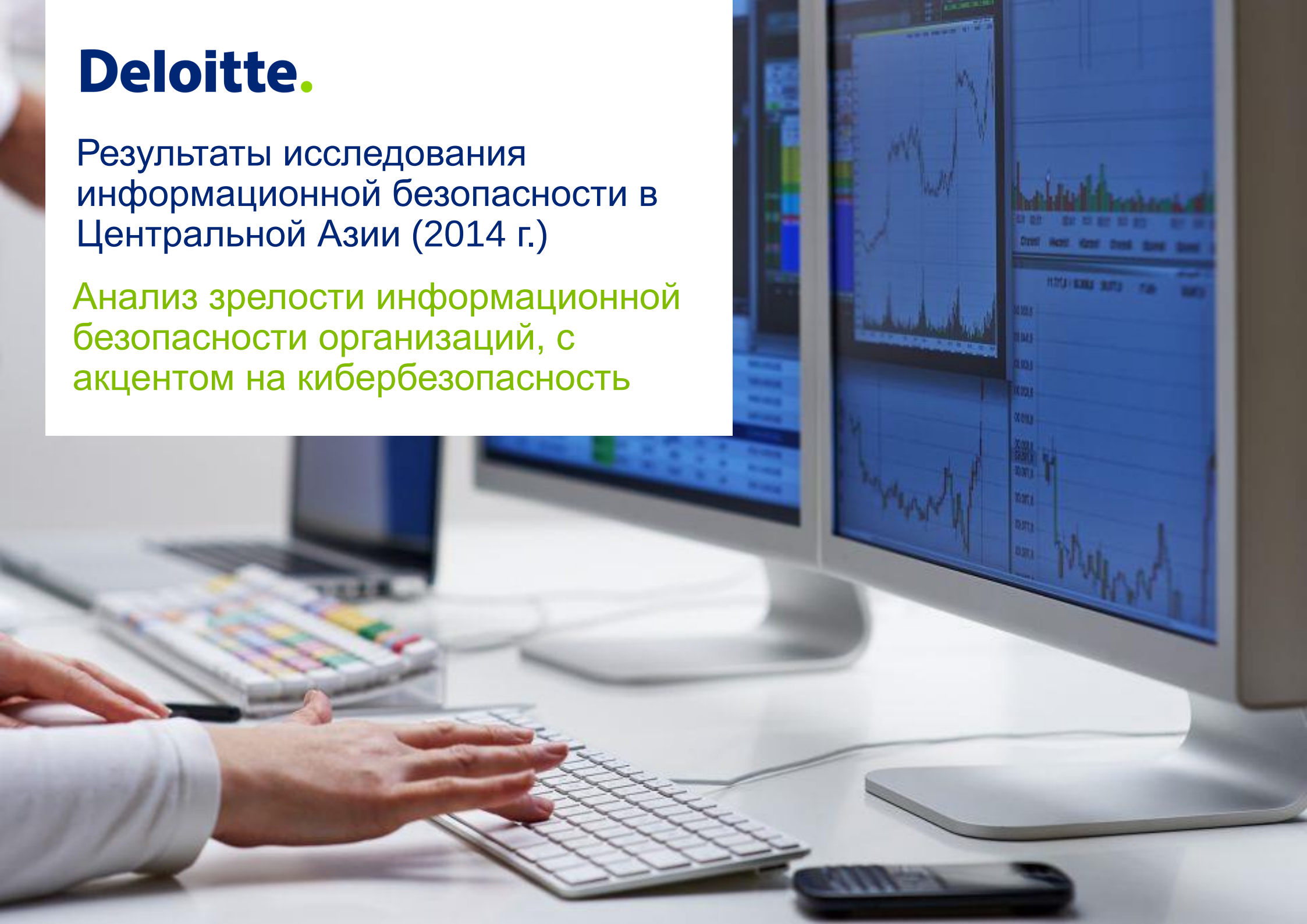
Deloitte.

Результаты исследования информационной безопасности в Центральной Азии (2014 г.)

Анализ зрелости информационной безопасности организаций, с акцентом на кибербезопасность



Введение и резюме для руководства

С сентября по ноябрь 2014 г. «Делойт» провел свое первое «исследование информационной безопасности» в Центральной Азии, чтобы лучше понять текущее состояние программ информационной безопасности и структур управления в организациях в регионе. Исследование охватывает различные отрасли и рассматривает то, каким образом организации оценивают, разрабатывают, внедряют и поддерживают свои программы по обеспечению информационной безопасности.

39 вопросов исследования охватывали следующие области:

1. Организационная информация
2. Сетевые атаки и угрозы информационной безопасности
3. Данные и технологии информационной безопасности
4. Мониторинг и реагирование на выявленные угрозы безопасности

Исследование было акцентировано на риски кибербезопасности, и с этой целью мы попросили около 100 компаний заполнить онлайн опросник.

Оговоримся, что мы представляем результаты опроса не делая различия по отраслям или по размеру организаций, и что результаты являются «анонимными» во избежание упоминания отдельных организаций.

Мы хотели бы поблагодарить организации, принявшие участие в опросе за их сотрудничество. Мы хотели бы призвать и другие компании принять участие в следующем исследовании «Делойт» в отношении информационной безопасности.

Резюме для руководства

По результатам исследования были выявлены пять самых существенных выводов о текущем состоянии программ информационной безопасности (кибербезопасности) в Центральной Азии, а именно:

1. Большинство компаний не были подвержены инцидентам кибербезопасности.
2. В большинстве компаний есть установленные политики, процедуры и сферы ответственности по информационной безопасности.
3. Существует недостаточно контролей для обеспечения соблюдения третьими лицами (т.е. поставщиками/партнерами) соответствующих стандартов безопасности.
4. (Высшее) руководство и конечные пользователи недостаточно осознают риски кибербезопасности.
5. Хотя применяются основные меры безопасности, более продвинутые решения являются редкостью.

Далее в этом отчете мы предоставляем более детальные результаты исследования.

Сравнение глобальных тенденций со статусом информационной безопасности в Центральной Азии

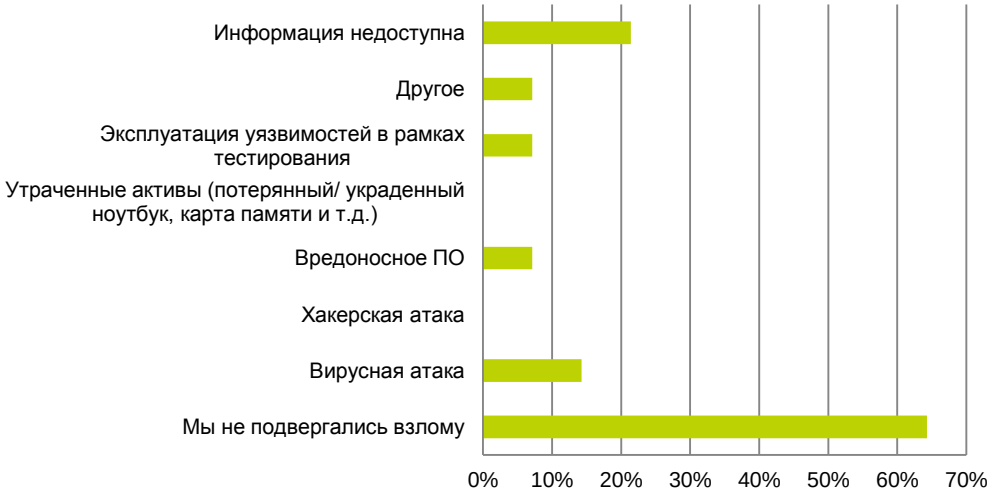
Количество инцидентов по информационной безопасности растет во всем мире, от пассивного мониторинга сообщений, до атак.

Несомненно, недавняя кибер-атака на Sony Pictures, в результате которой хакеры получили доступ к некоторым из самых конфиденциальных данных корпорации, привлекла большое внимание СМИ. Так же широкую огласку получила в свое время массивная утечка данных в JPMorgan Chase & Co., которая привела к краже данных 76 миллионов клиентов. Другой пример относится к компании “Home Depot”, у которой были похищены данные кредитных карт 56 миллионов клиентов с помощью установления вредоносного ПО на платежную систему.

В Центральной Азии также произошел ряд инцидентов, широко освещавшихся в новостях. Однако по сравнению с другими регионами, количество атак ограничено, а по тем атакам, которые были зарегистрированы, доступно мало информации о их фактическом влиянии. Согласно ответам респондентов исследования, примерно 65% из них не подвергались кибер-атакам, направленным на их организации (см. Вопрос 1).

Хотя количество широко известных кибератак кажется небольшим, это не значит, что организации в регионе неуязвимы; они могут иметь ложное чувство безопасности. Учитывая мировые тенденции и увеличение количества атак, а также повышенное внимание, уделяемое вопросам кибербезопасности, вполне может быть, что Центральная Азия может стать следующей мишенью для хакеров в ближайшем будущем. Когда – не если - это случится, организации должны быть готовы.

Вопрос 1: Подвергались ли Вы взлому в течение последних 12 месяцев? (возможны несколько вариантов ответов)?



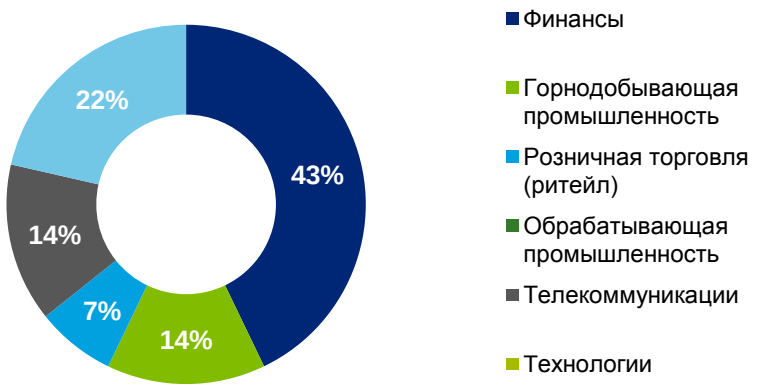
В большинстве компаний не происходили инциденты кибербезопасности. Тем не менее, имеется недостаточно доказательств относительно того, реальность ли это или просто восприятие.

Сферы деятельности респондентов исследования информационной безопасности в Центральной Азии

Сферы деятельности респондентов исследования информационной безопасности в Центральной Азии (1/2)

Неудивительно, что 65% респондентов относятся к сфере телекоммуникаций и финансов (см. вопрос 2), так как эти отрасли являются наиболее подверженными кибер-атакам.

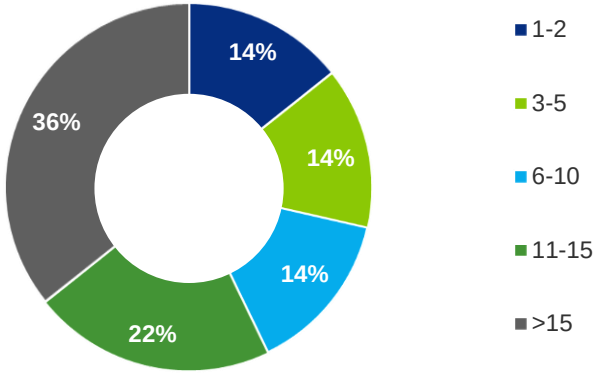
Вопрос 2: В какой отрасли осуществляет деятельность ваша организация?



В то же время, правительства начали уделять повышенное внимание безопасности своих стратегических предприятий (таких, как заводы и электростанции), чтобы защитить важнейшие ИТ-инфраструктуры - так называемые системы SCADA - от несанкционированного доступа. По этой причине, ожидается, что высшее руководство в отрасли ресурсов (нефти, газа, энергетики) должно также концентрироваться на информационной безопасности.

Большинство респондентов (58%) имеют более 10 сотрудников в IT-департаментах. Тем не менее, исследование также охватывает более мелкие ИТ-департаменты, как указано в вопросе 3 ниже.

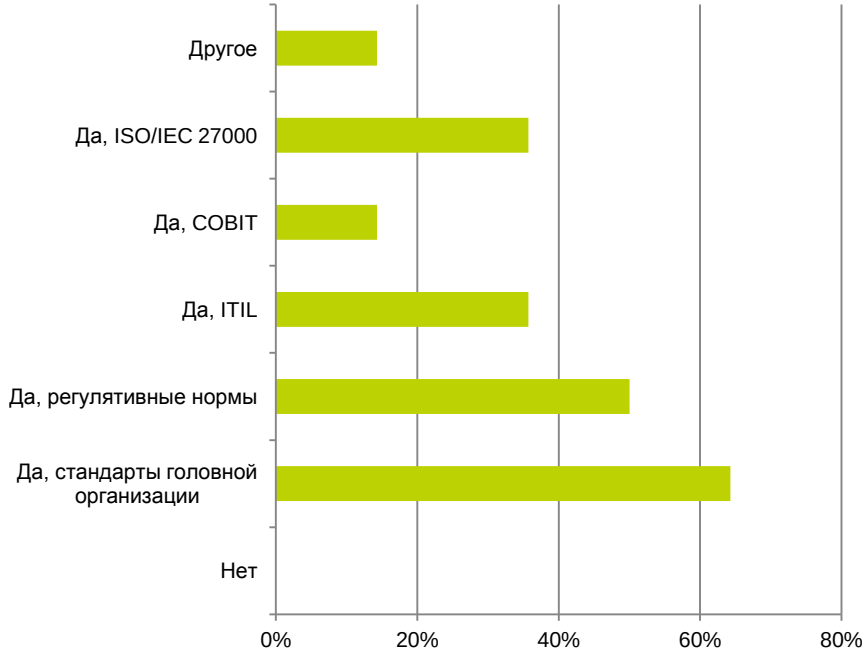
Вопрос 3: Сколько человек работает в вашем ИТ-отделе?



Сферы деятельности респондентов исследования информационной безопасности в Центральной Азии (2/2)

Когда респондентов спросили о стандартах IT-управления (см. вопрос 4), большинство организаций упомянули о внутренних политиках (65%) и нормативных требованиях (50%), а не о международных стандартах, таких как COBIT или ITIL.

Вопрос 4: Соблюдает ли Ваша организация какие-либо нормы и/или стандарты, касающиеся ИТ-процессов или безопасности *(возможны несколько вариантов ответов)?*



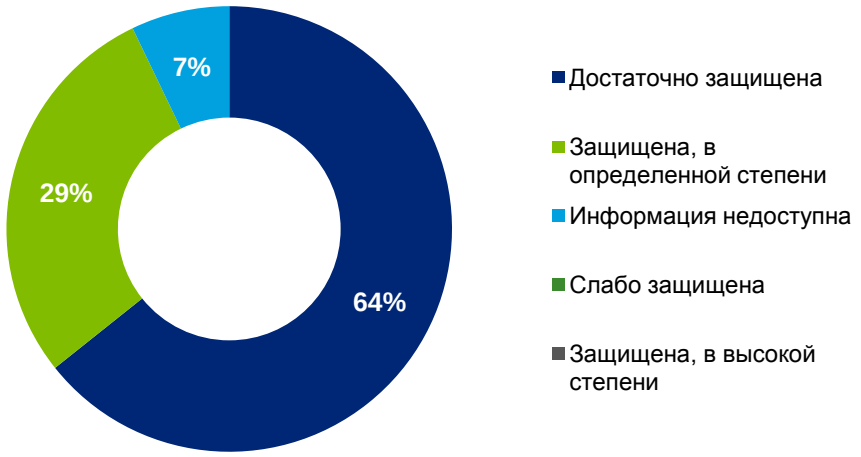
Зрелость корпоративной информационной безопасности в Центральной Азии

Зрелость корпоративной информационной безопасности в Центральной Азии (1/4)

Некоторые вопросы исследования касались уровня зрелости по информационной безопасности в отношении следующих тем: (1) осведомленность респондентов о своей сетевой безопасности (2) наличие политики, (3) степень, до которой определена ответственность по информационной безопасности, (4) текущий уровень зрелости и (5) ключевые сложности улучшения корпоративной информационной безопасности.

64% респондентов считают, что их организации имеют надлежащие политики и процедуры обеспечения безопасности (см. вопрос 5) и, что интересно, количество респондентов, сказавших, что в их организациях слабые или недостаточные политики и процедуры безопасности, был равен нулю.

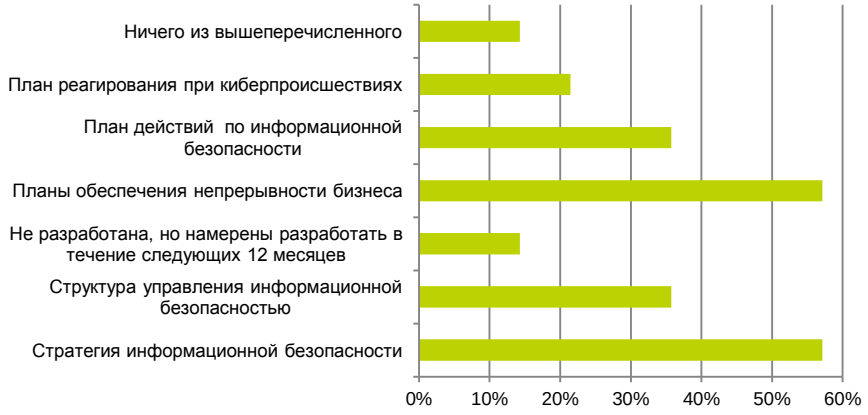
Вопрос 5: Насколько, на ваш взгляд, безопасна сеть вашей организации?



Большинство респондентов имеют политики и процедуры информационной безопасности (или собираются утвердить их в ближайшее время), в которых определена ответственность по информационной безопасности.

Похоже, что большинство респондентов имеют политику и процедуры, в основном связанные с (1) стратегией по ИТ-безопасности и (2) планами обеспечения непрерывности бизнеса (см. Вопрос 6). Однако лишь немногие респонденты указали, что они разработали план реагирования на инциденты в области кибербезопасности.

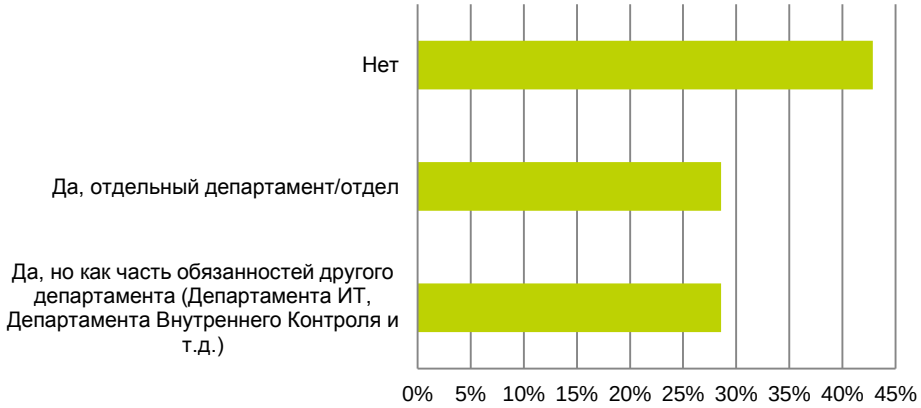
Вопрос 6: Какие из перечисленных политик/процедур документированы и утверждены в вашей организации (возможны несколько вариантов ответов)?



Зрелость корпоративной информационной безопасности в Центральной Азии (2/4)

Вопрос 7 показывает, что у 57% респондентов есть сотрудник по вопросам безопасности, а остальные 43% заявили, что они еще не определили обязанности по информационной безопасности.

Вопрос 7: Есть ли в вашей организации отдельный департамент, отвечающий за сетевую безопасность?



Отчеты по информационной безопасности, как правило, направляются не Главному Директору по ИТ, а Главному Исполнительному Директору (CEO) (36%) или Правлению (Совету директоров) (14%). См. вопрос 8.

Вопрос 8: Кому подотчетна служба информационной безопасности вашей организации?

Большинство (около 80%) организаций получают сведения об информационной безопасности посредством публикаций и журналов, рассылки и Интернета (см. вопросы 9 и 10).

Вопрос 9: Что повысило вашу осведомленность о кибер-атаках (возможны несколько вариантов ответов)?

Зрелость корпоративной информационной безопасности в Центральной Азии (3/4)

Учитывая, что в каждой организации различная структура, и что они сталкиваются с различными угрозами безопасности (см. вопрос 13), предполагалось, что все больше организаций будет оставаться в курсе дел через уникальные события и конкретные источники, например конференции и консультации.

Вопрос 10: Как вы узнаете о новых формах кибер-атак и угроз информационной безопасности (возможны несколько вариантов ответов)?

Мы попросили респондентов указать их текущий статус по информационной безопасности на основе нашей пятиуровневой модели. Около 30% респондентов признались, что находятся на 3 уровне (см. вопрос 11), подразумевающем «наличие набора определенных и документированных стандартных процессов и некоторую степень улучшения со временем».

Вопрос 11: На каком уровне зрелости находится ваша организация в настоящее время?

Зрелость корпоративной информационной безопасности в Центральной Азии (4/4)

Чтобы претендовать на 3-й уровень зрелости, важно, чтобы политика и процедуры были не только определены, но и выполнялись во всей организации. Мы не можем прокомментировать, в какой степени организации на самом деле выполняют политики и процедуры, поскольку для этого требуется более детальная оценка или проверка. Тем не менее, как показывает практика, на самом деле большинство организаций в Центральной Азии находятся на 2 уровне зрелости, и только некоторые на 3 уровне.

Наконец, мы попросили респондентов указать, что могло бы помочь им повысить зрелость информационной безопасности. Большинство отметили необходимость в: (1) более современных инструментах, (2) повышении уровня информированности и (3) приверженности со стороны высшего руководства улучшать информационную безопасность (см. вопрос 12).

Хотя Департаменты по ИТ осведомлены о рисках кибербезопасности, повышение осведомленности руководства и конечных пользователей считается недостаточным.

Вопрос 12: Что, по-вашему, поможет повысить уровень информационной безопасности вашей организации (возможны несколько вариантов ответов)?

Обзор наиболее часто используемых мер безопасности

Обзор наиболее часто используемых мер безопасности (1/2)

В этом разделе отчета содержится обзор угроз информационной безопасности, которые респонденты считают наиболее актуальными для их организации, и мер безопасности, которые были применены для контроля этих угроз, в частности, в отношении кибербезопасности.

Мы спросили респондентов о том, какой риск они считают наиболее существенным (см. вопрос 13). Результаты были весьма разнообразными, что указывает на широкий спектр рисков кибербезопасности, с которыми сталкиваются организации в регионе.

Вопрос 13: Какой риск безопасности вы считаете наиболее серьезным (возможны несколько вариантов ответов)?

Вопросы 14 и 15 показывают, что большинство респондентов применяют основные меры безопасности, такие как антивирусные решения, брандмауэры и списки управления доступом. Тем не менее, не так часто применяются более современные решения, такие как системы предотвращения вторжений, шифрование файлов, системы управления уязвимостью и управления журналами системных событий (в том числе активные обзоры). Учитывая, что хакеры по всему миру быстро становятся все более изощренными в своих методах взлома, текущее состояние мер безопасности может представлять большую угрозу для компаний в Центральной Азии.

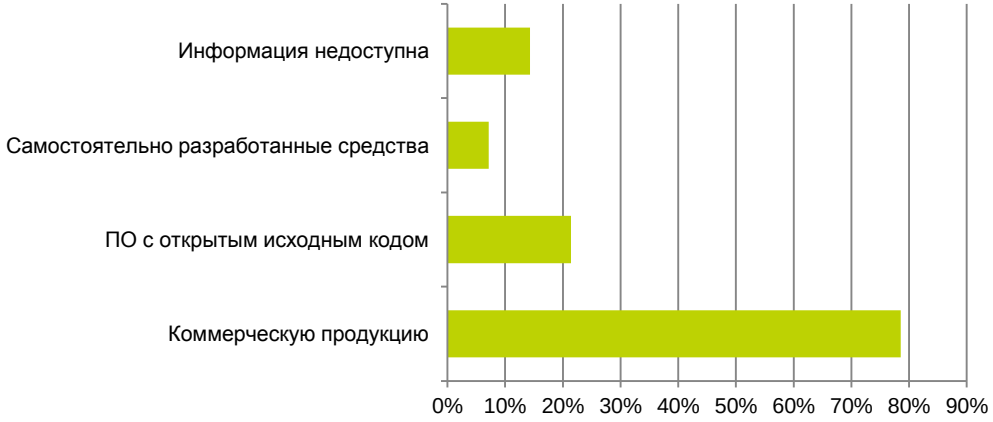
Вопрос 14: Какие меры безопасности применяет ваша организация (возможны несколько вариантов ответов)?

Обзор наиболее часто используемых мер безопасности (2/2)

Вопрос 16 показывает, что компании в Центральной Азии главным образом используют коммерческие продукты для защиты их среды, а не решения, специально предназначенные для компании. Если вы полагаетесь на коммерческие продукты, важно выполнять периодические обновления (для системы безопасности), чтобы обеспечить адекватную защиту от наиболее распространенных угроз безопасности.

Вопрос 15: Какие меры вы обычно применяете для минимизации сетевых атак, нацеленных на инфраструктуру/клиентов вашей организации (возможны несколько вариантов ответов)?

Вопрос 16: Какие инструменты использует ваша организация для выявления атак (возможны несколько вариантов ответов)?



Мы считаем, что постоянные инвестиции в изучение рисков безопасности, в том числе каких-либо инструментов и методов, которые могут быть использованы для снижения риска безопасности до приемлемого уровня, имеет первостепенное значение. Это включает в себя разработку мер, учитывающих специфику компании, т.е. сферу деятельности, типы данных и интеллектуальную собственность. Мы подчеркиваем, что эффективное управление информационной безопасностью требует как предупредительных, так и следственных контролей.

Большинство респондентов применяют основные меры безопасности, такие как антивирусные решения, брандмауэры и списки управления доступом. Тем не менее, не так часто применяются более современные решения, такие как системы предотвращения вторжений, шифрование файлов и системы управления уязвимостью.

Осведомленность об информационной безопасности внутри организации

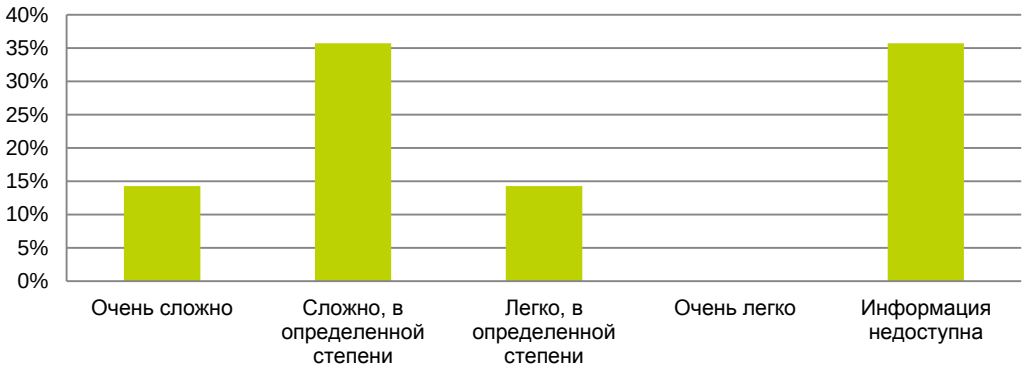
Осведомленность об информационной безопасности внутри организации (1/2)

Как показано в вопросах 9 и 10, IT-департамент узнает о рисках кибербезопасности в основном через публично доступную информацию и отчеты. Несмотря на то, что по-видимому IT-департаменты информированы и осведомлены о рисках кибербезопасности, осведомленность конечных пользователей и (высшего) руководства менее очевидна (см. вопрос 17).

Вопрос 17: Проводит ли ваша организация тренинги для сотрудников с целью повышения осведомленности об информационной безопасности?

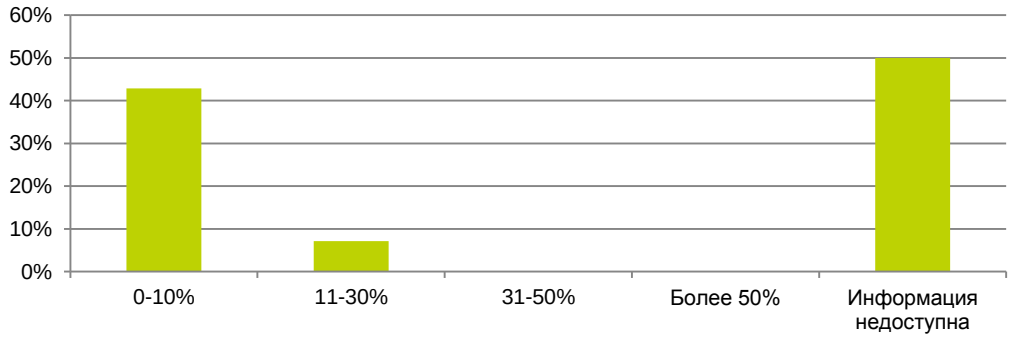
Внедрение в повестку дня руководства вопрос о кибербезопасности считается одной из основных задач, стоящих перед ИТ-департаментами в ближайшем периоде (см. вопрос 18).

Вопрос 18: Насколько трудно, на ваш взгляд, убедить руководство о необходимости инвестировать в сферу безопасности?



Вопросы 19 и 20 показывают, что значительное количество респондентов не предоставили информацию о (а) текущих расходах на ИТ безопасность и (б) ожидаемых затратах.

Вопрос 19: Какой процент вашего ИТ-бюджета был потрачен на безопасность в течение последних 12 месяцев?



Осведомленность об информационной безопасности внутри организации (2/2)

Это может означать, что респонденты считают эту информацию конфиденциальной или что такая информация просто не доступна. В случае последнего, мы настоятельно рекомендуем улучшить отслеживание средств, затрачиваемых на информационную безопасность, так как этот тип информации имеет важное значение для обеспечения эффективности процесса принятия решений (например, в случае анализа эффективности затрат для предлагаемых мер безопасности).

Вопрос 20: Можете ли вы описать свои межгодовые расходы относительно бюджета на информационную безопасность?

Хотя и не ясно, были ли связаны ответы респондентов с отсутствием информации о фактических и ожидаемых расходах, или информация была не предоставлена для целей данного исследования, мы должны отметить, что организации должны быть в курсе их текущего и будущего финансового положения, так как высшее руководство должно рассматривать, покрывают ли инвестиции потенциальные расходы в случае возникновения инцидентов.

Контроль третьих лиц должен стать основным направлением деятельности организаций в Центральной Азии

Контроль третьих лиц должен стать основным направлением деятельности организаций в Центральной Азии (1/2)

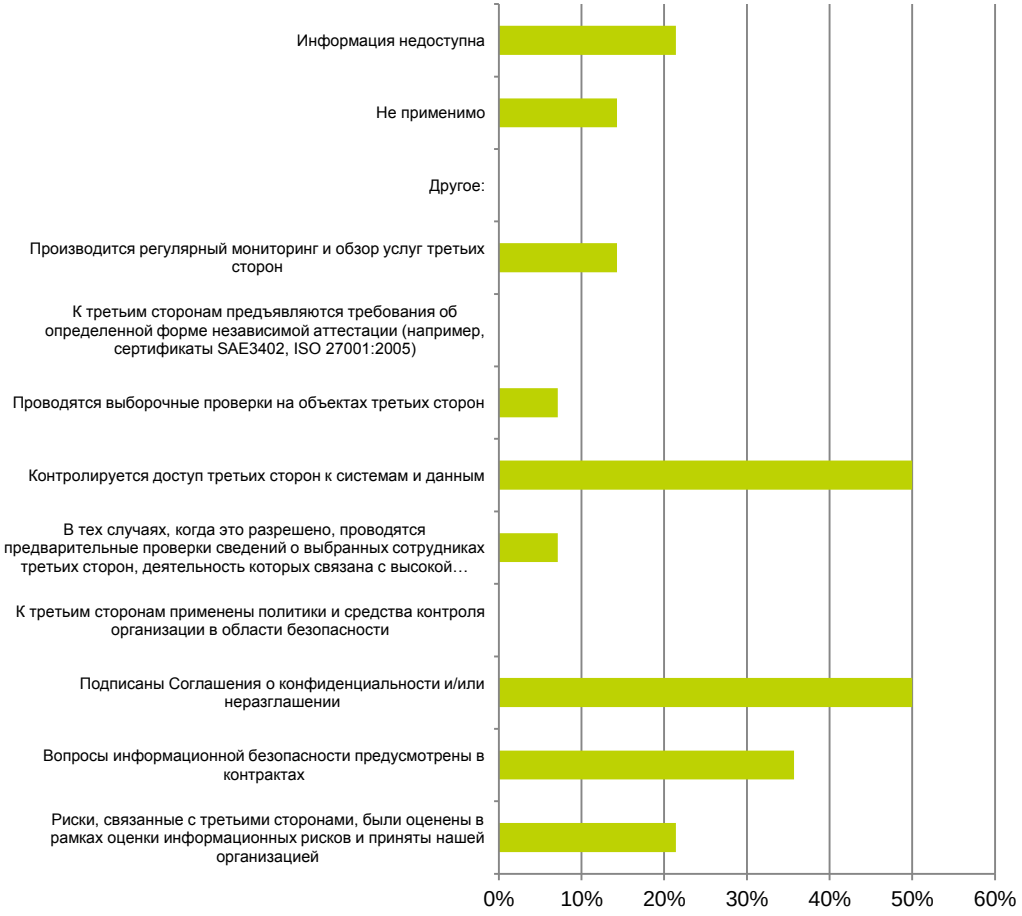
Одним из наиболее значимых результатов исследования является то, что контроль над информационной безопасностью третьих лиц (подрядчиков, поставщиков и партнеров) осуществляется главным образом на основании договорных требований и доверия.

- 50% респондентов отмечают, что контроль устанавливается соглашениями о конфиденциальности
- 36% респондентов отмечают, что контроль обеспечивается по договору

Тем не менее, 50% респондентов также отмечают, что управление обеспечивается через «политики доступа», значительно меньший процент респондентов имеет более строгие меры контроля, такие как (а) обзоры, выборочные проверки или аудит третьих лиц или (б) запрос у третьих лиц предоставления формальной сертификации (см. вопрос 21).

По всей видимости, контроль соблюдения третьими лицами, такими как поставщики и партнеры, соответствующих стандартов безопасности, является недостаточной мерой.

Вопрос 21: Каким способом ваша организация обеспечивает достаточный и надлежащий уровень информационной безопасности третьих лиц (возможны несколько вариантов ответов)?

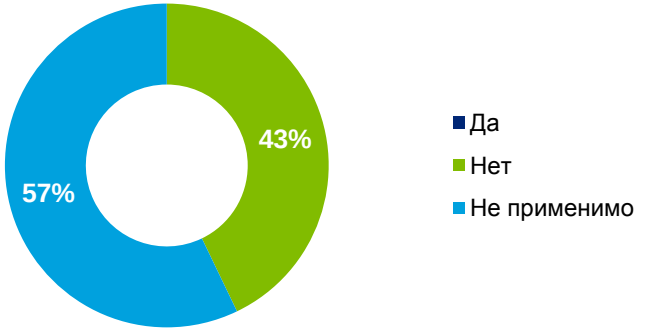


Контроль третьих лиц должен стать основным направлением деятельности организаций в Центральной Азии (2/2)

Неудивительно, что почти все респонденты не могут быть уверены в том, что третьи лица, задействованные в (существенные) операции, соблюдают необходимые стандарты информационной безопасности (см. вопросы 22 и 23).

Вопрос 22: Насколько вы уверены в мерах информационной безопасности, предпринимаемыми третьими лицами?

Вопрос 23: Делится ли ваша организация информацией о кибер-атаках с третьими сторонами?



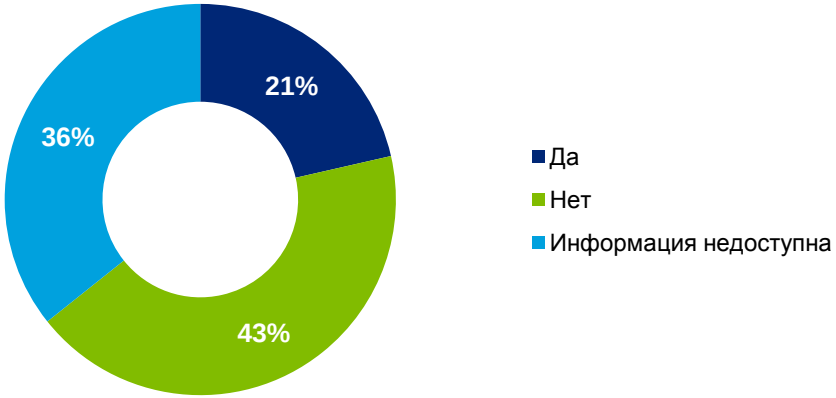
Даже если необязательно иметь договор, определяющий ответственность и обязательства по информационной безопасности, не следует полагаться исключительно на управление деловыми отношениями с третьей стороной. Не менее важно следить за соблюдением третьими лицами стандартов безопасности. Это может быть сделано несколькими способами, некоторые из которых более распространены, чем другие, но все они направлены на обеспечение того, чтобы договоры действительно выполнялись и соблюдались сторонами.

Аудит и тестирование принципов информационной безопасности

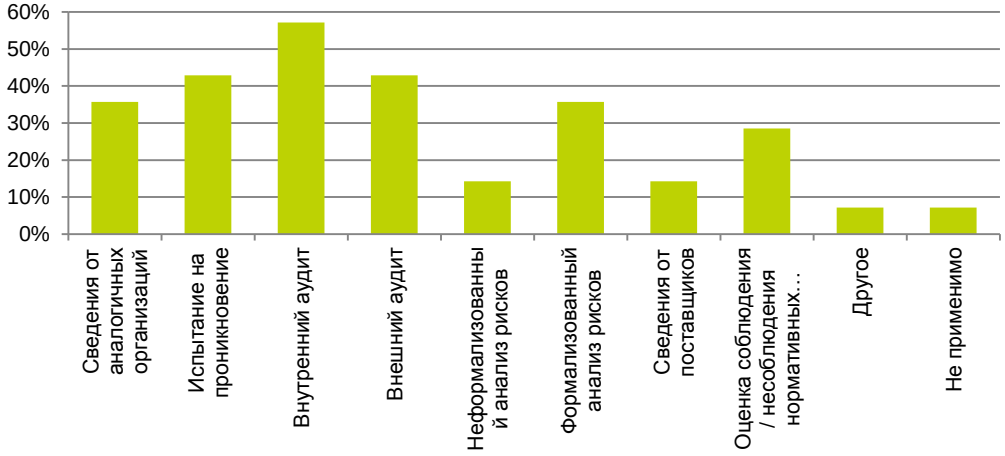
Аудит и тестирование принципов информационной безопасности (1/2)

Мы попросили респондентов указать, в какой степени их организации проводят аудит и тестирование безопасности. В целом, мы отметили, что, несмотря на то, что проводить внутреннюю «углубленную проверку пакетов» (УПП) не представляется возможным из-за отсутствия технических возможностей (см. вопрос 24), большинство организаций выполняют аудит и тестирование самостоятельно (см. вопросы 25 и 26).

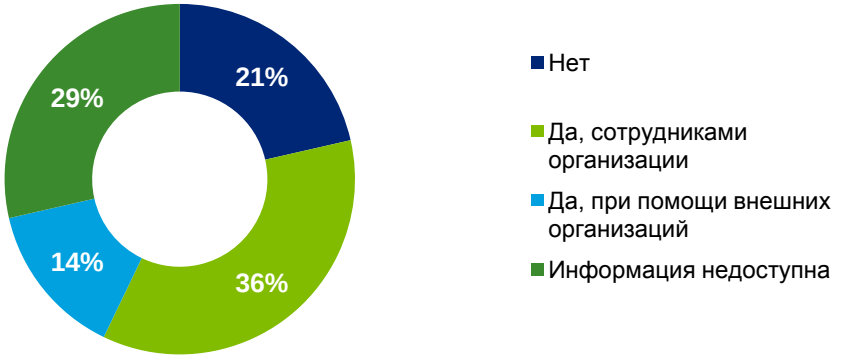
Вопрос 24: Имеет ли ваша организация технические возможности для проведения общесетевых углубленных проверок пакетов?



Вопрос 25: Как вы выделяете недостатки, риски и несоблюдения безопасности в вашей организации (возможно несколько вариантов ответов)?

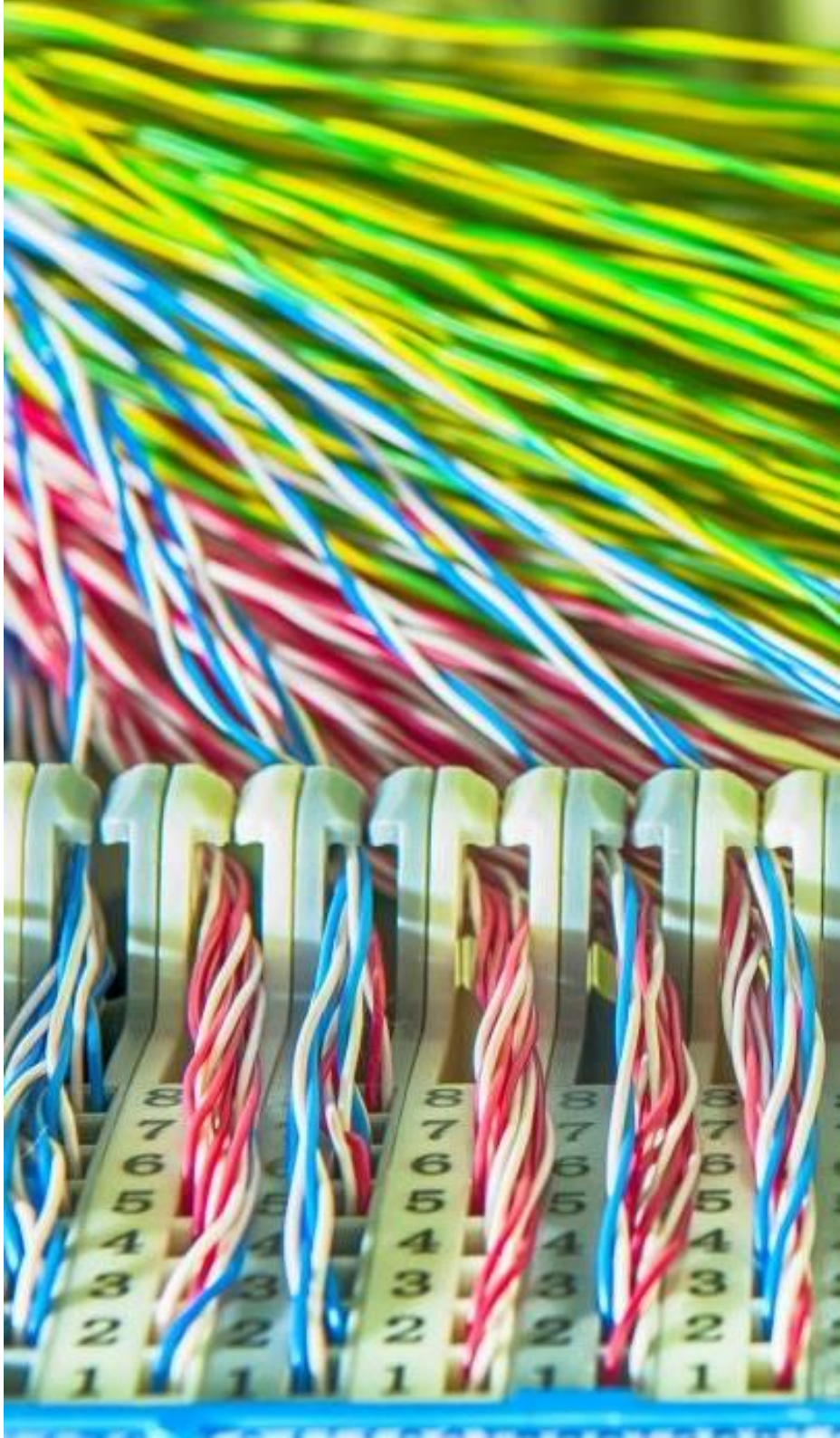


Вопрос 26: Проводилось ли когда-нибудь в Вашей организации тестирование на возможность несанкционированного доступа?



Аудит и тестирование принципов информационной безопасности (2/2)

Аудит и тестирование может дать важную информацию для высшего руководства о текущем состоянии зрелости информационной безопасности в организации. Для наибольшей эффективности, тестирование и аудит должны проводить профессионалы с обширными знаниями в вопросах информационной безопасности, передовой практики и международных достижений с тем, чтобы выявить потенциальные недостатки, которые могут быть использованы хакерами, и предоставить рекомендации о том, как их решить. Регулярное тестирование и аудит позволит снизить риск стать жертвой кибер-атаки.



Контакты:

Михель ван Хюльстейн
Старший менеджер
Тел: +7 (727) 258 13 40
Вн. 2796
Факс +7 (727) 258 13 41
Мобильный: +7 (777) 438 4518
Эл. почта: mvanhulsteijn@deloitte.kz

Сергей Буханов
Директор
Тел:+7 (495) 580-9778
Вн. 3032
Факс: +7 (495) 787 06 01
Мобильный: +7 (985) 787 6054
Эл. почта: sbuhanov@Deloitte.ru

Айтуар Акимжанов
Старший консультант
Тел: +7 (727) 258 13 40
Вн. 2782
Факс: +7 (727) 258 13 41
Мобильный: +7 (707) 555 5988
Эл. почта: aakimzhanov@deloitte.kz

Казахстан
пр. Аль-Фараби, 36
г. Алматы, 050059
Тел.: +7 (727) 258 13 40
Факс: +7 (727) 258 13 41

Кыргызстан
ул. Раззакова 19
Бизнес центр «Россия»
Офис 905/906
г. Бишкек, 720040
Тел.: +996 (312) 39 82 88
Факс: +996 (312) 39 82 89

Таджикистан
ул. Айни, 24а,
офис 307, Бизнес центр «С.А.С.»
г. Душанбе, 734012
Тел.: +992 (44) 600 62 00
Факс: +992 (44) 600 62 01

Узбекистан
Бизнес центр «Инконель»
Проспект Мустакиллик, 75
г. Ташкент, 100000
Тел.: +998 (71) 120 44 45/46
Факс: +998 (71) 120 44 47

Deloitte.