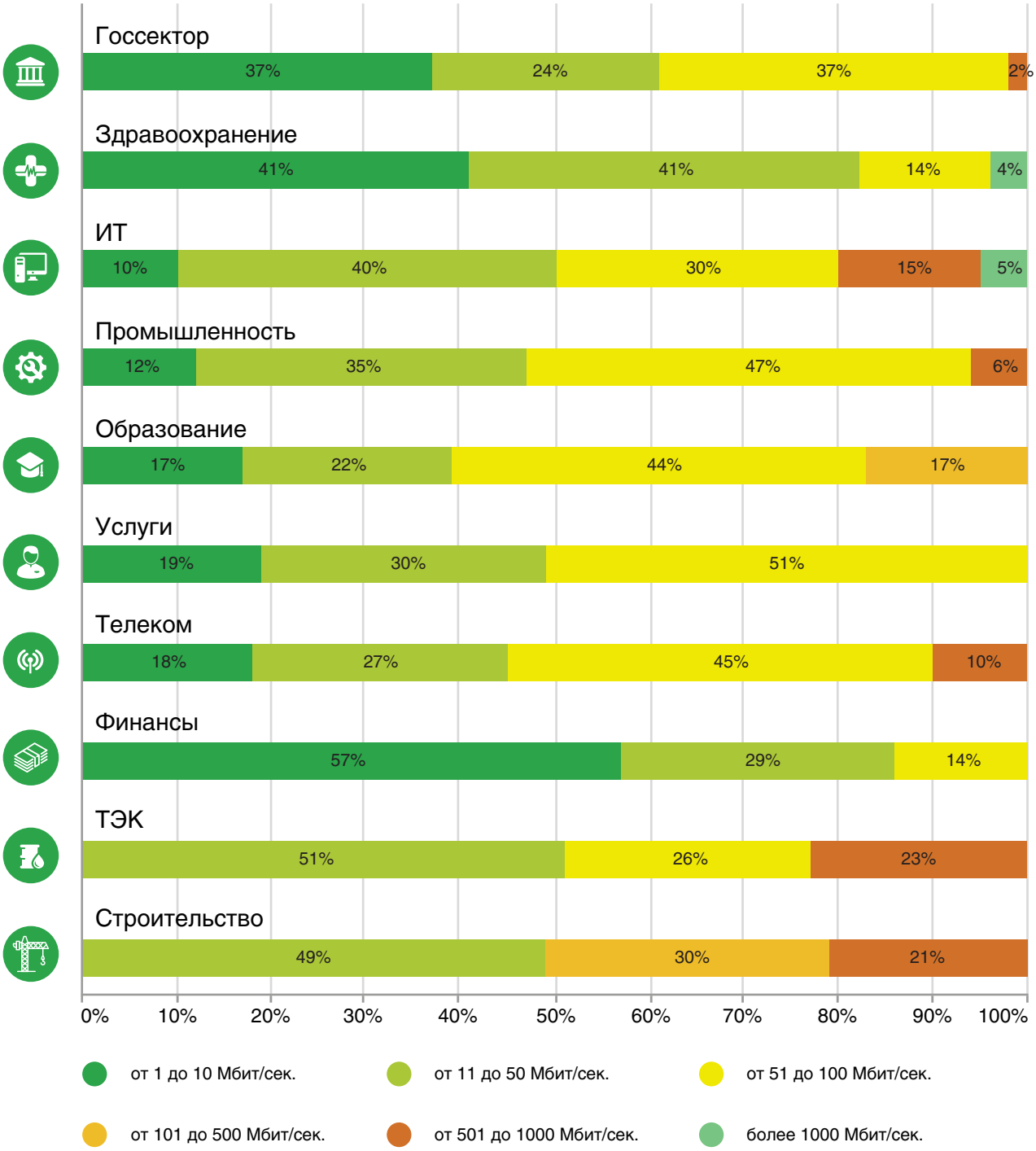
44% крупных компаний используют удаленный доступ к информационным системам с помощью ноутбуков, планшетов и смартфонов. В средних и малых компаниях наибольшие доли – 67% и 63% соответственно – приходятся на доступ из офисной сети.

Пропускная способность каналов связи

В любой системе обмен информацией производится по каналам связи. Общая схема передачи информации включает в себя устройство отправителя информации, канал передачи информации и устройство получателя информации. Основной характеристикой каналов передачи информации является их пропускная способность.

Характеристика сети

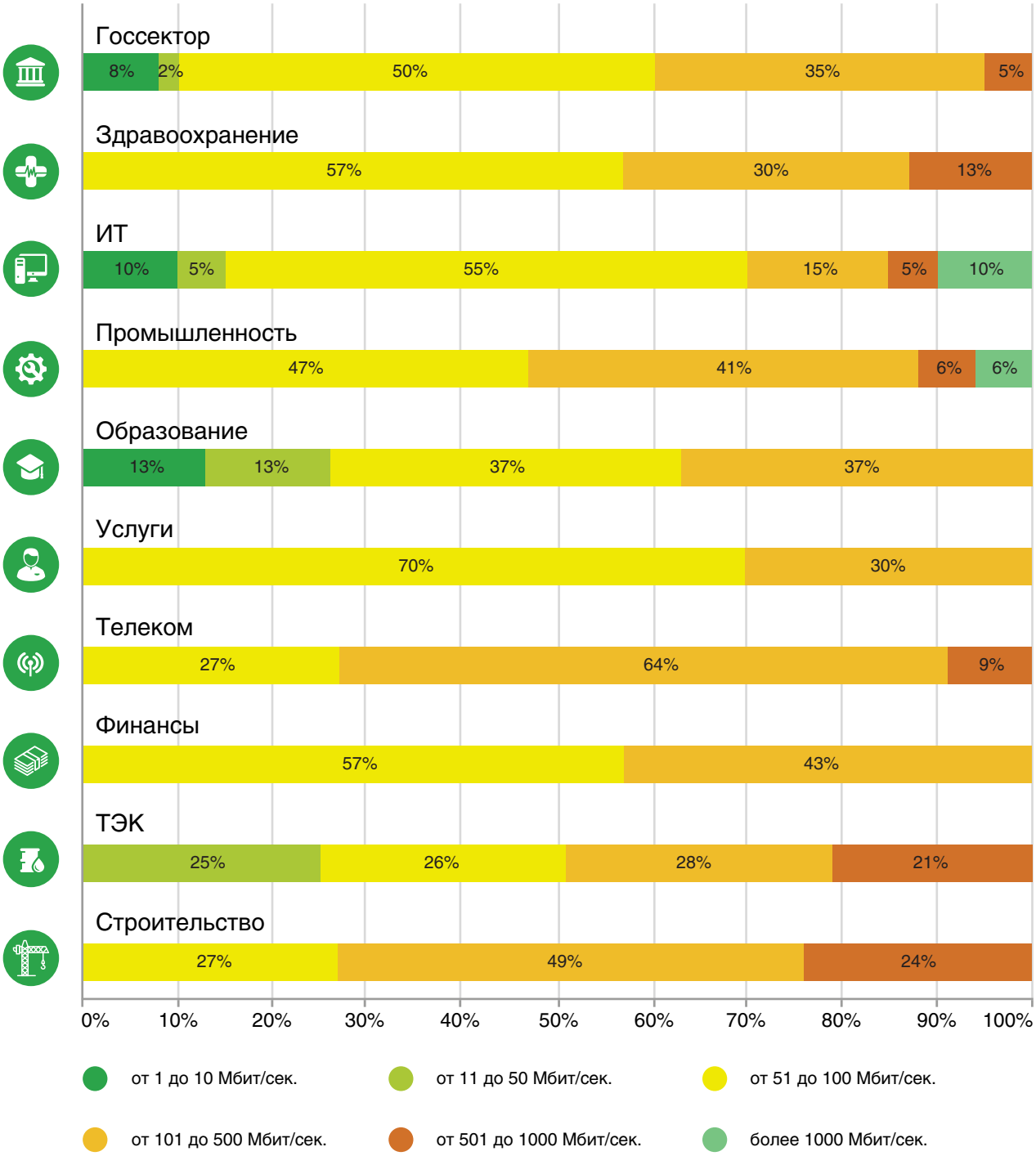
Пропускная способность каналов связи для подключения к интернету



Чаще всего пропускная способность канала связи с интернетом для всех отраслей составляет от 11 до 50 Мбит/сек.

Характеристика сети

Пропускная способность каналов связи внутренней сети

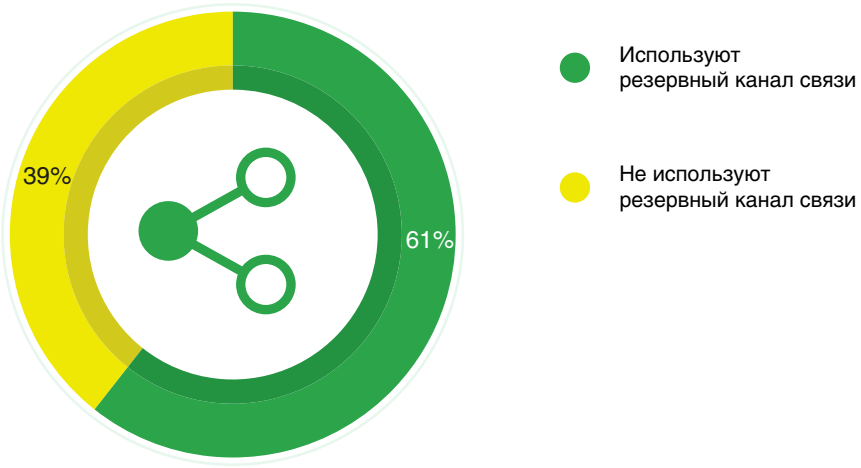


Пропускной способностью каналов связи внутренней сети более 10000 Мбит/сек. характеризуются информационные технологии и промышленность. Во всех отраслях чаще всего наблюдается пропускная способность каналов связи внутренней сети либо от 51 до 100 Мбит/сек., либо от 501 до 1000 Мбит/сек.

Использование резервного канала связи

Для большинства российских организаций при построении собственной корпоративной сети связи важнейшую роль играет ее надежность. В случае экстренного и непредвиденного выхода из строя участков коммуникационных линий резервные каналы смогут обеспечить стабильную и качественную связь до восстановления работоспособности поврежденного участка. Как показало исследование «Кода Безопасности», только 61% российских компаний используют резервные каналы связи.

Резервный канал связи

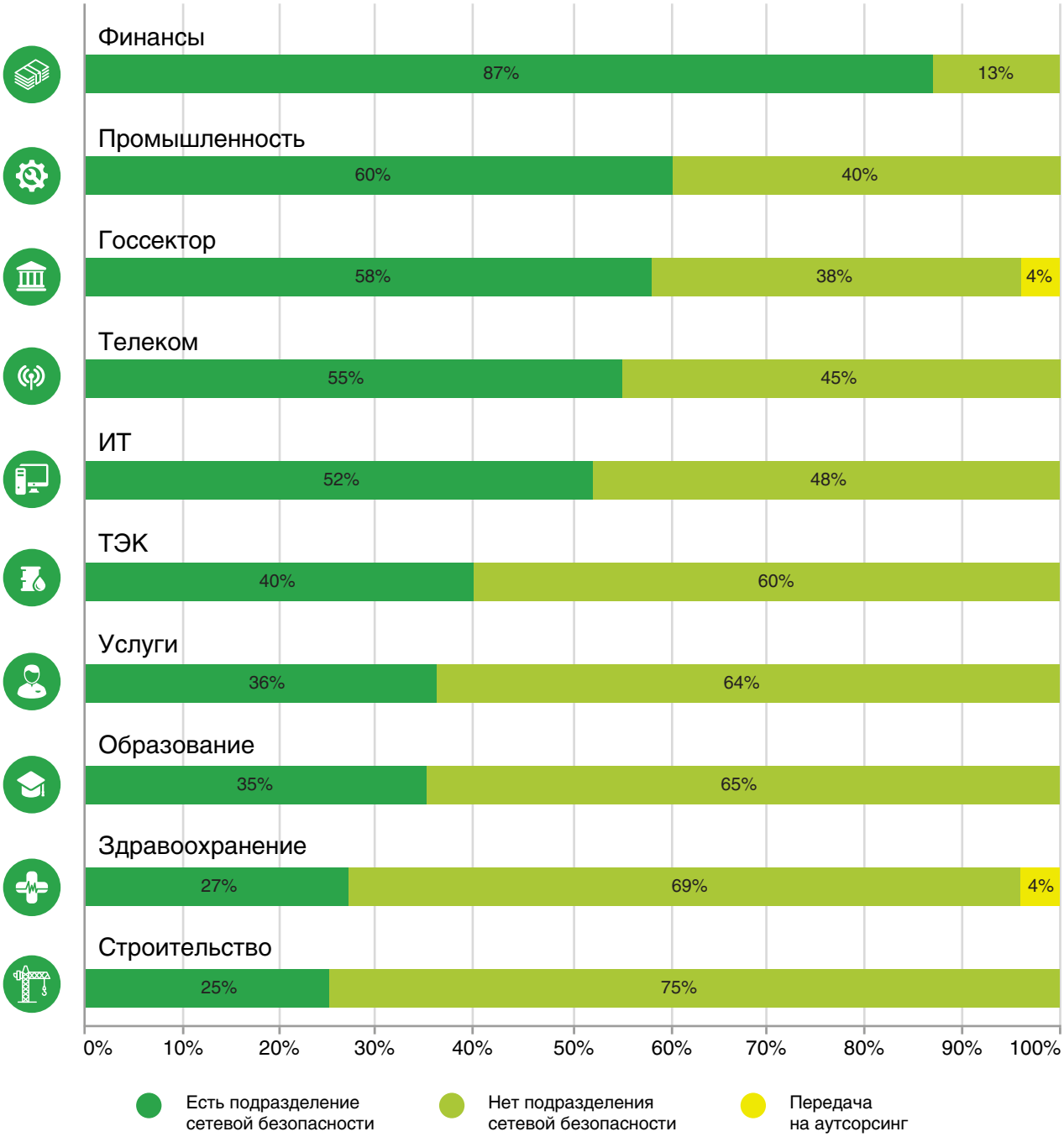


Кто отвечает за сетевую безопасность

Наиболее зрелые отрасли с точки зрения информационной безопасности – финансовая сфера и промышленность. В этих отраслях наблюдается наибольшая доля компаний, имеющих подразделение, отвечающее непосредственно за сетевую безопасность: финансы – 87%; промышленность – 60%. Сетевая безопасность передана на аутсорсинг в 4% компаний госсектора и 4% организаций здравоохранения. Не уделяют должного внимания сетевой безопасности строительная отрасль, образование, здравоохранение и сфера услуг. В среднем у 68% компаний этих отраслей нет выделенного подразделения, занимающегося сетевой безопасностью.

Характеристика сети

Наличие подразделения сетевой безопасности



Классификация информационных систем российских компаний

Для оптимизации затрат на построение системы защиты организации стремятся при классификации информационных систем минимизировать их класс.

Распределение классов информационных систем

50% российских компаний используют информационную систему персональных данных по уровню защищенности УЗ3; 26% российских компаний обрабатывают информацию в ГИС по классу К3.

Угрозы для корпоративных сетей

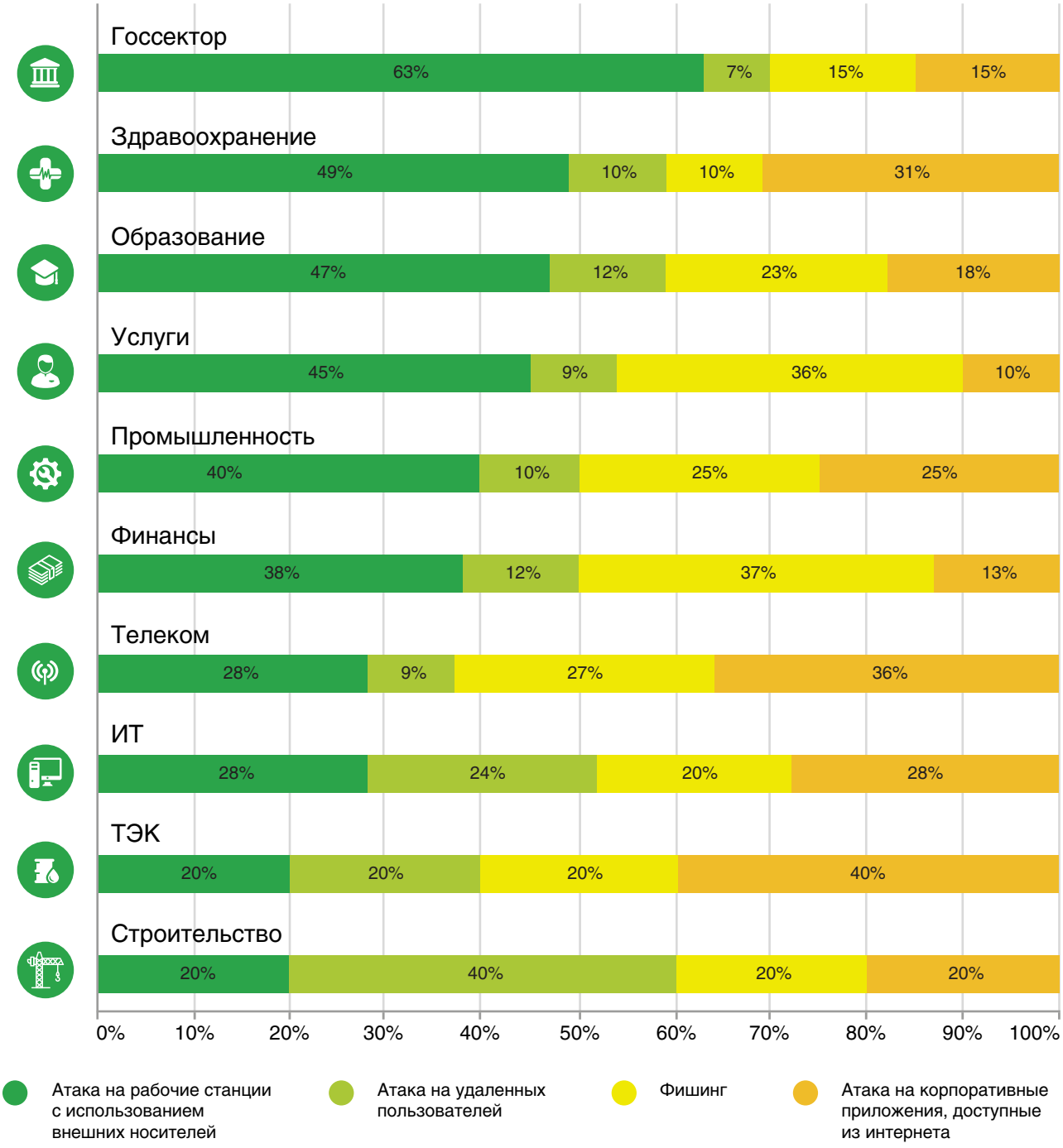
По данным опроса, наибольшую опасность для информации корпоративной сети представляет атака на рабочие станции с использованием внешних носителей. Данную угрозу отметили 47% респондентов.

Актуальные способы проникновения в сеть

Стандартным подходом к защите сетевой инфраструктуры является использование межсетевого экрана на периметре сети. Однако опрос показал, что специалистов по информационной безопасности беспокоят атаки на рабочие станции с использованием внешнего носителя в обход внешнего периметра сети. Таким образом, для эффективной защиты необходимо не только обеспечивать безопасность внешнего периметра, но и сегментировать внутреннюю сеть, то есть разделить сегмент пользователей и сегмент серверов.

Угрозы для корпоративных сетей

Актуальный способ проникновения в сеть по отраслям

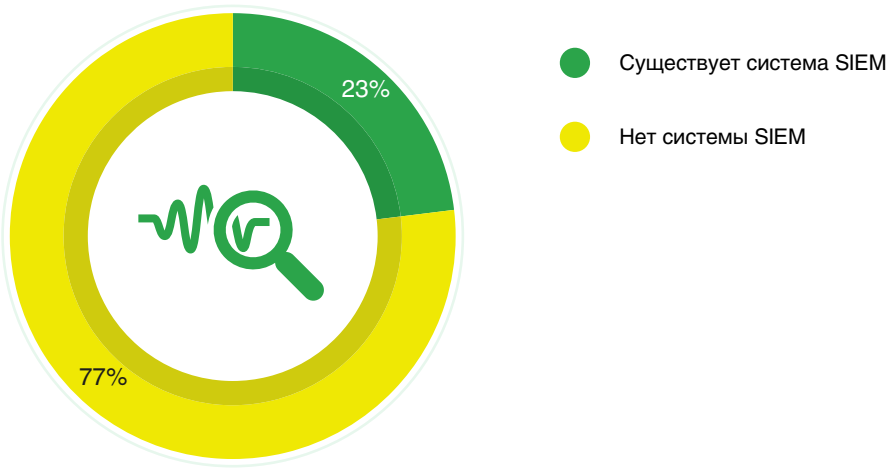


Атака на рабочие станции с использованием внешних носителей актуальна для госсектора (63%), здравоохранения (49%) и образования (47%). Атака на удаленных пользователей чаще характерна для строительства (40%) и информационных технологий (24%). Проблемы фишинга отметили финансовые компании (37%) и сфера услуг (36%). Атака на корпоративные приложения, доступные из интернета, актуальна для 40% компаний топливно-энергетического комплекса и 36% компаний телекома.

Централизованная система мониторинга ИБ (SIEM)

Для повышения эффективности средств информационной безопасности на рынке активно продвигаются продукты класса SIEM. Они позволяют централизованно собирать и анализировать поток событий, поступающих со средств защиты.

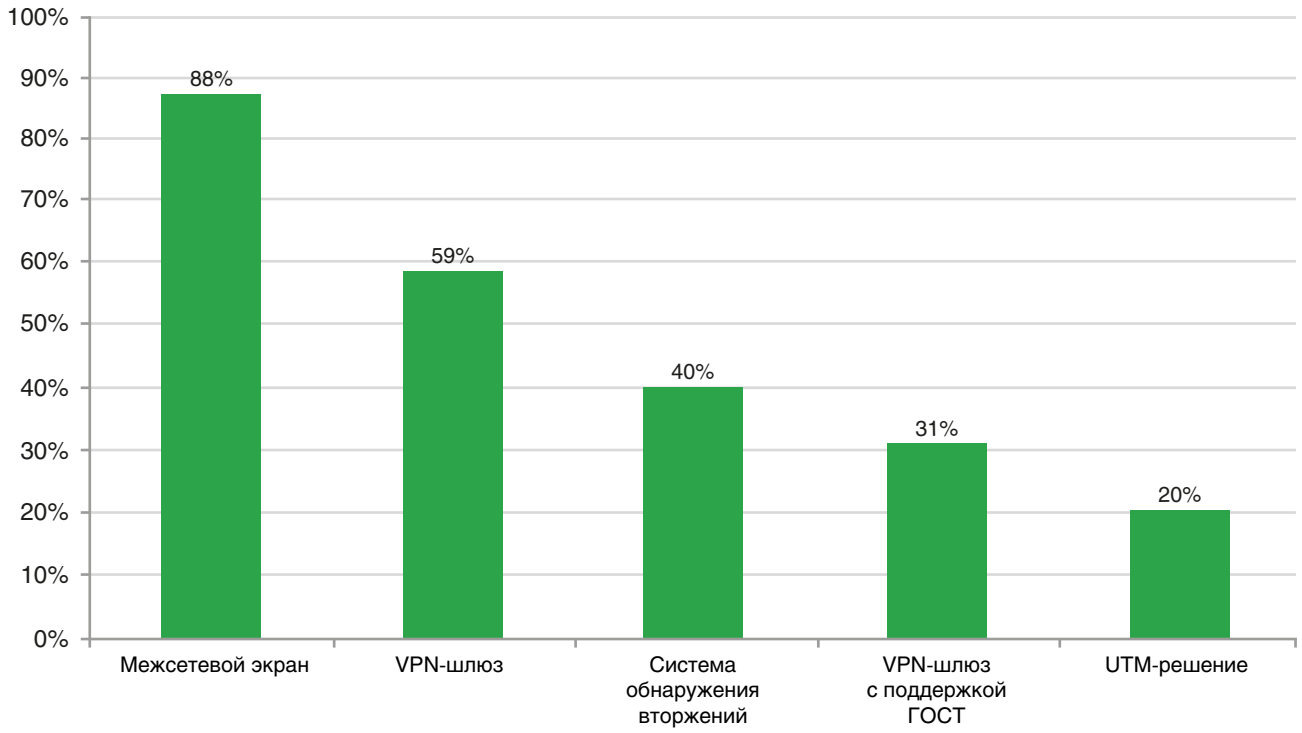
Наличие SIEM у российских компаний



По результатам исследования компании «Код Безопасности», лишь у 23% российских компаний имеется централизованная система мониторинга ИБ (SIEM).

В среднем российские компании используют решения трех вендоров для обеспечения сетевой безопасности.

Какие СЗИ развернуты в структуре российских компаний



Межсетевой экран стоит у 88% участников опроса. VPN-шлюз есть у 59% респондентов. Данная защита востребована в топливно-энергетическом комплексе (60% компаний) и финансовом секторе (56% компаний). Система обнаружения вторжений востребована у половины организаций здравоохранения и информационных технологий. UTM-решение используют 20% российских компаний.

Бюджет на сетевую безопасность

На защиту корпоративных сетей компании в среднем выделяют 11% из ИТ-бюджета.

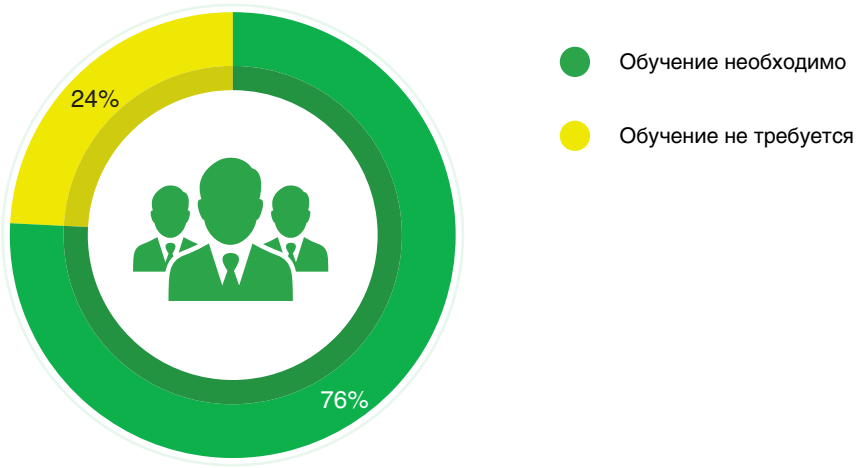
Потребность в обучении персонала, отвечающего за ИБ

Обсуждая проблемы информационной безопасности, не стоит обходить стороной квалификацию специалистов. Для надежного обеспечения информационной безопасности важно не только подбирать соответствующих специалистов, но и регулярно повышать их квалификацию.

Согласно результатам опроса, в 76% российских компаний существует потребность в обучении персонала, отвечающего за информационную безопасность.

Данный аспект важен для 90% компаний телекоммуникационной сферы, 87% организаций госсектора и 80% компаний топливно-энергетического комплекса. Остальные отрасли также акцентируют внимание на вопросах обучения специалистов по информационной безопасности (по всем отраслям данный показатель выше 50%).

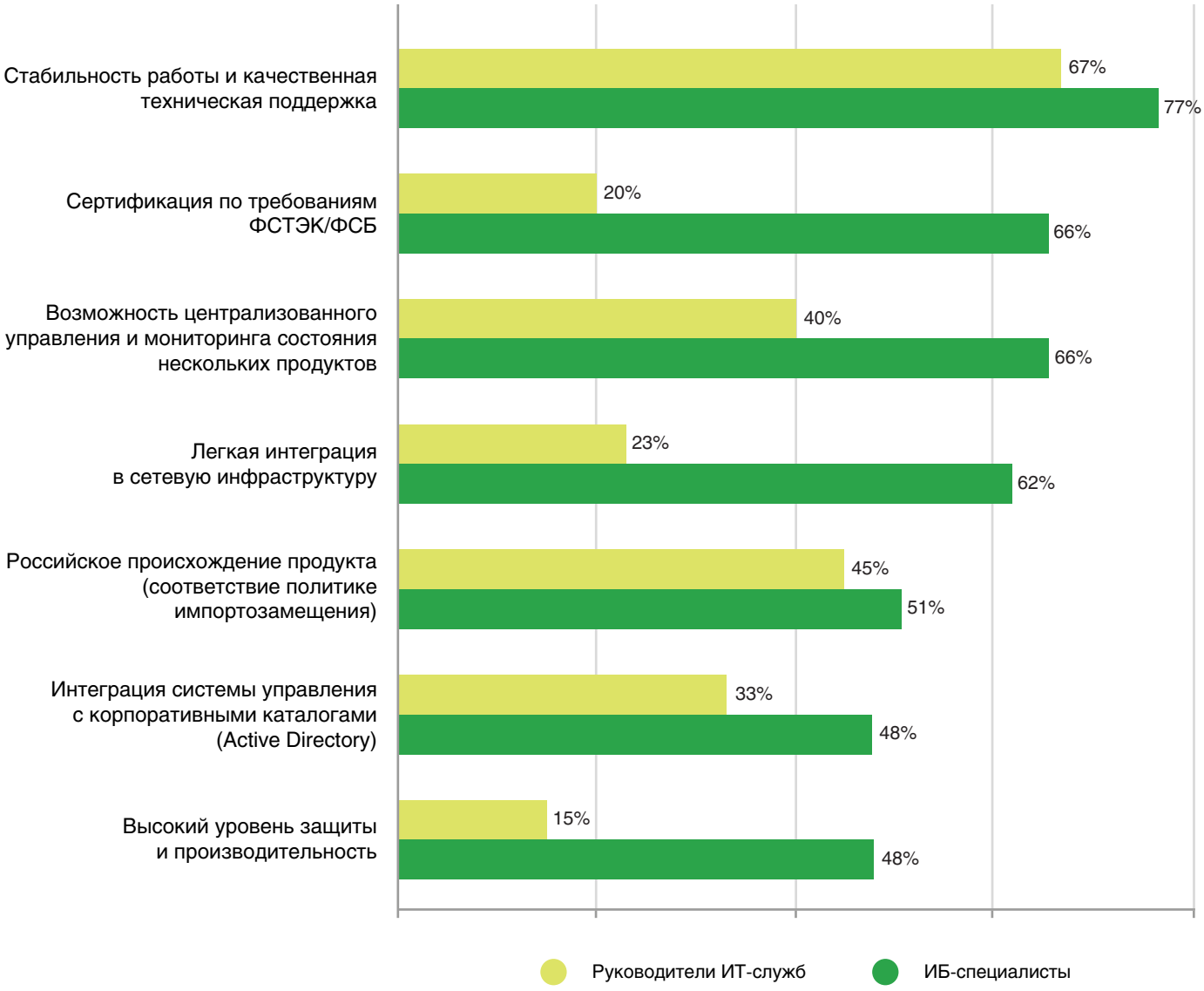
Потребность в обучении ИБ персонала



Приоритетные требования к средствам сетевой безопасности

На сегодняшний день системы защиты информации, представленные на рынке, сильно различаются как по набору механизмов защиты, так и по подходам к реализованным возможностям. Что должно быть положено в основу требований к средствам защиты? Какие приоритетные требования выдвигают к средствам сетевой безопасности заказчики? Сравнительный анализ ответов ИБ-специалистов и руководителей ИТ-служб представлен на графике ниже.

Приоритетные требования к средствам сетевой безопасности



И для CIO, и для ИБ-специалистов на первом месте по важности стоит стабильность работы и качественная техническая поддержка. Значимость этого фактора отметили 67% руководителей ИТ-служб и 77% специалистов по информационной безопасности. Этот показатель в первую очередь важен для финансовой сферы, информационных технологий, строительной отрасли и здравоохранения. 77% организаций госсектора и 62% организаций здравоохранения отметили приоритетным фактором российское происхождение продукта (соответствие политике импортозамещения). С этим согласились практически в одинаковой степени и CIO (45%), и специалисты по информационной безопасности (51%) всех отраслей.

Для ИБ-специалистов важен параметр «Высокий уровень защиты и производительность», его отметили больше половины организаций госсектора, здравоохранения, промышленности, телекоммуникаций и топливно-энергетического комплекса.

Заключение

Сетевая безопасность имеет решающее значение для отечественных организаций. В среднем 75% российских структур всех отраслей имеют филиалы, объединенные сетью передачи данных. Для большинства российских организаций при построении собственной корпоративной сети связи важнейшую роль играет фактор надежности, но только 61% российских компаний используют резервные каналы связи.

Стратегия обеспечения сетевой безопасности должна учитывать такие факторы, как повышение уровня надежности сети, эффективное управление безопасностью и защита от постоянно меняющихся угроз и новых методов атак. Меньше чем у четверти российских компаний внедрена централизованная система мониторинга ИБ (SIEM). Низкое проникновение SIEM-систем повышает значение встроенных в средства защиты механизмов мониторинга безопасности.

Компаниям необходимо обеспечивать безопасный доступ для сотрудников к сетевым ресурсам в любое время. 44% крупных компаний используют удаленный доступ к информационным системам с помощью ноутбуков, планшетов и смартфонов. И для многих компаний проблема обеспечения сетевой безопасности становится все более сложной, поскольку мобильные устройства сотрудников – это потенциальные проблемы.

Сегодня хакеры используют разнообразные методы атаки на сети компаний. Исследование показало, что ИБ-специалистов в наибольшей степени беспокоят два типа вторжений: атака на рабочие станции с использованием внешних носителей и фишинг. Каждая вторая российская компания отметила их актуальность. Защиты периметра для обеспечения сетевой безопасности недостаточно, необходима сегментация внутренней сети, особенно разделение сегментов пользователей и серверов.

На защиту корпоративных сетей компании в среднем выделяют 11% из ИТ-бюджета. В среднем российские компании используют решения трех вендоров для обеспечения сетевой безопасности, что повышает нагрузку на администраторов и риск простоя корпоративной сети, вызванный ошибками при конфигурации.

При выборе средств сетевой безопасности приоритетными требованиями CIO и ИБ-специалисты назвали:

стабильность работы
и качественную техническую поддержку;

централизованное управление
и мониторинг состояния продуктов;

российское происхождение продукта
(соответствие политике импортозамещения).

Заключение

В настоящее время большое количество как иностранных, так и отечественных компаний предлагают различные аппаратно-программные и программные реализации межсетевых экранов – их применение стало ключевым элементом в построении высокопроизводительных, безопасных и надежных информационно-аналитических систем и систем автоматизации предприятий, финансовых систем, распределенных баз данных, систем удаленного доступа работников к внутренним ресурсам корпоративных сетей, сегментов корпоративной сети и корпоративной сети в целом.

Для целостного решения задач обеспечения безопасности сетевой инфраструктуры заказчикам потребуется продукт, обладающий следующими качествами:

Эффективная фильтрация трафика не только на сетевом уровне, но и на уровне приложений. Это связано с распространением приложений, которые умеют туннелировать свой трафик через всегда открытые на межсетевых экранах порты. Эффективно запретить их работу можно только на прикладном уровне. Применение продуктов, позволяющих это сделать, значительно повысит безопасность сетевой инфраструктуры.

Развитые механизмы управления. Единая консоль управления защитой сетевой инфраструктуры позволяет оптимизировать затраты на эксплуатацию средств защиты. Интуитивно понятный интерфейс системы мониторинга позволяет оперативно отследить инциденты безопасности и минимизировать время ликвидации последствий. Это позволяет организации перенаправить специалистов по сетевой безопасности на решение более важных задач.

Обеспечение высокой производительности. Защита от современных угроз предполагает очень тщательный анализ сетевого трафика, что может вызвать эффект «бутылочного горлышка», когда межсетевой экран или IPS ограничивают общую производительность сети. Это в свою очередь создает проблемы в функционировании бизнес-критичных приложений и работе организации в целом. Ранее для соблюдения баланса между безопасностью и производительностью каждой организации требовалось идти на компромисс. Высокопроизводительные устройства позволяют избежать этого и обеспечить как высокий уровень безопасности, так и высокий уровень производительности.

КОД БЕЗОПАСНОСТИ

«Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, облачных сред, мобильных устройств, а также коммерческой и государственной тайны. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

Тел.: +7 (495) 982 30 20

analytics@securitycode.ru

www.securitycode.ru