Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

## Полный отчет

Настоящий отчет содержит следующие разделы:



Партнер корпорации Майкрософт может разобрать этот отчет вместе с вами и помочь в разработке подробного плана действий по реализации рекомендаций. Если в настоящее время у вас нет сложившихся взаимоотношений с каким-либо партнером корпорации Майкрософт, вы можете ознакомиться со списком партнеров корпорации Майкрософт в области решений по обеспечению безопасности по адресу: https://solutionfinder.microsoft.com/.

---

Средств Microsoft для оценки риска, связанного с безопасностью, предназначено для оказания помощи в определении уровня риска, которому подвергается ваша вычислительная среда, и шагов, предпринятых вами с целью снижения этого уровня, а также для выработки предложений с описанием дополнительных шагов, которые можно предпринять, чтобы еще больше снизить уровень риска. Оно не заменяет аудит, который выполняется профессиональным консультантом в области безопасности.
Использование средства Microsoft для оценки риска, связанного с безопасностью, регулируется условиями лицензионного соглашения, которое прилагалось к программному обеспечению, и в отношении данного отчета также действуют исключения, отказы и ограничения, которые содержатся в лицензионном соглашении.

Этот отчет предоставляется только для информационных целей. Ни корпорация Майкрософт, ни ее поставщики и партнеры не делают никаких заявлений и не дают никаких гарантий, будь то явные или подразумеваемые, относительно средства Microsoft для оценки риска, связанного с безопасностью, его использования, точности или надежности результатов оценок и сведений, содержащихся в этом отчете.

---

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

# Итоговый отчет

## Введение

Средство Microsoft для оценки риска, связанного с безопасностью, предназначено для оказания помощи в определении и устранении угроз безопасности в существующей вычислительной среде. В данном средстве реализован целостный подход к оценке стратегии обеспечения безопасности с учетом персонала, процессов и технологий. Кроме полученных результатов, приводятся рекомендации по снижению риска, а также ссылки на дополнительную информацию, которая содержит другие необходимые советы. Эти ресурсы могут помочь в получении дополнительных знаний о специальных средствах и методах, позволяющих повысить безопасность среды.

Этот раздел, содержащий итоговые сведения, предназначен для того, чтобы дать ИТ-менеджерам и высшему руководству представление о текущей ситуации с общей безопасностью в компании. Подробные результаты и рекомендации приводятся в приведенном далее детальном отчете.

## Вводные данные: процесс и масштабы оценки

Оценка предназначена для выявления риска для бизнеса организации и определения мер безопасности, предпринимаемых для снижения риска. Сосредоточение внимания на общих проблемах этого сегмента рынка позволило разработать вопросы для обеспечения высококачественной оценки рисков, которые представляют для ведения бизнеса используемые технологии, процессы и персонал.

Профиль риска для бизнеса (ПРБ) создается средством на основе серии предварительных вопросов о бизнес-модели компании, и тем самым измеряется риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Вторая группа вопросов предлагается с целью составления списка мер безопасности, которые со временем должны быть предприняты компанией. В целом, эти меры безопасности формируют уровни защиты, обеспечивающие более серьезную защиту от угроз безопасности и конкретных уязвимых мест в системе. Каждый уровень способствует укреплению комбинированной стратегии эшелонированной защиты. В сумме это рассматривается как индекс эшелонированной защиты (DiDI). Затем ПРБ и DiDI сравниваются для измерения распределения риска по всем областям анализа — инфраструктуре, приложениям, операциям, персоналу.

Кроме измерения соотношения угрозы безопасности и методов защиты, средство также измеряет уровень безопасности организации. Уровень безопасности подразумевает развитие высокоэффективных и стабильных методик обеспечения безопасности. При низком значении используется ограниченное число методов защиты, а действия предпринимаются постфактум. При высоком значении практикуются устоявшиеся и проверенные процессы, которые позволяют компании предпринимать упреждающие меры и при необходимости реагировать еще эффективнее и согласованнее.

Для конкретной среды предлагаются рекомендации по управлению рисками, учитывающие уже развернутые технологии, текущее состояние безопасности и стратегии эшелонированной защиты. Выработанные предложения предназначены для того, чтобы помочь перейти к общепризнанным передовым методикам.

Данная оценка — включающая вопросы, меры и рекомендации — предназначена для средних предприятий (организаций), в среде которых насчитывается от 50 до 500 настольных компьютеров. Она предполагает более обширную защиту областей потенциального риска во всей среде, а не проведение углубленного анализа конкретной технологии или процесса. Как результат, данное средство не рассчитано на измерение эффективности используемых мер безопасности. Таким образом, настоящий отчет следует использовать как

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02
предварительное руководство, позволяющее сосредоточить внимание на определенных областях, требующих более пристального изучения. Он не должен заменять оценки в специфических областях, предлагаемые компетентными сторонними группами оценки.

## Ситуационный анализ

В этом разделе, исходя из представленных вами ответов, в графическом виде представлены концепции, описанные выше, для вашей организации. Напоминание:

- ПРБ является мерой, отражающей риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели.
- DiDI - это величина измерения защитных мер по обеспечению безопасности, используемых в отношении персонала, процессов и технологий для снижения рисков, выявленных на предприятии.
- Уровень безопасности - это величина измерения способностей организации к эффективному использованию инструментов, доступных для создания стабильного уровня безопасности по многим дисциплинам.

[См. Приложения для получения дополнительных сведений об этих терминах и методах интерпретации графиков.]

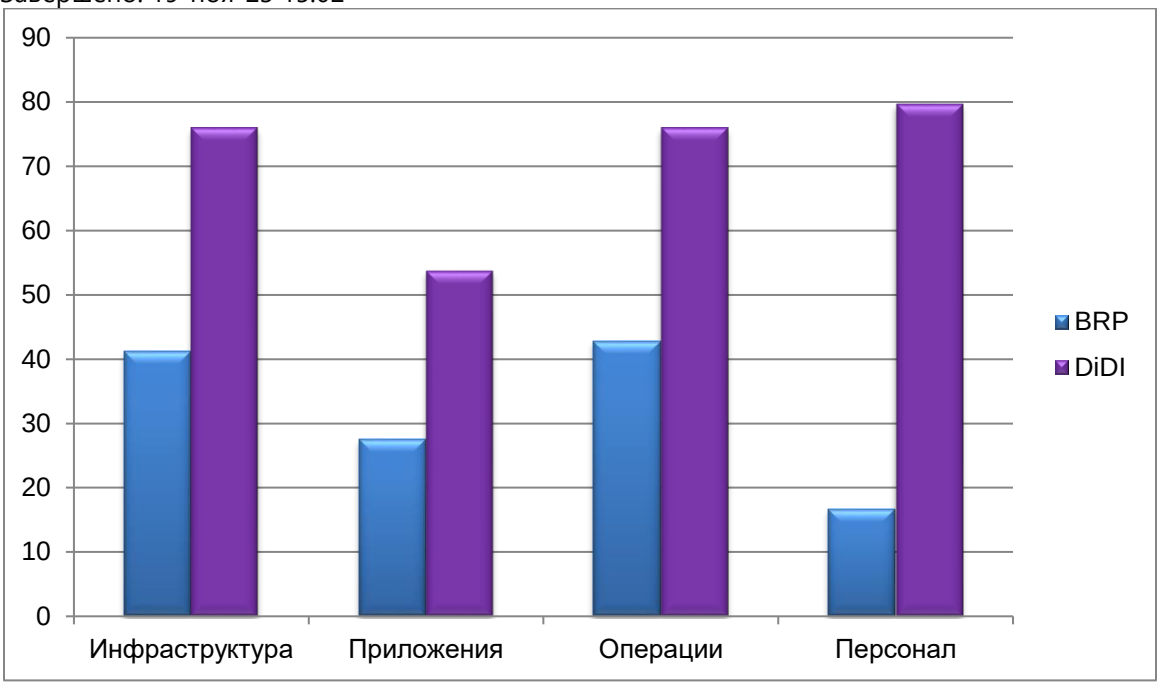
## Результаты:

| Области анализа | Сравнение риска и защиты | уровень безопасности |
|---|---|---|
| Инфраструктура | 🔴 | 🟢 |
| Приложения | 🔴 | 🟢 |
| Операции | 🔴 | 🟢 |
| Персонал | 🔴 | 🟢 |

## Risk-Defense

Данная диаграмма отображает разность показателей эшелонированной защиты, упорядоченных по областям анализа.

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02




Вообще, для одной и той же категории лучше всего иметь и рейтинг DiDI, и рейтинг ПРБ. Дисбаланс внутри одной категории или между разными категориями — в любом направлении — может означать необходимость перегруппировки инвестиций в ИТ.

## уровень безопасности

Уровень безопасности включает элементы управления (как физические, так и технические), техническую интуицию ИТ-ресурсов, политику, процесс и стабильные методики. Уровень безопасности можно измерить только способностью организации к эффективному использованию инструментов, доступных для создания стабильного уровня безопасности по многим дисциплинам. Для определения областей, на которые должны быть нацелены программы безопасности организации, необходимо установить и применить базис уровня безопасности. Не все организации могут достичь оптимизированного уровня, однако все они должны оценить, на каком уровне они находятся и на каком должны находиться, учитывая существующий риск для бизнеса. Например, компании, осуществляющей деятельность в среде с низким риском, усовершенствования, находящиеся выше верхнего предела уровня "Базис" или ниже нижнего предела уровня "Стандарт", могут никогда не потребоваться. Компании же, осуществляющей деятельность в среде с высоким риском, возможно, потребуется выйти на уровень "Оптимизация". Показатели профиля риска для бизнеса помогают оценить уровень риска.

| | |
|---|---|
| **уровень безопасности** | Величина, позволяющая сравнить методики, используемые компанией, с передовыми отраслевыми методиками с точки зрения стабильного уровня безопасности. Каждая компания должна стремиться к тому, чтобы ее уровень безопасности и связанная с ним стратегия безопасности соответствовали рискам, возникающим в процессе ведения бизнеса: |
| **Базис** | В качестве первичного механизма защиты применены некоторые упреждающие меры безопасности; в текущей деятельности и при реагировании на происшествия меры предпринимаются постфактум |
| **Стандарт** | В соответствии с определенной стратегией, развернуто несколько уровней защиты |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

**Оптимизация** Эффективная защита по правильным направлениям с использованием надлежащих мер и постоянное использование передовых методик

## Результаты

Исходя из ваших ответов на вопросы, связанные с оценкой рисков, вашим защитным мерам присвоены следующие рейтинги. В разделах Подробная оценка и Список рекомендуемых действий настоящего отчета содержатся более подробные сведения о результатах, передовых методиках и рекомендациях.

Подпись: ●Соответствует передовым методикам ●Требует усовершенствования ●Неудовлетворительно

| | |
|---|---|
| **Инфраструктура** | ● |
| **Защита по периметру** | ● |
| Правила и фильтры межсетевого экрана | ● |
| Антивирус | ● |
| Антивирус - Настольные компьютеры | ● |
| Антивирус - Серверы | ● |
| Удаленный доступ | ● |
| Сегментация | ● |
| Система определения вторжения (IDS) | ● |
| Беспроводная связь | ● |
| **Проверка подлинности** | ● |
| Административные пользователи | ● |
| Внутренние пользователи | ● |
| Пользователи с удаленным доступом | ● |
| Политики паролей | ● |
| Политики паролей - Учетная запись администратора | ● |
| Политики паролей - Учетная запись пользователя | ● |
| Политики паролей - Учетная запись для удаленного доступа | ● |
| Неактивные учетные записи | ● |
| **Управление и контроль** | ● |
| Нарушения безопасности: реагирование и создание отчетов | ● |
| Защищенная сборка | ● |
| Физическая безопасность | ● |
| **Приложения** | ● |
| **Развертывание и использование** | ● |
| Балансировка нагрузки | ● |
| Кластеризация | ● |

| | |
|---|---|
| **Операции** | ● |
| **Среда** | ● |
| Узел управления | ● |
| Узел управления - Серверы | ● |
| Узел управления - Сетевые устройства | ● |
| **Политика безопасности** | ● |
| Классификация данных | ● |
| Утилизация данных | ● |
| Протоколы и службы | ● |
| Правильное использование | ● |
| Управление учетными записями | ● |
| Управление | ● |
| Политика безопасности | ● |
| **Управление средствами исправления и обновления** | ● |
| Документация о сети | ● |
| Поток данных приложений | ● |
| Управление средствами исправления | ● |
| Управление изменениями и конфигурация | ● |
| **Архивация и восстановление** | ● |
| Файлы журнала | ● |
| Планирование аварийного восстановления и возобновления деятельности предприятия | ● |
| Архивация | ● |
| Резервные носители | ● |
| Архивация и восстановление | ● |
| **Персонал** | ● |
| **Требования и оценки** | ● |
| Требования по безопасности | ● |
| Оценки безопасности | ● |
| **Политика и процедуры** | ● |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| Восстановление приложений и данных | ● |
| Независимый сторонний поставщик программного обеспечения | ● |
| Внутренняя разработка | ● |
| Уязвимые места в системе | ● |
| **Схема приложения** | ● |
| Проверка подлинности | ● |
| Политики паролей | ● |
| Авторизация и управление доступом | ● |
| Ведение журнала | ● |
| Подтверждение ввода | ● |
| Методологии разработки систем безопасности программного обеспечения | ● |
| **Хранение данных и связь** | ● |
| Шифрование | ● |
| Шифрование - Алгоритм | ● |

| | |
|---|---|
| Проверка в фоновом режиме | ● |
| Политика отдела кадров | ● |
| Сторонние взаимосвязи | ● |
| **Обучение и осведомленность** | ● |
| Осведомленность о безопасности | ● |
| Обучение в области безопасности | ● |

## Инициативы по обеспечению безопасности

В следующих областях существует недостаток передовых методик, и для повышения безопасности среды они требуют усовершенствования. В разделах Подробная оценка и Список рекомендуемых действий настоящего отчета содержатся более подробные сведения о результатах, передовых методиках и рекомендациях.

| Высокий приоритет | Средний приоритет | Низкий приоритет |
|---|---|---|
| • Пользователи с удаленным доступом<br>• Независимый сторонний поставщик программного обеспечения<br>• Уязвимые места в системе<br>• Планирование аварийного восстановления и возобновления деятельности предприятия<br>• Сторонние взаимосвязи | • Защищенная сборка<br>• Административные пользователи<br>• Удаленный доступ<br>• Методологии разработки систем безопасности программного обеспечения<br>• Система определения вторжения (IDS) | • Узел управления - Серверы<br>• Узел управления - Сетевые устройства<br>• Правильное использование<br>• Архивация<br>• Антивирус - Настольные компьютеры |

# Подробная оценка

В этом разделе отчета содержатся подробные результаты для каждой категории, а также описываются передовые методики, даются рекомендации и ссылки на дополнительную информацию. Рекомендации приведены в порядке приоритета в следующем разделе.

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

## Области анализа

В следующей таблице перечислены области, использованные для обеспечения высокого качества анализа при оценке угроз безопасности, и описана значимость каждой области для безопасности. В разделе "Подробная оценка" настоящего документа описывается состояние организации с точки зрения безопасности (исходя из предоставленных во время оценки ответов) в каждой из этих областей, а также признанные в отрасли передовые методики и рекомендации по их выполнению.

| Категория | Важность для обеспечения безопасности |
|---|---|
| **Профиль риска для бизнеса** | |
| Профиль риска для бизнеса | Понимание того, каким образом характер вашей деятельности оказывает влияние на риск, имеет огромное значение для определения тех областей, в которых следует применить ресурсы, чтобы ослабить угрозу безопасности. Распознавание критических областей риска для бизнеса поможет оптимизировать выделение средств на обеспечение безопасности. |
| **Инфраструктура** | |
| Защита по периметру | Защита по периметру направлена на обеспечение безопасности на границах сети, где внутренняя сеть соединяется с внешним миром. Благодаря этому создается первая линия защиты от нежелательного вторжения. |
| Проверка подлинности | Строгие процедуры проверки подлинности для пользователей, администраторов и удаленных пользователей гарантируют невозможность получения несанкционированного доступа к сети с помощью локальных или удаленных атак. |
| Управление и контроль | Управление, контроль и правильное ведение файлов журналов являются важными условиями для обслуживания и анализа среды ИТ. Важность этих инструментов еще более повышается после того, как имела место атака и требуется выполнить анализ происшествия. |
| **Приложения** | |
| Развертывание и использование | При развертывании основных бизнес-приложений на производстве должна быть обеспечена как безопасность, так и доступность этих приложений и серверов. Непрерывное обслуживание имеет важное значение для своевременного создания исправлений, позволяющих устранить ошибки системы безопасности, и предотвращения появления новых проблем безопасности в среде. |
| Схема приложения | Схема, которая неверно работает с такими механизмами обеспечения безопасности, как проверка подлинности, авторизация и проверка данных, помогает злоумышленникам воспользоваться уязвимыми местами в системе безопасности и тем самым получить доступ к конфиденциальной информации. |
| Хранение данных и связь | Целостность и конфиденциальность данных - это одна из главных забот на любом предприятии. Потеря или кража данных может неблагоприятно сказаться на доходах организации и ее репутации. Важно понимать, каким образом приложения обрабатывают важные бизнес-данные и как эти данные защищены. |
| **Операции** | |
| Среда | Безопасность организации зависит от эксплуатационных процедур, |

| | |
|---|---|
| | процессов и руководящих принципов, применяемых в среде. Они могут повысить безопасность организации благодаря тому, что представляют собой нечто большее, чем просто методы защиты технологий. Точная документация, относящаяся к среде, и правильные инструкции очень важны для группы по вопросам эксплуатации, так как они влияют на ее способность поддерживать и сохранять безопасность среды. |
| Политика безопасности | Корпоративная политика безопасности связана с существующими индивидуальными политиками и инструкциями, которые позволяют управлять безопасным и надлежащим использованием технологии и процессов в организации. Эта область охватывает политики, направленные на обеспечение всех видов безопасности, относящихся к пользователю, системе и данным. |
| Управление средствами исправления и обновления | Надлежащее управление исправлениями и обновлениями имеет важное значение для обеспечения безопасности в среде ИТ организации. Своевременное применение исправлений и обновлений является обязательным условием для обеспечения защиты от известных проблем безопасности, которые могут быть использованы злоумышленниками. |
| Архивация и восстановление | Архивация и восстановление данных - важная часть поддержки непрерывности ведения бизнеса в случае аварии или отказа аппаратного/программного обеспечения. Если в процедурах архивации и восстановления существуют ошибки или недостатки, они могут привести к значительным потерям данных и производительности. |
| **Персонал** | |
| Требования и оценки | Все лица, принимающие решения, должны понимать требования по безопасности и следовать им, с тем чтобы их технические решения и бизнес-решения повышали безопасность, а не противоречили ей. Регулярно проводимые независимые оценки помогут компании рассмотреть, оценить и определить области, требующие улучшения. |
| Политики и процедуры | Четкие практические процедуры для управления взаимосвязями с поставщиками и партнерами помогают ограничить подверженность компании риску. Процедуры, связанные с наймом сотрудников и их увольнением, помогают компании защититься от недобросовестных и недовольных сотрудников. |
| Обучение и осведомленность | Необходимо проводить обучение сотрудников и разъяснять им важность обеспечения безопасности в повседневной работе, чтобы они не подвергали компанию всевозможным рискам. |

## Оценочный анализ

Этот раздел содержит четыре части, посвященные основным областям анализа — инфраструктуре, приложениям, операциям и персоналу.

### Инфраструктура

Под безопасностью инфраструктуры подразумевается то, каким образом должна функционировать сеть, какие бизнес-процессы (внутренние или внешние) она должна поддерживать, как создаются и развертываются узлы и как организовать управление сетью и ее обслуживание. Действенная безопасность инфраструктуры обеспечит значительные улучшения в областях сетевой защиты, реагирования на происшествия, сетевой доступности и анализа отказов. Создав надежную и понятную инфраструктуру и следуя ей, организация получает возможность определить области риска и разработать способы его снижения. Оценка

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02
предусматривает проверку процедур высокого уровня, которые организация может применять для снижения угрозы со стороны инфраструктуры, сосредоточившись на следующих областях безопасности, связанных с инфраструктурой:

- Защита по периметру — Межсетевые экраны, Антивирусные программы, Удаленный доступ, Сегментация
- Проверка подлинности — Политики паролей
- Управление и контроль — Узлы управления, Файлы журналов
- Рабочая станция — Конфигурация сборки

| **Защита по периметру** | | |
|---|---|---|
| **Подкатегория** | **Передовые методики** | |
| **Правила и фильтры межсетевого экрана** | Брандмауэры представляют собой первый уровень защиты и должны размещаться на всех точках границ сетей. Применяемые на брандмауэрах правила должны отличаться высокой степенью ограничений и устанавливаться по принципу «узел-узел» и «служба-служба».При создании правил брандмауэра и списков ACL (списки управления доступом) маршрутизатора следует уделить особое внимание защите устройств управления доступом и сети от атак. Брандмауэр должен быть по умолчанию настроен на запрет любого трафика за исключением необходимого.<br>* Организуйте поток данных с помощью сетевых ACL и правил брандмауэра.<br>* Протестируйте правила брандмауэра и списки ACL маршрутизатора, чтобы определить, достаточно ли существующих правил для предотвращения атак типа «отказ в обслуживании» (DoS).<br>* Разверните одну или несколько демилитаризованных зон (DMZ) в качестве систематического и формального расширения брандмауэра.<br>* Разместите в демилитаризованных зонах все серверы, доступ к которым осуществляется через Интернет. Ограничьте входящие и исходящие подключения от демилитаризованных зон (DMZ). | |
| | **Полученные данные** | **Рекомендации** |
| **Правила и фильтры межсетевого экрана** | Вы указали, что межсетевые экраны развернуты в каждом офисе. | Продолжайте развертывать межсетевые экраны или другие элементы управления доступом на сетевом уровне в каждом офисе и регулярно проверяйте их правильную работу. |
| **Правила и фильтры межсетевого экрана** | Ваши ответы указывают на то, что вы не только развернули межсетевые экраны на границах сети, но и приняли также дополнительные меры предосторожности, создав один или более сегментов демилитаризованной зоны | Регулярно проверяйте политику межсетевого экрана и удаляйте устаревшие или неподходящие правила. Введите правила проверки входного и выходного доступа и рассмотрите необходимость реализации выходных |

| | | |
|---|---|---|
| | (ДМЗ) для защиты ресурсов, доступных по Интернету. | фильтров для предотвращения лишних исходящих подключений.<br>Ограничьте прямой доступ внутренних пользователей к сегментам демилитаризованной зоны (ДМЗ), так как маловероятно, что они будут работать с хост-компьютерами, находящимися в ДМЗ на постоянной основе.<br>Ограничьте доступ из основной сети в сегмент ДМЗ только конкретными узлами или административными сетями. |
| **Правила и фильтры межсетевого экрана** | Вы указали, что для защиты серверов используется программное обеспечение межсетевого экрана на хост-компьютере. | Продолжайте устанавливать узловые межсетевые экраны на все серверы и рассмотрите необходимость использования этого программного обеспечения на всех настольных и переносных компьютерах в организации. |
| **Правила и фильтры межсетевого экрана** | Вы указали, что межсетевой экран регулярно проверяется для обеспечения должной производительности. | Продолжайте регулярную проверку межсетевого экрана. Проверьте правильную работу межсетевого экрана по отношению не только к внешнему, но также и внутреннему трафику. |
| **Подкатегория** | **Передовые методики** | |
| **Антивирус** | Разверните антивирусное программное обеспечение во всей среде предприятия, как на уровне сервера, так и на уровне настольных компьютеров. Разверните специализированные антивирусные решения для выполнения конкретных задач, например средства проверки файловых серверов, средства отслеживания содержимого, а также средства проверки отправляемых и загружаемых данных. Настройте антивирусное программное обеспечение на поиск вирусов, пытающихся как проникнуть в ИТ-среду предприятия, так и покинуть ее.Антивирусное программное обеспечение должно быть в первую очередь установлено на критически важных файловых серверах. Затем область действия антивирусных программ следует распространить на почту, базы данных и веб-серверы.<br>Антивирусное программное обеспечение настольных и переносных компьютеров следует включить в устанавливаемый по умолчанию набор программ.<br>При работе с сервером Microsoft Exchange следует использовать его дополнительные возможности по антивирусной защите и фильтрации содержимого на уровне почтовых ящиков. | |

| | Полученные данные | Рекомендации |
|---|---|---|
| **Антивирус** | Вы указали, что на почтовых серверах не установлено антивирусное программное обеспечение. | На всех компьютерах среды организации необходимо установить антивирусное программное обеспечение. |
| **Антивирус** | Вы указали, что на шлюзах доступа не установлено антивирусное программное обеспечение. | На всех компьютерах среды организации необходимо установить антивирусное программное обеспечение. |
| **Подкатегория** | **Передовые методики** | |
| **Антивирус - Настольные компьютеры** | | |
| | **Полученные данные** | **Рекомендации** |
| **Антивирус - Настольные компьютеры** | Ваш ответ указывает на то, что антивирусные решения развернуты на уровне настольного компьютера. | Продолжайте использовать такую практику. Реализуйте политику, в соответствии с которой пользователям необходимо регулярно обновлять сигнатуры вирусов. Рассмотрите необходимость установки клиента антивирусной программы с использованием настроек для рабочей станции по умолчанию. |
| **Подкатегория** | **Передовые методики** | |
| **Антивирус - Серверы** | | |
| | **Полученные данные** | **Рекомендации** |
| **Антивирус - Серверы** | Вы указали, что антивирусные решения не развернуты на уровне сервера. | Рассмотрите необходимость развертывания антивирусного решения сначала на критических файловых серверах, а затем на почтовых серверах, серверах баз данных и веб-серверах. Если используется Microsoft Exchange, рассмотрите необходимость активизации дополнительных антивирусных функций и функции фильтров содержимого на уровне почтового ящика. |
| **Подкатегория** | **Передовые методики** | |
| **Удаленный доступ** | В целях обеспечения единообразия при проверке и оценке проблем и нарушений важно строго следовать задокументированным процедурам создания отчетов и реагирования на эти проблемы и нарушения.<br>Важно, чтобы все пользователи осознавали свою ответственность за своевременное сообщение о любых нарушениях или проблемах, связанных с безопасностью. Поэтому необходимо иметь четко определенный процесс создания отчетов о подобных проблемах. | |

| | Полученные данные | Рекомендации |
|---|---|---|
| **Удаленный доступ** | Ваши ответы указывают на то, что вы не только реализовали VPN для удаленного доступа, но и задействовали также многофакторную проверку подлинности в качестве второй линии защиты. | Следует проводить регулярную проверку списка доступа для всех пользователей на устройстве в сети VPN. Рассмотрите необходимость управления устройством в сети VPN только из внутренней корпоративной сети. |
| **Удаленный доступ** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Подкатегория** | **Передовые методики** | |
| **Сегментация** | Сегментация используется для отделения определенных внешних сетей от доступа поставщика, партнера и клиента. В каждом сегменте внешней сети должна быть разрешена передача трафика только определенного приложения на определенные узлы и порты, которые используются для предоставления услуг клиентам.<br><br>Следует убедиться, что сетевые элементы управления разрешают доступ только для тех служб, которые требуются для каждого стороннего подключения.<br><br>Необходимо ограничить доступ к сетевым службам на входе и выходе, а также ограничить доступ между разными сетевыми сегментами. | |
| | **Полученные данные** | **Рекомендации** |
| **Сегментация** | Ваш ответ указывает на то, что в сети вашей организации размещены службы, связанные с Интернетом. | Убедитесь в наличии межсетевого экрана, сегментирования и систем определения вторжения для защиты инфраструктуры компании от атак из Интернета. |
| **Сегментация** | Вы указали, что в сети имеется более одного сегмента. | Продолжайте использовать сегментацию сети для оптимизации управления сетевым трафиком и ограничения доступа к ресурсам в зависимости от требований к пользователям. |
| **Сегментация** | Ваш ответ указывает на то, что | Постоянно совершенствуйте |

| | | |
|---|---|---|
| | в вашей среде уже реализована сегментация сети. | сеть, используя перечисленные передовые методики. Каждая внешняя сеть должна находиться в своем сегменте, а возможность обмена данными между сетевыми сегментами и внутренними корпоративными ресурсами должна быть ограничена. |
| **Подкатегория** | **Передовые методики** | |
| **Система определения вторжения (IDS)** | Сетевые и узловые системы определения вторжения необходимо разворачивать для определения и уведомления об атаках корпоративных систем. | |
| | **Полученные данные** | **Рекомендации** |
| **Система определения вторжения (IDS)** | Вы указали, что у вас используется сетевая система определения вторжения (HIDS) | Продолжайте практику развертывания сетевой системы определения вторжения. Следите за регулярным обновлением сигнатур вирусов, а также изучайте технологии предотвращения вторжения, так они становятся широко востребованными. |
| **Система определения вторжения (IDS)** | Вы указали, что у вас не используется узловая система определения вторжения (HIDS) | Рассмотрите необходимость развертывания узловых систем определения вторжения для оповещения администраторов об атаках, предпринятых против узлов, чтобы они могли своевременно реагировать на них. |
| **Подкатегория** | **Передовые методики** | |
| **Беспроводная связь** | Передовые методики для беспроводной реализации должны гарантировать невыполнение сетью широковещательной рассылки SSID, использование WPA-шифрования и признание сети как не заслуживающей доверия. | |
| | **Полученные данные** | **Рекомендации** |
| **Беспроводная связь** | Вы указали, что существует возможность беспроводного подключения к сети | Чтобы уменьшить риск, связанный с беспроводными сетями, реализация должна предусматривать отмену передачи идентификатора SSID, шифрование WPA и определение доверительных отношений в сети. |
| **Беспроводная связь** | Ваш ответ указывает на то, что свойства идентификатора наборов служб (SSID) по умолчанию были изменены в точке доступа. | Изменение идентификатора SSID, заданного по умолчанию, является первым шагом в процессе повышения безопасности беспроводной сети. Однако, чтобы снизить |

| | | |
|---|---|---|
| | | риск, его необходимо выполнять вместе с другими рекомендациями. К ним относятся: отмена передачи идентификатора SSID, шифрование WPA и определение доверительных отношений в сети. |
| **Беспроводная связь** | Вы указали, что отключили широковещание идентификатора наборов служб (SSID) в точке доступа. | Отключение передачи идентификатора SSID является частью рекомендаций по повышению безопасности беспроводной сети. Однако эту меру следует использовать в сочетании с шифрованием WPA и определением доверительных отношений в сети. |
| **Беспроводная связь** | Вы указали, что в вашей беспроводной среде используется WEP-шифрование. | Несмотря на то, что шифрование WEP все же лучше, чем полное его отсутствие, лучше использовать шифрование WPA, которое является более надежным. |
| **Беспроводная связь** | Вы указали, что в вашей беспроводной среде используется WPA-шифрование. | В настоящее время WPA является стандартом наиболее безопасного шифрования, однако возможность его расшифровки все равно существует. рассмотрите необходимость использования дополнительного шифрования (например, VPN) для дополнительной защиты данных. |
| **Беспроводная связь** | Вы указали, что в вашей беспроводной среде используются ограничения MAC. | Ограничение доступа по MAC-адресам позволяет предотвратить подключение к сети посторонних компьютеров, однако эту защиту легко обойти. Рассмотрите необходимость использования проверки подлинности WPA в дополнение к MAC-фильтрам. |
| **Беспроводная связь** | Вы указали, что беспроводная сеть рассматривается как не имеющая доверия. | Рассмотрение беспроводной сети как небезопасной и требование от пользователей использовать VPN или аналогичные технологии для подключения к корпоративным ресурсам является лучшим решением для поддержания |

| | | |
|---|---|---|
| | | целостности данных, однако это не предотвращает несанкционированное подключение посторонних пользователей. Рассмотрите необходимость использования проверки подлинности WPA и ограничение MAC-адресов, чтобы разрешить доступ только для определенных пользователей. |

| **Защита по периметру - Ресурсы** | | |
|---|---|---|
| Windows Server 2008 | Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that try to connect to your network comply with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution and Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations. | http://www.microsoft.com/windowsserver2008/en/us/overview.aspx |
| Internet Security and Acceleration Server | Internet Security and Acceleration (ISA) Server 2006 is the integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users with fast and secure remote access to applications and data.Deploy ISA Server 2006 for Secure Remote Access, Branch Office Security, and Internet Access Protection. | http://www.microsoft.com/forefront/edgesecurity/default.mspx |
| Intelligent Application Gateway | Microsoft's Intelligent Application Gateway (IAG) 2007 is the comprehensive, secure remote access gateway that provides secure socket layer (SSL)-based application access and protection with endpoint security management. IAG 2007 enables granular access control, authorization, and deep content inspection from a broad range of devices and locations to a wide variety of line-of-business, intranet, and client/server resources. | http://www.microsoft.com/forefront/edgesecurity/iag/default.mspx |
| Network Access Protection | Network Access Protection (NAP) is a new platform and solution that controls access to network resources based on a client computer identity and compliance with corporate | http://technet.microsoft.com/en-us/network/bb545879.aspx |

| | |
|---|---|
| | governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access. |

| **Проверка подлинности** | | |
|---|---|---|
| **Подкатегория** | **Передовые методики** | |
| **Административные пользователи** | Для администраторских учетных записей следует реализовывать строгую политику, требующую использования сложных паролей, отвечающих следующим требованиям:<br><br>+ Алфавитно-цифровой<br>+ Строчные и прописные буквы<br>+ Хотя бы один специальный символ<br>+ Минимальная длина 14 символов<br><br>Чтобы еще более снизить риск взлома пароля, выполните следующие рекомендации:<br><br>+ Истечение срока действия пароля<br>+ Блокировка учетной записи после 7 - 10 попыток неправильного ввода пароля<br>+ Ведение журнала системы<br><br>Кроме использования сложных паролей, следует также реализовать многофакторную проверку подлинности. Следует обеспечить расширенный контроль над управлением учетными записями (запретить общие учетные записи), а также вести журнал доступа к учетной записи. | |
| | **Полученные данные** | **Рекомендации** |
| **Административные пользователи** | Вы указали, что для административного доступа к управлению устройствами и хост-компьютерами необходима многофакторная проверка подлинности. | Чтобы еще более снизить риск взлома пароля в административных учетных записях, выполните следующие рекомендации:<br>+ Истечение срока действия пароля<br>+ Блокировка учетной записи после 7 - 10 попыток неправильного ввода пароля<br>+ Ведение журнала системы |

| | | |
|---|---|---|
| **Административные пользователи** | Вы указали, что в вашей среде для безопасного управления системами и устройствами используются индивидуальные имена для входа в систему. | Продолжайте требовать введения различных учетных записей для административных/управленческих процессов, и убедитесь, что учетные данные для группы администраторов меняются часто. |
| **Административные пользователи** | Вы указали, что пользователям был предоставлен административный доступ к рабочим станциям. | Рассмотрите необходимость запрещения административных прав доступа для пользователей, чтобы ограничить возможность изменения защищенной сборки. |
| **Подкатегория** | **Передовые методики** | |
| **Внутренние пользователи** | Внедрите политику учетных записей пользователей, требующую использования сложных паролей, которые соответствуют следующим критериям:* буквенно-цифровые;<br>* с использованием нижнего и верхнего регистра;<br>* с использованием не менее одного специального символа;<br>* длиной не менее восьми символов.<br>Чтобы снизить вероятность атак с использованием пароля, введите следующие элементы управления:<br>* истечение срока пароля;<br>* блокировка учетной записи после как минимум десяти неудачных попыток входа в систему;<br>* ведение системного журнала.<br>В дополнение к использованию сложных паролей рассмотрите возможность реализации многофакторной проверки подлинности. Реализуйте дополнительные элементы управления учетными записями (с запретом на совместное использование учетных записей) и ведение журнала доступа к учетным записям. | |
| | **Полученные данные** | **Рекомендации** |
| **Внутренние пользователи** | Вы указали, что для доступа пользователей к внутренней сети и хост-компьютерам необходима многофакторная проверка подлинности. | Чтобы еще более снизить риск проникновения путем использования учетных записей низкого уровня, выполните следующие рекомендации.<br>+ Истечение срока действия пароля<br>+ Блокировка учетной записи после хотя бы 10 попыток неправильного ввода пароля<br>+ Ведение журнала системы<br><br>Убедитесь, что установлены пароли как локального доступа, так и для доступа в домен. |
| **Подкатегория** | **Передовые методики** | |
| **Пользователи с удаленным доступом** | Внедрите элементы управления на основе сложных паролей для всех пользователей удаленного доступа независимо от того, предоставляется ли доступ через телефонную сеть или через | |

| | | |
|---|---|---|
| | виртуальную частную сеть (VPN). Пароль считается сложным, если соответствует следующим критериям:* буквенно-цифровой;<br>* с использованием нижнего и верхнего регистра;<br>* с использованием не менее одного специального символа;<br>* длиной не менее восьми символов.<br>Реализуйте дополнительные меры проверки подлинности для учетных записей с разрешением на удаленный доступ. Реализуйте также дополнительные элементы управления учетными записями (с запретом на совместное использование учетных записей) и ведение журнала доступа к учетным записям.<br>В случае использования удаленного доступа особенно важно защитить рабочую среду с помощью надежных методов управления учетными записями, продуманного ведения журналов и средств обнаружения нарушений безопасности. Чтобы снизить вероятность атак методом прямого перебора паролей, можно реализовать следующие меры защиты:<br>* истечение срока пароля;<br>* блокировка учетной записи после 7—10 неудачных попыток входа в систему;<br>* ведение системного журнала.<br>Службы удаленного доступа также должны учитывать системы, которые будут использоваться для получения доступа к сети или узлам. Также необходимо учесть возможность реализации элементов управления для узлов, с которых разрешен удаленный доступ к сети. | |
| | **Полученные данные** | **Рекомендации** |
| **Пользователи с удаленным доступом** | Вы указали, что сотрудники способны удаленно подключаться к сети. | Если это еще не было сделано, рассмотрите необходимость использования многофакторной проверки подлинности для удаленного доступа и предоставьте доступ только тем сотрудникам, у которых реально существует потребность в удаленном подключении. |
| **Пользователи с удаленным доступом** | Вы указали, что для удаленного доступа пользователей к внутренней сети и хост-компьютерам необходима многофакторная проверка подлинности. | Чтобы еще более снизить риск взлома пароля через службы удаленного доступа, выполните следующие рекомендации:<br>+ Истечение срока действия пароля<br>+ Завершение сеанса пользователя<br>+ Ведение журнала системы<br><br>В случае использования удаленного доступа особенно важно защитить систему путем использования надежных практик управления учетной записью, ведения журнала, а также возможностей обнаружения |

| | | |
|---|---|---|
| | | происшествий.<br><br>В службах удаленного доступа должны также учитываться системы, которые будут использоваться для доступа к сети и узлам. Рассмотрите необходимость реализации контроля узлов, для которых разрешен доступ к сети через функцию удаленного доступа. |
| **Пользователи с удаленным доступом** | Вы указали, что подрядчики способны удаленно подключаться к сети. | Кроме использования передового опыта в отношении удаленного доступа для сотрудников, рассмотрите необходимость ограничения доступа для подрядчиков, чтобы они могли получать доступ только к тем системам, к которым они вынуждены подключаться удаленно. Рассмотрите также необходимость использования отдельной точки входа для подрядчиков, чтобы упростить контроль и ограничение доступа. |
| **Пользователи с удаленным доступом** | Вы указали, что третьи стороны не могут удаленно подключаться к сети. | Если удаленный доступ запретить, общая угроза снижается. Однако если удаленный доступ планируется или будет реализован в будущем, обязательно используйте передовой опыт при развертывании решения удаленного доступа, чтобы уменьшить риск, связанный с этим доступом. |
| **Подкатегория** | **Передовые методики** | |
| **Политики паролей** | Использование сложных паролей для всех учетных записей является ключевым элементом эшелонированной защиты. Сложные пароли должны быть длиной от 8 до 14 символов и содержать буквы, цифры и специальные символы. Для обеспечения дополнительной защиты необходимо задать минимальную длину, ведение хронологии журнала, длительность, а также преждевременное истечение срока действия паролей. Обычно срок истечения действия пароля должен задаваться следующим образом:<br><br>+ Максимальная продолжительность 90 дней<br>+ Новые учетные записи должны изменять пароль при входе в систему<br>+ 8 паролей в журнале паролей (минимум 8 дней)<br><br>Кроме использования сложных паролей, рекомендуется | |

| | |
|---|---|
| | многофакторная проверка подлинности (особенно для учетных записей администратора и удаленного пользователя).<br><br>Для всех учетных записей пользователей необходимо включить блокировку учетной записи после 10 неудачных попыток ввода пароля. Контроль блокировки учетной записи может варьироваться от простой блокировки в случае взлома пароля до необходимости вмешательства администратора для разблокировки учетной записи.<br><br>Настоятельно рекомендуется включить блокировку учетных записей администраторов (хотя бы для сетевого доступа). При этом учетная запись будет блокироваться не на консоли, а только из сети. Возможно, это устроит не все организации, особенно те, которые имеют удаленные офисы.<br><br>Для учетной записи удаленного доступа рекомендуется разблокировка учетной записи администратором, так как атаки могут оставаться незамеченными в течение значительного времени, если для отслеживания сбоев при проверке подлинности не используются другие средства. Рекомендуется выполнить следующие инструкции при реализации контроля блокировки учетной записи:<br><br>+ Блокировка после 7 - 10 неудачных попыток ввода пароля для учетных записей администратора и удаленного доступа<br>+ Блокировка после как минимум 10 неудачных попыток ввода пароля для обычных учетных записей пользователей<br>+ Необходим доступ с правами администратора для разблокировки учетных записей администратора и удаленного доступа, а также автоматическая разблокировка обычных учетных записей пользователей через 5 минут |
| **Политики паролей** | Обычно ограничения по созданию паролей для администраторов должны быть еще более строгими, чем для обычных учетных записей.<br>В системах Windows учетные записи администраторов (и учетные записи служб) должны задаваться с паролями длиной 14 символов, содержащими буквы, цифры и специальные символы. |

| **Подкатегория** | **Передовые методики** | |
|---|---|---|
| **Политики паролей - Учетная запись администратора** | | |
| | **Полученные данные** | **Рекомендации** |
| **Политики паролей - Учетная запись администратора** | Вы указали, что для учетных записей администратора реализованы политики паролей. | Рассмотрите необходимость реализации дополнительной системы защиты, связанной с учетными записями администратора, например службы ведения журналов и учета |

| | | |
|---|---|---|
| | | всех успешных и неудачных попыток проверки подлинности. Перейдите с протоколов незашифрованного текста. |
| **Подкатегория** | **Передовые методики** | |
| **Политики паролей - Учетная запись пользователя** | | |
| | **Полученные данные** | **Рекомендации** |
| **Политики паролей - Учетная запись пользователя** | Вы указали, что для учетных записей пользователей реализованы политики паролей. | Рассмотрите необходимость реализации пороговых значений для неудачных попыток проверки подлинности при входе, чтобы системным администраторам посылались соответствующие сигналы.<br>Рассмотрите необходимость тестирования политик паролей на месте. |
| **Подкатегория** | **Передовые методики** | |
| **Политики паролей - Учетная запись для удаленного доступа** | | |
| | **Полученные данные** | **Рекомендации** |
| **Политики паролей - Учетная запись для удаленного доступа** | Вы указали, что для учетных записей удаленного доступа реализованы политики паролей. | Рассмотрите необходимость реализации дополнительной системы безопасности, связанной с учетными записями удаленного доступа, в которой используются службы регистрации и мониторинга на устройстве или узле для удаленного доступа.<br>Рассмотрите необходимость реализации пороговых значений для неудачных попыток проверки подлинности при входе, чтобы системным администраторам посылались соответствующие сигналы. |
| **Подкатегория** | **Передовые методики** | |
| **Неактивные учетные записи** | Продолжайте наблюдать за неактивными учетными записями и управлять ими. | |
| **Неактивные учетные записи** | Разработайте процедуру срочного уведомления всех системных администраторов об уволенных сотрудниках для немедленного отключения их учетных записей (особенно это касается учетных записей с возможностью удаленного доступа). Рассмотрите | |

| | | |
|---|---|---|
| | необходимость проверки текущих учетных записей сотрудников, переводимых в другие отделы внутри организации. | |
| **Неактивные учетные записи** | Проверьте открытые компоненты вместе в ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). | |
| **Неактивные учетные записи** | Следует регулярно посещать узлы соответствующего поставщика для получения обновлений сигнатур вирусов и загрузки обновлений в область карантина для проверки в лабораторных условиях. Перед развертыванием обновлений необходимо убедиться, что они не вызывают конфликты с развернутыми операционными системами или приложениями. Возможности автоматического обновления для антивирусных решений необходимо отключить во всех системах, чтобы предотвратить возможное повреждение файлов при их развертывании до проверки.<br><br>Для антивирусных приложений рекомендуется развернуть центральную консоль, на которой можно будет просмотреть отчеты по устаревшим системам или отключенным программам.<br><br>При наличии удаленных пользователей, которые редко подключаются к корпоративной сети, рекомендуется использовать функцию автообновления. | |
| **Неактивные учетные записи** | Во избежание несанкционированного доступа к данным со стороны уволенного сотрудника или другого пользователя использующего учетную запись уволенного сотрудника, данные учетные записи должны своевременно отключаться. Если системные администраторы не осведомлены об изменении статуса пользователя (например при переводе пользователя в другой отдел), они не смогут своевременно повлиять на возможность доступа пользователя к системе или на возможность физического доступа. Такая ситуация может привести к несанкционированному доступу или доступу с повышенными правами таких сотрудников к данным. | |
| | **Полученные данные** | **Рекомендации** |
| **Неактивные учетные записи** | Ваш ответ указывает на то, что в вашей среде все же существуют политики для обновления базы известных вирусов. | Регулярно просматривайте узлы поставщиков и систем безопасности для ознакомления с предупреждениями о недавних атаках и появлении новых вирусов. Регулярно выполняйте аудит удаленных пользователей, чтобы проверить, выполняют ли они обновление своих систем. Постоянно выполняйте необходимые процедуры, используя перечисленные передовые методики. |

| | | |
|---|---|---|
| **Неактивные учетные записи** | Ответ указывает на то, что в организации отсутствует формальный процесс проверки неактивных учетных записей пользователей. | Разработайте процедуру срочного уведомления всех системных администраторов об уволенных сотрудниках для немедленного отключения их учетных записей (особенно это касается учетных записей с возможностью удаленного доступа). Рассмотрите необходимость проверки текущих учетных записей сотрудников, переводимых в другие отделы внутри организации. |
| **Неактивные учетные записи** | Ваш ответ указывает на отсутствие политики обновления базы известных вирусов для антивирусного решения. | Проведите работу по разработке политики, требующей регулярных обновлений сигнатур вирусов для антивирусных решений. Регулярно просматривайте узлы поставщиков и систем безопасности для ознакомления с предупреждениями о недавних атаках и появлении новых вирусов и обновляйте сигнатуры вирусов для всех развернутых антивирусных решений.<br><br>Требуйте от удаленных пользователей регулярного обновления их систем. |

| **Проверка подлинности - Ресурсы** | | |
|---|---|---|
| Windows Server 2008 | Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that try to connect to your network comply with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution and Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations. | http://www.microsoft.com/windowsserver2008/en/us/overview.aspx |
| Windows Server Active Directory | A central component of the Windows platform, Active Directory directory service provides the means to manage the identities and relationships that make up network environments. Windows | http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx |

| | | |
|---|---|---|
| | Server 2003 makes Active Directory simpler to manage, easing migration and deployment. Windows Server Active Directory is already used by companies around the world to gain unified management of identities and resources across the enterprise network. Active Directory enables organizations to centrally manage and track information about users and their privileges. In addition, Active Directory Lightweight Directory Services (ADLDS), an LDAP directory service, provides organizations with flexible support for directory-enabled applications. Integration with Microsoft Federated Identity, Strong Authentication, Information Protection and Identity Lifecycle Management solutions, makes Active Directory an ideal foundation for building a comprehensive identity and access solution. | http://www.microsoft.com/windowsserver2003/technologies/idm/DirectoryServices.mspx |
| Windows Server Group Policy | Group Policy provides an infrastructure for centralized configuation management for the operating system and applications that run oh the operating system. Group Policy is supported in both Windows Server 2003 and has advanced features in Windows Server 2008 to extend the current configuration capabilites. | http://technet2.microsoft.com/windowsserver2008/en/library/3b4568bc-9d3c-4477-807d-2ea149ff06491033.mspx?mfr=true |
| Windows Server 2003 - Internet Authenication Services (IAS) | Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2003. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers. In Windows Server 2008, IAS has been replaced with Network Policy Server (NPS). | http://technet.microsoft.com/en-us/network/bb643123.aspx |
| Windows Server 2008 - Network Policy Server (NPS) | Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2008. NPS is the replacement for Internet Authentication Service (IAS) in Windows Server 2003. As a RADIUS server, NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, NPS forwards authentication and accounting messages to other RADIUS servers. NPS also acts as a health evaluation server for Network Access Protection (NAP). | http://www.microsoft.com/windows/products/windowsvista/enterprise/benefits/operatingsystem.mspx?tab=Improve%20Security%20and%20Compliance |

| | | |
|---|---|---|
| Public Key Infrastructure | Microsoft Public Key Infrastructure (PKI) for Windows Server 2003 provides an integrated public key infrastructure that enables you to secure and exchange information with strong security and easy administration across the Internet, extranets, intranets, and applications. | http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx |
| Certificates | Windows Certificate Services (CS) provides an integrated public key infrastructure that enables the secure exchange of information. With strong security and easy administration across the Internet, extranets, intranets, and applications, CS provides customizable services for issuing and managing the certificates used in software security systems employing public key technologies. | http://www.microsoft.com/windowsserver2003/technologies/idm/StrongAuthentication.mspx |
| Microsoft Identity Lifecycle Manager | Microsoft Identity Lifecycle Manager 2007 (ILM 2007) provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. It provides identity synchronization, certificate and password management, and user provisioning in a single solution that works across Microsoft Windows and other organizational systems. As a result, IT organizations can define and automate the processes used to manage identities from creation to retirement. | http://www.microsoft.com/windowsserver2003/technologies/idm/ILM.mspx |

| **Управление и контроль** | |
|---|---|
| **Подкатегория** | **Передовые методики** |
| **Нарушения безопасности: реагирование и создание отчетов** | Продолжайте следовать формальным процедурам реагирования на нарушения безопасности и предоставления отчетов. |
| **Нарушения безопасности: реагирование и создание отчетов** | Разработайте и внедрите процедуры создания отчетов и реагирования на нарушения безопасности, а также на все проблемы, связанные с безопасностью. Назначьте группу быстрого реагирования, состоящую из представителей различных служб, включая технических специалистов, руководящих работников и юристов, чтобы обеспечить своевременное реагирование на все возможные проблемы, связанные с нарушением безопасности. Рассмотрите необходимость реализации комплексной программы реагирования на нарушения безопасности, включающей создание групп быстрого реагирования, управление содержимым, анализ и процедуры реагирования на нарушения безопасности. |
| **Нарушения безопасности: реагирование и создание отчетов** | Проверьте открытые компоненты вместе в ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). |

| | | |
|---|---|---|
| **Нарушения безопасности: реагирование и создание отчетов** | Планы аварийного восстановления и возобновления деятельности предприятия должны быть документально оформлены и соответствовать современным требованиям. Это позволит обеспечивать восстановление в приемлемые сроки. Планы (включая планы восстановления приложений из резервных копий) должны регулярно тестироваться на полноту и правильность.<br>Планы непрерывной работы должны охватывать всю среду предприятия, включая ее физические и технологические составляющие, а также персонал. | |
| **Нарушения безопасности: реагирование и создание отчетов** | В целях обеспечения единообразия при проверке и оценке проблем и нарушений важно строго следовать задокументированным процедурам создания отчетов и реагирования на эти проблемы и нарушения. Важно, чтобы все пользователи осознавали свою ответственность за своевременное сообщение о любых нарушениях или проблемах, связанных с безопасностью. Поэтому необходимо иметь четко определенный процесс создания отчетов о подобных проблемах. | |
| | **Полученные данные** | **Рекомендации** |
| **Нарушения безопасности: реагирование и создание отчетов** | Ваши ответы указывают на то, что в создаваемых рабочих станциях не используется формальный образ или документация. | Создайте безопасный образ для каждого типа рабочей станции. Следует регулярно выполнять обновления, устанавливая последние пакеты обновления, исправления и другие меры безопасности. |
| **Нарушения безопасности: реагирование и создание отчетов** | Ответ указывает на то, что организация следует единообразным, формальным и документально закрепленным процессам реагирования на нарушения безопасности и предоставления отчетов. | Продолжайте следовать формальным процедурам реагирования на нарушения безопасности и предоставления отчетов. |
| **Нарушения безопасности: реагирование и создание отчетов** | Ответ указывает на то, что организация не следует единообразным, формальным или документально закрепленным процессам реагирования на нарушения безопасности и предоставления отчетов. | Разработайте и внедрите процедуры создания отчетов и реагирования на нарушения безопасности, а также на все проблемы, связанные с безопасностью. Назначьте группу быстрого реагирования, состоящую из представителей различных служб, включая технических специалистов, руководящих работников и юристов, чтобы обеспечить своевременное реагирование на все возможные проблемы, связанные с нарушением безопасности. Рассмотрите |

| | | |
|---|---|---|
| | | необходимость реализации комплексной программы реагирования на нарушения безопасности, включающей создание групп быстрого реагирования, управление содержимым, анализ и процедуры реагирования на нарушения безопасности. |
| **Подкатегория** | **Передовые методики** | |
| **Защищенная сборка** | | |
| | **Полученные данные** | **Рекомендации** |
| **Защищенная сборка** | Вы указали, что персональные межсетевые экраны установлены на всех рабочих станциях в среде. | Рассмотрите необходимость развертывания сначала личных межсетевых экранов на всех мобильных переносных компьютерах. По умолчанию следует полностью заблокировать доступ к рабочей станции извне. |
| **Защищенная сборка** | Вы указали, что процессы сборки для устройств инфраструктуры были документированы. | Продолжайте документирование процесса сборки для устройств инфраструктуры и обновляйте сборку при выпуске новых исправлений. |
| **Защищенная сборка** | Вы указали, что клиентское программное обеспечение удаленного доступа было установлено на рабочих станциях, которые удаленно подсоединяются к внутренней сети. | Рассмотрите возможность использования единого решения удаленного доступа для среды, если развернуто несколько типов решений. |
| **Защищенная сборка** | Вы указали, что процессы сборки для серверов были документированы. | Продолжайте документирование процесса сборки для серверов и обновляйте сборку при выпуске новых исправлений. |
| **Защищенная сборка** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Защищенная сборка** | Вы указали, что в вашей среде не используется программное обеспечение шифрования данных на диске. | Рассмотрите необходимость использования программного обеспечения шифрования данных на диске во избежание нарушения их безопасности в случае кражи компьютера. |
| **Защищенная сборка** | Вы указали, что процессы | Продолжайте |

| | | |
|---|---|---|
| | сборки для рабочих станций и переносных компьютеров были документированы. | документирование процесса сборки для рабочих станций и переносных компьютеров и обновляйте сборку при выпуске новых исправлений. |
| **Защищенная сборка** | Вы указали, что в вашей среде не используется программное обеспечение удаленного контроля/управления. | Продолжайте практику отказа от использования программного обеспечения удаленного контроля/управления. |
| **Защищенная сборка** | Вы указали, что в вашей среде не используется экранная заставка с парольной защитой. | Рассмотрите необходимость обязательной установки на компьютеры всех пользователей экранной заставки с парольной защитой с коротким периодом ожидания. |
| **Защищенная сборка** | Вы указали, что в вашей среде не используются модемы. | Продолжайте практику отказа от использования удаленного доступа через модем или телефонную сеть для снижения риска прямого подключения к компьютерам. |
| **Подкатегория** | **Передовые методики** | |
| **Физическая безопасность** | Продолжайте реализовывать средства контроля физического доступа для обеспечения безопасности. | |
| **Физическая безопасность** | Разработайте и внедрите средства контроля физического доступа для защиты от несанкционированного проникновения в офисное здание и получения доступа к конфиденциальным данным. Рассмотрите необходимость переоценки мер контроля физического доступа для определения их эффективности, а также степени их соблюдения. Повысьте осведомленность работников о политике контроля доступа персонала. Поощряйте уведомления о несанкционированном присутствии людей в офисном здании. | |
| **Физическая безопасность** | Все компьютерные системы должны быть защищены от простых взломов. Необходимо поместить серверы и сетевые системы в запираемые корпуса и закрытые помещения с контролируемым доступом. | |
| **Физическая безопасность** | Физический доступ необходимо строго контролировать с целью предотвращения несанкционированного доступа в офисные здания, к конфиденциальным данным и системам. Получив физический доступ, злоумышленник может изменить конфигурацию системы, нарушить безопасность сети и даже уничтожить или украсть оборудование. | |
| | **Полученные данные** | **Рекомендации** |
| **Физическая безопасность** | Ваш ответ показал, что элементы управления физической безопасностью были развернуты для защиты имущества организации. | Можно продолжить использование физических элементов управления, а также рассмотреть необходимость распространения их на все компьютерное оборудование, |

| | | |
|---|---|---|
| | | если этого еще не было сделано. |
| **Физическая безопасность** | Вы указали, что система сигнализации была установлена для обнаружения незаконного вторжения и оповещения. | Продолжите использование системы сигнализации. Периодически проверяйте ее (вместе с обслуживающей компанией), чтобы убедиться, что она работает правильно. |
| **Физическая безопасность** | Ответ указывает на то, что все указанные меры или некоторые из них применяются. (идентификационные карточки для сотрудников и посетителей, сопровождение посетителей, журналы регистрации посетителей, контрольно-пропускные пункты) | Продолжайте реализовывать средства контроля физического доступа для обеспечения безопасности. |
| **Физическая безопасность** | Вы указали, что сетевое оборудование находится в закрытом помещении с ограниченным доступом. | Продолжите практику защиты сетевого оборудования в запертой комнате и убедитесь, что доступ в нее имеют только те, кому это требуется по служебным обязанностям. |
| **Физическая безопасность** | Ответ указывает на то, что (идентификационные карточки для сотрудников и посетителей, сопровождение посетителей, журналы регистрации посетителей, контрольно-пропускные пункты) не применяются. | Разработайте и внедрите средства контроля физического доступа для защиты от несанкционированного проникновения в офисное здание и получения доступа к конфиденциальным данным. Рассмотрите необходимость переоценки мер контроля физического доступа для определения их эффективности, а также степени их соблюдения. Повысьте осведомленность работников о политике контроля доступа персонала. Поощряйте уведомления о несанкционированном присутствии людей в офисном здании. |
| **Физическая безопасность** | Вы указали, что сетевое оборудование находится также в запираемом шкафу или стойке. | Установка сетевого оборудования в запираемом шкафу или стойке обеспечивает дополнительную защиту от несанкционированного использования. Убедитесь, что доступ к клавишам и |

| | | |
|---|---|---|
| | | комбинациям имеют только те, кому это требуется по служебным обязанностям. |
| **Физическая безопасность** | Ответ указывает на то, что все указанные меры или некоторые из них применяются. (идентификационные карточки для сотрудников и посетителей, сопровождение посетителей, журналы регистрации посетителей, контрольно-пропускные пункты) | Продолжайте реализовывать средства контроля физического доступа для обеспечения безопасности. |
| **Физическая безопасность** | Вы указали, что серверы находятся в закрытом помещении с ограниченным доступом. | Продолжите практику защиты серверов в запертой комнате и убедитесь, что доступ в нее имеют только те, кому это требуется по служебным обязанностям. |
| **Физическая безопасность** | Ответ указывает на то, что все указанные меры или некоторые из них применяются. (идентификационные карточки для сотрудников и посетителей, сопровождение посетителей, журналы регистрации посетителей, контрольно-пропускные пункты) | Продолжайте реализовывать средства контроля физического доступа для обеспечения безопасности. |
| **Физическая безопасность** | Вы указали, что серверы находятся также в запираемом шкафу или стойке. | Установка серверов в запираемом шкафу или стойке обеспечивает дополнительную защиту от несанкционированного использования. Убедитесь, что доступ к клавишам и комбинациям имеют только те, кому это требуется по служебным обязанностям. |
| **Физическая безопасность** | Вы указали, что рабочие станции не защищены кабельными замками | Чтобы предотвратить кражу обеспечьте защиту рабочих станций с помощью кабельных замков. |
| **Физическая безопасность** | Вы указали, что переносные компьютеры не защищены кабельными замками | Чтобы предотвратить кражу обеспечьте защиту переносных компьютеров с помощью кабельных замков. |
| **Физическая безопасность** | Вы указали, что конфиденциальные печатные материалы не хранятся в запираемых картотечных | Важные документы следует хранить в запираемых шкафах, чтобы предотвратить кражу и разглашение |

| | | |
|---|---|---|
| | шкафах. | конфиденциальной информации. |

| **Управление и контроль - Ресурсы** | | |
|---|---|---|
| Windows Server 2008 | Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that try to connect to your network comply with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution and Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations. | http://www.microsoft.com/windowsserver2008/en/us/overview.aspx |
| Windows Server Active Directory | A central component of the Windows platform, Active Directory directory service provides the means to manage the identities and relationships that make up network environments. Windows Server 2003 makes Active Directory simpler to manage, easing migration and deployment. Windows Server Active Directory is already used by companies around the world to gain unified management of identities and resources across the enterprise network. Active Directory enables organizations to centrally manage and track information about users and their privileges. In addition, Active Directory Lightweight Directory Services (ADLDS), an LDAP directory service, provides organizations with flexible support for directory-enabled applications. Integration with Microsoft Federated Identity, Strong Authentication, Information Protection and Identity Lifecycle Management solutions, makes Active Directory an ideal foundation for building a comprehensive identity and access solution. | http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx<br><br>http://www.microsoft.com/windowsserver2003/technologies/idm/DirectoryServices.mspx |
| Public Key Infrastructure | Microsoft Public Key Infrastructure (PKI) for Windows Server 2003 provides an integrated public key infrastructure that enables you to secure and exchange information with strong security and easy administration across the Internet, extranets, intranets, and applications. | http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx |
| Certificates | Windows Certificate Services (CS) provides an integrated public key infrastructure that enables the secure exchange of information. With strong | http://www.microsoft.com/windowsserver2003/technologies/idm/StrongAuthentication. |

| | | |
|---|---|---|
| | security and easy administration across the Internet, extranets, intranets, and applications, CS provides customizable services for issuing and managing the certificates used in software security systems employing public key technologies. | mspx |
| Forefront Client Security | Forefront Client Security helps guard against emerging threats, such as spyware and rootkits, as well as traditional threats, such as viruses, worms, and Trojan horses. By delivering simplified administration through central management and providing critical visibility into threats and vulnerabilities, Forefront Client Security helps you protect your business with confidence and efficiency. Forefront Client Security integrates with your existing infrastructure software, such as Microsoft Active Directory, and complements other Microsoft security technologies for enhanced protection and greater control. | http://www.microsoft.com/forefront/clientsecurity/en/us/overview.aspx |
| Windows Vista - BitLocker Drive Encryption | Bitlocker Drive Encryption is a data protection feature available in Windows Vista Enterprise and Ulitmate editions and in Windows Server 2008. Bitlocker enhances data protection by bringing together drive encription and integrity checking of early boot components. | http://www.microsoft.com/windows/products/windowsvista/features/details/bitlocker.mspx |
| Windows Vista - Encrypted File System (EFS) | Encrypting File System (EFS) is a data protection feature in the Business, Enterprise and Ultimate editions of Windows Vista. If is userful for user-level file and folder encryption. | http://www.microsoft.com/windows/products/windowsvista/features/details/encryptingfilesystem.mspx |
| Windows Vista and XPsp2 - Windows Defender | Windows Defender works with Internet Explorer 7 to help make conscious choices installing software on your PS by providing always-on protection and monitoring of key system locations watching for changes that signal the installation and presence of spyware. | http://www.microsoft.com/windows/products/windowsvista/features/details/defender.mspx |
| Windows Firewall | Windows Firewall is a critiacal first line of defense to protect your computer against many types of malicious software. It can help stop malware before it infects your computer. Windows Firewall comes with Windows Vista and is turned on by default to protect your system as soon as windows starts. | http://www.microsoft.com/windows/products/windowsvista/features/details/firewall.mspx |
| Windows Security Center | Windows Security Center alers you when your security software is out of date or when your security settings should be strengthened. It displays your firewall settings and tells you whether your PC is set up to receive automatic updates from Microsoft. | http://www.microsoft.com/windows/products/windowsvista/features/details/securitycenter.mspx |

| | | |
|---|---|---|
| Windows Live One Care | Protect, maintain, and manage your computer with Windows Live OneCare, the always-on PC-care service from Microsoft. Working quietly in the background on your computer, OneCare protects against viruses, spyware, hackers, and other unwanted intruders. New features allow for multi-PC management to form a circle of protection, printer sharing support, and centralized backup of up to three PCs covered under the same OneCare subscription. | http://onecare.live.com/standard/en-us/default.htm |
| ISA Server | Internet Security and Acceleration (ISA) Server 2006 is the integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users with fast and secure remote access to applications and data.Deploy ISA Server 2006 for Secure Remote Access, Branch Office Security, and Internet Access Protection. | http://www.microsoft.com/forefront/edgesecurity/iap.mspx<br><br>http://www.microsoft.com/forefront/edgesecurity/sra.mspx<br><br>http://www.microsoft.com/forefront/edgesecurity/bos.mspx |
| ADFS | Microsoft Active Directory Federation Services (ADFS) provides the interoperability required to simplify the broad, federated sharing of digital identities and policies across organizational boundaries. Seamless yet secure, customers, partners, suppliers, and mobile employees can all securely gain access to the information they need, when they need it. ADFS Boost cross-organizational efficiency and collaboration with secure data access across companies and Improves operational efficiency with streamlined federation systems and simplified management of IDs and passwords. It boost visibility into cross-boundary processes with transparent, auditable information rights and roles and improves security with ADFS claim mapping, SAML tokens, and Kerberos authentication. ADFS helps to reduce operations costs by taking advantage of existing investments in Active Directory and security systems and eliminates the complexity of managing federation by using Active Directory as the main identity repository. | http://www.microsoft.com/windowsserver2003/technologies/idm/federatedidentity.mspx |
| (IPV6) Direct Connect | IPv6 is designed to solve many of the problems of the current version of IP (known as IPv4) such as address depletion, security, autoconfiguration, and extensibility. Its use will also expand the capabilities of the Internet to enable a variety of valuable and exciting scenarios, including peer-to-peer and mobile applications. Support for Internet Protocol version 6 (IPv6), a new suite of standard protocols for the Network layer of the Internet, is built into the latest versions of | http://technet.microsoft.com/en-us/network/bb530961.aspx |

| | | |
|---|---|---|
| | Microsoft Windows, which include Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP with Service Pack 2, Windows XP with Service Pack 1, Windows XP Embedded SP1, and Windows CE .NET. | |
| IPSec | Internet Protocol security (IPsec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on standards developed by the Internet Engineering Task Force (IETF) IPsec working group. IPsec is supported by the Microsoft Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 2000 operating systems and is integrated with the Active Directory directory service. IPsec policies can be assigned through Group Policy, which allows IPsec settings to be configured at the domain, site, or organizational unit level. | http://technet.microsoft.com/en-us/network/bb531150.aspx |
| 802.1 | The IEEE 802.1X standard for wired networks provides authentication and authorization protection at the network edge where a host attaches to the network. IPsec provides peer authentication and cryptographic protection of IP traffic from end-to-end. This white paper describes the security and capabilities of 802.1X for wired networks and IPsec based on industry standards and their support in Windows Server 2003, Windows Server 2008, Windows XP and Windows Vista and provides comparison information when evaluating deployment of these security technologies. | http://technet2.microsoft.com/windowsserver/en/library/908d13e8-c4aa-4d62-8401-86d7da0eab481033.mspx?mfr=true |

## Приложения

Для полного понимания вопросов безопасности, касающихся приложений, требуются глубокие знания в области общей архитектуры приложений, а также абсолютное понимание пользовательской базы приложения. Только тогда можно приступать к определению потенциальных векторов угроз.
Учитывая ограниченный масштаб данной самооценки, полный анализ архитектуры приложений и всестороннее понимание пользовательской базы невозможны. Эта оценка предназначена для обзора приложений в организации и их оценки с точки зрения безопасности и доступности. Для усовершенствования эшелонированной защиты выполняется проверка технологий, используемых в среде. Оценка предусматривает проверку процедур высокого уровня, которые организация может выполнять для снижения угрозы со стороны приложений, сосредоточившись на следующих областях безопасности, связанных с приложениями:

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

- Развертывание и использование — Механизмы повышения доступности
- Схема приложения — Проверка подлинности, Управление доступом, Управление средствами обновления, Проверка входных данных, Ведение журнала и проверка
- Хранение данных и связь — Шифрование, Передача данных, Ограничение доступа

| **Развертывание и использование** | | |
|---|---|---|
| **Подкатегория** | **Передовые методики** | |
| **Балансировка нагрузки** | | |
| | **Полученные данные** | **Рекомендации** |
| **Балансировка нагрузки** | Вы указали, что в вашей среде в настоящее время развернуты средства выравнивания нагрузки. | Периодически следует проверять настройку устройств выравнивания нагрузки и выполнять диагностику для поддержания правильного функционирования. |
| **Подкатегория** | **Передовые методики** | |
| **Кластеризация** | | |
| | **Полученные данные** | **Рекомендации** |
| **Кластеризация** | Ваш ответ указывает на то, что в среде развернута кластеризация. | Необходимо реализовать формальную политику периодической проверки отказоустойчивости механизмов кластеризации. |
| **Подкатегория** | **Передовые методики** | |
| **Восстановление приложений и данных** | | |
| | **Полученные данные** | **Рекомендации** |
| **Восстановление приложений и данных** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Восстановление приложений и данных** | Ваш ответ указывает на то, что регулярная проверка приложения и восстановление данных выполняются. | Рассмотрите необходимость реализации политики хранения резервных носителей за пределами сети и политики периодического чередования этих носителей. |
| **Подкатегория** | **Передовые методики** | |
| **Независимый сторонний поставщик программного обеспечения** | Сторонние независимые поставщики программного обеспечения должны регулярно предоставлять исправления и обновления собственных приложений, в которых должны содержаться сведения о назначении исправлений и их влиянии на функциональные возможности, конфигурацию или безопасность исправляемого приложения.<br>Сторонние независимые поставщики программного обеспечения должны четко определить критические исправления для их | |

| | | |
|---|---|---|
| | немедленного применения.<br><br>Сторонний независимый поставщик программного обеспечения должен объяснить все механизмы обеспечения безопасности приложения и предоставить последнюю версию документации.<br><br>Организации должны быть известны все требования к конфигурации, необходимые для гарантии высочайшего уровня безопасности. | |
| | **Полученные данные** | **Рекомендации** |
| **Независимый сторонний поставщик программного обеспечения** | Вы указали, что в вашей среде сторонние поставщики разработали одно или несколько основных приложений. | Убедитесь, что сторонняя организация, которая разработала основное программное обеспечение, будет продолжать его поддержку, своевременно обеспечивать доставку обновлений и сможет предоставить исходный текст приложения в случае невозможности его дальнейшей поддержки. |
| **Независимый сторонний поставщик программного обеспечения** | Ваши ответы указывают на то, что сторонние независимые поставщики программного обеспечения (ISV) регулярно предоставляют вам программные обновления и исправления, повышающие безопасность, для разработанных ими приложений. | Продолжите работу со сторонним поставщиком приложений для решения всех вопросов, связанных с развернутыми приложениями и безопасностью.<br>Когда появится исправление, прежде чем развертывать, тщательно проверьте его в лабораторных условиях.<br><br>Получите от поставщика документацию по защите приложения, если таковая существует, и проверьте параметры настройки приложения. |
| **Независимый сторонний поставщик программного обеспечения** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Независимый сторонний поставщик программного обеспечения** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или |

| | | |
|---|---|---|
| | | специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Независимый сторонний поставщик программного обеспечения** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |

| **Подкатегория** | **Передовые методики** |
|---|---|
| **Внутренняя разработка** | Собственная группа разработки должна регулярно предоставлять исправления и обновления собственных приложений, в которых должны содержаться сведения о назначении исправлений и их влиянии на функциональные возможности, конфигурацию или безопасность исправляемого приложения.<br>Группа разработки должна четко определить критические исправления для их немедленного применения в организации.<br><br>Группа разработки должна объяснить все механизмы обеспечения безопасности приложения и предоставить последнюю версию документации.<br><br>Организации должны быть известны все требования к конфигурации, необходимые для гарантии высочайшего уровня безопасности.<br><br>Рекомендуется заключить контракт с независимой сторонней фирмой на проверку архитектуры и развертывания приложения с целью определения всех проблем системы безопасности. |

| | **Полученные данные** | **Рекомендации** |
|---|---|---|
| **Внутренняя разработка** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Внутренняя разработка** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| Подкатегория | Передовые методики |
|---|---|
| **Уязвимые места в системе** | Все известные проблемы системы безопасности должны быть определены и исправлены. Следует регулярно посещать веб-узлы поставщика и сторонних компаний, посвященные безопасности, для получения сведений о проблемах безопасности и имеющихся исправлениях.<br>Если имеются известные проблемы системы безопасности, для которых нет исправлений, следует выяснить, когда выйдет исправление, и разработать промежуточный план снижения рисков по этой проблеме.<br><br>Рекомендуется обращаться к сторонней фирме для проведения периодических оценок системы безопасности приложения. Сторонняя оценка может также выявить области, где необходимы дополнительные механизмы обеспечения безопасности. |

| | Полученные данные | Рекомендации |
|---|---|---|
| **Уязвимые места в системе** | Ваши ответы указывают на то, что процедуры, направленные на устранение известных проблем безопасности в используемых приложениях, существуют. | Эти процедуры включают проверку исправлений в лабораторных условиях, а также проверку приложений после установки исправления, чтобы определить наличие конфликтов, из-за которых может потребоваться выполнить откат исправления. Периодически повторяйте эти процедуры, чтобы убедиться, что они соответствуют текущим требованиям приложения. |

| Развертывание и использование - Ресурсы | | |
|---|---|---|
| 2007 Office Security Guide | As risks from malicious attack have increased, desktop application security mechanisms have evolved. The new security model in the 2007 Microsoft Office release provides new mechanisms, settings, and features that allow your organization to achieve an effective balance between protection and productivity while minimizing user disruption. You might think that such risks come from outside your organization, and can therefore be stopped by effective network security mechanisms such as firewalls, proxy servers, and intrusion detection systems. However, many of these business risks can come from internal users and unsecured systems that are at the heart of your organization. Unless | http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/default.mspx |

| | | |
|---|---|---|
| | securely configured, the desktop applications that your information workers rely on to send e-mail, write documents, create presentations, and analyze data can be critical pathways for attack by malicious software (malware), including spyware, Trojan horses, viruses, and worms. | |
| Microsoft Rights Management Services for Windows Server 2003 | Microsoft Windows Rights Management Services (RMS) for Windows Server 2003 is information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized use—both online and offline, inside and outside of the firewall. RMS augments an organization's security strategy by protecting information through persistent usage policies, which remain with the information, no matter where it goes. Organizations can use RMS to help prevent sensitive information—such as financial reports, product specifications, customer data, and confidential e-mail messages—from intentionally or accidentally getting into the wrong hands. This services is built into Windows Server 2008 as Active Directory Rights Management Services (ADRMS) | http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx |
| Windows Server 2008 - Active Directory Rights Management Services | Windows Server 2008 - Active Directory Rights Management Services (AD RMS) is an information protection technology that works with AD RMS-enabled applications (Office 2007) to help safegaurd digital information from unauthorized use. Content owners can define who can open, modify, print, forward or take other actions with the information. | http://technet2.microsoft.com/windowsserver2008/en/library/37c240d3-8928-4267-867b-4c005b72cca21033.mspx?mfr=true |
| Windows Server 2008 - Clustering | Failover clustering in Windows Server 2008 can help you build redundancy into your network and eliminate single points of failure. The improvements to failover clusters (formerly known as server clusters) in Windows Server 2008 are aimed at simplifying clusters, making them more secure, and enhancing cluster stability. All of which helps reduce downtime, guard against data loss, and reduce your total cost of ownership. Because they are included in the enhanced-capability editions of Windows Server 2008, such as Windows Server 2008 Enterprise and Windows Server 2008 Datacenter, Windows Server 2008 failover clusters are much less expensive than comparable systems, which can cost thousands of dollars. Ease of deployment and affordability make Windows Server 2008 an ideal high-availability solution for organizations of all sizes. | http://www.microsoft.com/windowsserver2008/en/us/clustering-home.aspx |
| Microsoft Security Development Lifecycle | Trustworthy Computing is a Microsoft initiative for ensuring the production of secure code. A key | http://msdn.microsoft.com/en-us/library/aa969774.aspx |

| | |
|---|---|
| | element of the Trustworthy Computing initiative is the Microsoft Security Development Lifecycle (SDL). The SDL is an engineering practice that is used in conjunction with standard engineering processes to facilitate the delivery of secure code. The SDL consists of ten phases that combine best practices with formalization, measurability, and additional structure, including: security design analysis, tool-based quality checks, penetration testing, final security review, post release product security management. This methodology is also available in book form through Microsoft Press. |

| **Схема приложения** | | |
|---|---|---|
| **Подкатегория** | **Передовые методики** | |
| **Проверка подлинности** | В приложении должен быть реализован способ проверки подлинности, надежность которого соответствует требованиям безопасности данных или доступа к функциям. В приложениях, зависящих от паролей, должны быть предусмотрены ограничения с точки зрения сложности пароля, включающие сочетание букв, цифр и символов, минимальную длину, ведение журнала, длительность, преждевременное истечение срока действия и проверку по словарю.<br>Приложение должно регистрировать безуспешные попытки входа в систему в обход пароля. Каждый компонент, предоставляющий доступ к данным или функциям, должен контролировать наличие правильных учетных данных для проверки подлинности.<br><br>Административные права доступа к системам должны быть защищены самым надежным механизмом проверки подлинности. Обычно ограничения по созданию паролей для администраторов должны быть еще более строгими, чем для обычных учетных записей.<br><br>Кроме использования сложных паролей с надежными политиками, для дополнительной безопасности рекомендуется использовать многофакторную проверку подлинности. | |
| | **Полученные данные** | **Рекомендации** |
| **Проверка подлинности** | Ваши ответы указывают на то, что в настоящее время для основных приложений используется многофакторная проверка подлинности. | Чтобы еще более снизить риск взлома пароля во внешних приложениях, выполните следующие рекомендации:<br>+ Истечение срока действия пароля<br>+ Блокировка учетной записи после хотя бы 10 попыток неправильного ввода пароля<br>+ Ведение журнала системы |

| Подкатегория | Передовые методики |
|---|---|
| **Политики паролей** | Использование сложных паролей является ключевым элементом эшелонированной защиты. Сложные пароли должны быть длиной от 8 до 14 символов и содержать буквы, цифры и специальные символы. Для обеспечения дополнительной защиты паролей необходимо задать минимальную длину, ведение хронологии журнала, длительность, а также преждевременное истечение срока действия паролей. Обычно срок истечения действия пароля должен задаваться следующим образом:<br>+ Максимальная продолжительность 90 дней<br>+ Новые учетные записи должны изменять пароль при входе в систему<br>+ 8 паролей в журнале паролей (минимум 8 дней)<br><br>Административные права доступа к системам должны быть защищены самым надежным механизмом проверки подлинности. —Обычно ограничения по созданию паролей для администраторов должны быть еще более строгими, чем для обычных учетных записей. Если для обычных учетных записей длина пароля должна составлять 8 символов, то для учетных записей администраторов пароли должны быть длиной 14 символов.<br><br>Для всех учетных записей пользователей необходимо включить блокировку учетной записи после 10 неудачных попыток ввода пароля. Контроль блокировки учетной записи может варьироваться от простой блокировки в случае взлома пароля до сложных случаев, требующих вмешательства администратора для разблокировки учетной записи. Рекомендуется выполнить следующие инструкции при реализации контроля блокировки учетной записи:<br><br>+ Блокировка после как минимум 10 неудачных попыток ввода пароля для учетных записей пользователей<br>+ Необходим доступ с правами администратора для разблокировки учетных записей важных приложений, а также автоматическая разблокировка обычных учетных записей пользователя через 5 минут для других приложений<br>+ Промежуток в 30 минут для кэширования сбоев обычных учетных записей пользователя |

| | Полученные данные | Рекомендации |
|---|---|---|
| **Политики паролей** | Ваш ответ указывает на то, что для основных приложений реализованы эффективные элементы управления, предусматривающие наличие паролей. | Рассмотрите необходимость реализации пороговых значений для неудачных попыток проверки подлинности при входе, чтобы системным администраторам посылались соответствующие сигналы. Кроме того, рассмотрите необходимость |

| | | |
|---|---|---|
| | | распространения использования надежных паролей на все приложения. |
| **Политики паролей** | Ваш ответ указывает на то, что в основных приложениях реализован элемент управления истечением срока действия пароля. | Рассмотрите необходимость распространения политики ограничения срока действия паролей на все внешние приложения и основные внутренние приложения. |
| **Политики паролей** | Ваш ответ указывает на то, что в основных приложениях реализованы элементы управления блокировкой учетных записей. | Рассмотрите необходимость распространения политики блокировки учетных записей на все внешние приложения и важные внутренние приложения. |
| **Подкатегория** | **Передовые методики** | |
| **Авторизация и управление доступом** | В приложениях должен быть реализован механизм авторизации, который обеспечивает доступ к критическим данным и функциям только для пользователей и клиентов, имеющих соответствующие права.<br>Управление доступом на основе ролей должно быть усилено на уровне базы данных и интерфейса приложения.<br><br>Это обеспечит защиту базы данных в случае "взлома" клиентского приложения.<br><br>До выполнения успешной проверки подлинности необходимо пройти авторизацию.<br><br>Все попытки получения доступа без авторизации должны регистрироваться в журнале.<br><br>Следует проводить регулярные проверки основных приложений, которые обрабатывают критические данные, а также интерфейсов, доступных для пользователей из сети Интернет. Приложения следует проверять в режимах "черного ящика" и "подробного описания". Необходимо определить, имеют ли пользователи доступ к данным с других учетных записей. | |
| | **Полученные данные** | **Рекомендации** |
| **Авторизация и управление доступом** | Ваш ответ указывает на то, что основные приложения ограничивают доступ к критическим данным и функциональным возможностям исходя из привилегий, назначенных учетной записи. | Рассмотрите необходимость проведения целенаправленной проверки основных приложений, которые обрабатывают критические данные, а также интерфейсов, доступных для пользователей из сети Интернет. Приложения следует проверять в режимах "черного ящика" и "подробного описания", а также проверка |

| | | |
|---|---|---|
| | | обнаружения попыток превышения имеющихся привилегий. |

| **Подкатегория** | **Передовые методики** |
|---|---|
| **Ведение журнала** | Ведение журнала должно быть включено для всех приложений в системе. Данные файла журнала важны для анализа происшествий и тенденций, а также для проверки. Приложение должно регистрировать все безуспешные и удачные попытки проверки подлинности, изменения данных приложения, включая учетные записи пользователей, неустранимые ошибки приложений, а также безуспешный и успешный доступ к ресурсам.<br><br>При записи данных в файл журнала приложение не должно записывать конфиденциальные данные. |

| | **Полученные данные** | **Рекомендации** |
|---|---|---|
| **Ведение журнала** | Ваши ответы указывают на то, что в данной среде разные события регистрируются приложениями. Приложения должны заносить в журналы все события на основе перечисленных передовых методик. | Для облегчения управления файлами журнала и их анализа рассмотрите необходимость интеграции с централизованным механизмом ведения журналов. Механизм ведения журналов должен обеспечивать сохранение и архивирование журналов в соответствии с действующими политиками хранения корпоративных данных. |
| **Ведение журнала** | Вы указали, что неудачные попытки проверки подлинности фиксируются в журнале. | Продолжайте ведение журнала неудачных попыток проверки подлинности. |
| **Ведение журнала** | Вы указали, что успешные проверки подлинности фиксируются в журнале. | Продолжайте ведение журнала успешных проверок подлинности. |
| **Ведение журнала** | Вы указали, что ошибки приложения фиксируются в журнале. | Продолжайте ведение журнала ошибок приложений. |
| **Ведение журнала** | Вы указали, что отказ в доступе к ресурсам фиксируется в журнале. | Продолжайте ведение журнала отказов в доступе к ресурсам |
| **Ведение журнала** | Вы указали, что успешный доступ к ресурсам фиксируется в журнале. | Продолжайте ведение журнала успешного доступа к ресурсам |
| **Ведение журнала** | Вы указали, что изменения в данных фиксируются в журнале. | Продолжайте ведение журнала изменений данных |
| **Ведение журнала** | Вы указали, что изменения в | Продолжайте ведение журнала |

| | | |
|---|---|---|
| | учетных записях пользователей фиксируются в журнале. | изменений в учетных записях пользователей. |
| **Подкатегория** | **Передовые методики** | |
| **Подтверждение ввода** | Приложение может принимать входные данные во многих точках от внешних источников, например пользователей, клиентских приложений, а также передач данных. Оно должно проводить проверки вводимых данных на синтаксическую и семантическую достоверность. Это приложение также должно проверять, не нарушают ли вводимые данные ограничения базовых или зависимых компонентов, в частности, по длине строки и набору символов.<br>Все пользовательские поля должны проверяться на сервере. | |
| | **Полученные данные** | **Рекомендации** |
| **Подтверждение ввода** | Ваш ответ указывает на то, что проверяются все входные данные конечных пользователей. | Регулярно осуществляйте аудит каждого приложения, чтобы обеспечить постоянную и надлежащую проверку всех данных, вводимых пользователями.<br>Ограничения, связанные с проверкой входных данных, должны обеспечивать прием только синтаксически и семантически верных данных, а не просто предусматривать обычную фильтрацию недопустимых символов на входе. |
| **Подтверждение ввода** | Ваш ответ указывает на то, что проверяются все входные данные клиентских приложений. | Регулярно осуществляйте аудит каждого приложения, чтобы обеспечить постоянную и надлежащую проверку всех вводимых данных.<br>Ограничения, связанные с проверкой входных данных, должны обеспечивать прием только синтаксически и семантически верных данных, а не просто предусматривать обычную фильтрацию недопустимых символов на входе. |
| **Подтверждение ввода** | Ваш ответ указывает на то, что проверяются все входные данные от источников подачи данных. | Регулярно осуществляйте аудит каждого приложения, чтобы обеспечить постоянную и надлежащую проверку всех вводимых данных. |

| | | |
|---|---|---|
| | | Ограничения, связанные с проверкой входных данных, должны обеспечивать прием только синтаксически и семантически верных данных, а не просто предусматривать обычную фильтрацию недопустимых символов на входе. |
| **Подкатегория** | **Передовые методики** | |
| **Методологии разработки систем безопасности программного обеспечения** | Продолжайте использовать методологии разработки систем безопасности программного обеспечения. | |
| **Методологии разработки систем безопасности программного обеспечения** | Разработайте и внедрите методологии разработки систем безопасности программного обеспечения для повышения безопасности приложений. | |
| **Методологии разработки систем безопасности программного обеспечения** | При сотрудничестве с консультантами или поставщиками на любом этапе цикла разработки убедитесь в том, что их персонал прошел обучение методологии разработки систем безопасности программного обеспечения, используемой или рекомендуемой к использованию в организации. | |
| **Методологии разработки систем безопасности программного обеспечения** | Весь коллектив разработчиков организации должен пройти обучение по рекомендуемой методологии разработки систем безопасности программного обеспечения. Это касается руководителей отделов разработки, разработчиков, испытателей и специалистов по контролю качества. | |
| **Методологии разработки систем безопасности программного обеспечения** | Учитывая постоянное развитие угроз безопасности, следует ежегодно обновлять программу обучения методологии разработки систем безопасности программного обеспечения и программу обучения моделированию угроз. Все разработчики должны ежегодно проходить обновленные курсы по разработке систем безопасности программного обеспечения. | |
| **Методологии разработки систем безопасности программного обеспечения** | Применение средств тестирования программ для обеспечения безопасности расширяет возможности команды разработчиков по эффективному написанию безопасного кода. Результаты применения средств тестирования должны включаться в программу обязательного ежегодного обучения. | |
| | **Полученные данные** | **Рекомендации** |
| **Методологии разработки систем безопасности программного обеспечения** | Ответ указывает на то, что организация обучает разработчиков методологии разработки систем безопасности программного обеспечения. | Продолжайте обучать разработчиков принципам разработки систем безопасности программного обеспечения. |
| **Методологии разработки систем безопасности программного обеспечения** | Ответ указывает на то, что организация не обучает разработчиков методологии разработки систем безопасности программного обеспечения. | Разработайте программу обучения методологии разработки систем безопасности программного обеспечения, чтобы усовершенствовать навыки сотрудников по созданию |

| | | |
|---|---|---|
| | | безопасного кода. |
| **Методологии разработки систем безопасности программного обеспечения** | Ответ указывает на то, что 75 % разработчиков в организации прошли обучение методологии разработки систем безопасности программного обеспечения. | Продолжайте обучать разработчиков принципам разработки систем безопасности программного обеспечения. |
| **Методологии разработки систем безопасности программного обеспечения** | Ответ указывает на то, что организация не обучает разработчиков методологии разработки систем безопасности программного обеспечения. | Разработайте программу обучения методологии разработки систем безопасности программного обеспечения, чтобы усовершенствовать навыки сотрудников по созданию безопасного кода. |
| **Методологии разработки систем безопасности программного обеспечения** | Ответ указывает на то, что организация не требует от своих разработчиков ежегодного прохождения обновленной программы обучения методологии разработки систем безопасности программного обеспечения. | Разработайте и внедрите процедуры ежегодного обновления программы обучения методологии разработки систем безопасности программного обеспечения. |
| **Методологии разработки систем безопасности программного обеспечения** | Ответ указывает на то, что организация не использует средства тестирования программ для обеспечения безопасности в качестве части процесса разработки систем безопасности. | Разработайте и внедрите процедуры использования средств тестирования программ для обеспечения безопасности в качестве первостепенного средства реализации планов разработки систем безопасности. |
| **Методологии разработки систем безопасности программного обеспечения** | Ответ указывает на то, что организация не использует методологию разработки систем безопасности программного обеспечения, чтобы усовершенствовать навыки в сфере разработки безопасного кода. | Разработайте и внедрите методологии разработки систем безопасности программного обеспечения для повышения безопасности приложений. |
| **Методологии разработки систем безопасности программного обеспечения** | Ответ указывает на то, что разработчики организации не проходили обучение методологии разработки систем безопасности программного обеспечения с целью усовершенствования навыков по разработке безопасного кода. | Продолжайте обновлять программу обучения разработке систем безопасности программного обеспечения и сделайте ежегодное прохождение персоналом этой программы обязательным. |

| **Хранение данных и связь** | |
|---|---|
| **Подкатегория** | **Передовые методики** |

| | |
|---|---|
| **Шифрование** | Критические данные должны быть зашифрованы или хешированы в базе данных и файловой системе. В приложении должно проводиться различие между критическими для раскрытия данными, которые необходимо шифровать, данными, которые являются критическими только с точки зрения подделки, для которых необходимо генерировать введенное хеш-значение (HMAC), а также данными, которые могут быть безвозвратно преобразованы (хешированы) без потери функциональности (например пароли). Ключи, использующиеся для дешифрации, должны храниться в приложении отдельно от зашифрованных данных.<br>Критические данные должны шифроваться до передачи в другие компоненты. Следует проверить, что промежуточные компоненты, обрабатывающие данные в незашифрованной форме до передачи получателю, не представляют угрозы для данных. Приложение должно воспользоваться средствами проверки подлинности, доступными в рамках механизма обеспечения безопасности транспорта.<br><br>Примерами широко используемых шрифтов являются 3DES, AES, RSA, RC4 и Blowfish. Рекомендуется использовать ключи не менее 128 бит (1024 бит для RSA). |

| | **Полученные данные** | **Рекомендации** |
|---|---|---|
| **Шифрование** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |

| **Подкатегория** | **Передовые методики** |
|---|---|
| **Шифрование - Алгоритм** | В приложении должны использоваться стандартные для отрасли алгоритм шифрования с ключами соответствующих размеров и необходимыми режимами шифрования.<br>К признанным в отрасли шифрам относятся 3DES, AES, RSA, Blowfish и RC4.<br><br>Необходимо использовать ключ размером не менее 128 бит (1024 бит для RSA). |

## Операции

В этой области анализа исследуются методы, процедуры эксплуатации и рекомендации, которым следует организация, для усовершенствования эшелонированной защиты. Данная оценка предполагает проверку политик и процедур, управляющих сборками системы, сетевой документацией и использованием технологий в среде. Она также включает поддержку функций, необходимых для управления информацией и процедурами, которые используются администраторами и оперативным персоналом в данной среде. Создав понятные

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02
рабочие методики, процедуры и рекомендации и следуя им, организация может потенциально улучшить состояние эшелонированной защиты. Оценка предусматривает проверку процедур высокого уровня, которые организация может выполнять для снижения угрозы со стороны операций, сосредоточившись на следующих областях безопасности, связанных с операциями:

- Среда — Сборка системы, Сетевая документация, Поток данных приложения, Архитектура приложений
- Политика безопасности — Протоколы и службы, Правильное использование, Управление учетными записями
- Управление средствами исправления и обновления — Управление исправлениями, Сигнатуры вирусов
- Архивация и восстановление — Архивация, Хранение, Проверка

| **Среда** | | |
|---|---|---|
| **Подкатегория** | **Передовые методики** | |
| **Узел управления** | При использовании пакетов управления следует позаботиться об усилении безопасности и физической защите консолей администрирования.Усильте безопасность рабочих станций, используемых для управления серверами сети и сетевыми устройствами.<br>Защитите протоколы управления, использующие открытый текст, с помощью SSH или VPN-подключений.<br>Рабочие станции управления должны быть выделены конкретным сетям и администраторам узлов.<br>Протестируйте все системы управления, использующие SNMP, чтобы убедиться в том, что они обновлены до последних версий и не используют строк сообщества по умолчанию.<br>В системах общего пользования не должно храниться никаких данных, относящихся к управлению. Рабочие станции с совместным доступом не следует использовать для администрирования сетевых устройств или узлов. | |
| **Подкатегория** | **Передовые методики** | |
| **Узел управления - Серверы** | | |
| | **Полученные данные** | **Рекомендации** |
| **Узел управления - Серверы** | Ваши ответы указывают на то, что для серверов существует выделенный управляющий компьютер. | Рассмотрите необходимость использования SSH или VPN для защиты текстовых протоколов. |
| **Подкатегория** | **Передовые методики** | |
| **Узел управления - Сетевые устройства** | | |
| | **Полученные данные** | **Рекомендации** |
| **Узел управления - Сетевые устройства** | Вы указали, что развернули выделенный управляющий компьютер для управления сетевыми устройствами. | Следует протестировать все системы управления, в которых используется SNMP, чтобы убедиться, что в них используются последние версии исправлений и не используются настройки |

| | |
|---|---|
| | сообщества по умолчанию. |

| Среда - Ресурсы | | |
|---|---|---|
| Windows Vista - User Account Controls | User Account Controls in Windows Vista improves the safety and securty of your computer by preventing dangerous software form making changes to your computer withue your explicit consent. This also helps in prohibiting users from installing rougue programs, changing system settings and performing other tasks that are the province administrators. | http://www.microsoft.com/windows/products/windowsvista/features/details/useraccountcontrol.mspx |
| Data Classification and Protection Whitepaper | Data Classification and protection deals with how to apply security classifications levels to the data either on a system or in transmission. | http://www.microsoft.com/technet/security/guidance/complianceandpolicies/compliance/rcguide/4-11-00.mspx?mfr=true |

| Политика безопасности | | |
|---|---|---|
| **Подкатегория** | **Передовые методики** | |
| **Классификация данных** | Продолжайте реализовывать классификацию данных с соответствующими рекомендациями по защите. | |
| **Классификация данных** | Определите схему классификации корпоративных данных и организуйте соответствующие инструктаж и обучение всего персонала. Определите требования к обработке и защите данных в соответствии с уровнями их классификации. | |
| **Классификация данных** | Проверьте открытые компоненты вместе в ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). | |
| **Классификация данных** | Необходимо иметь схему классификации данных с соответствующими рекомендациями по их защите. Недостаточное разделение и классификация данных может привести к тому, что конфиденциальные данные станут доступны персоналу, деловым партнерам или широкой общественности. Подобное несанкционированное раскрытие конфиденциальных данных может нанести урон репутации торговой марки или поставить компанию в неловкое положение. Ограниченный объем ресурсов по защите данных может быть использован нерационально и не обеспечит их надлежащей классификации. Если персонал компании не осведомлен о том, какие данные являются конфиденциальными, а также о том, как следует их защищать, вероятность несанкционированного доступа к этим данным увеличивается. | |
| | **Полученные данные** | **Рекомендации** |
| **Классификация данных** | Ответ указывает на то, что в организации применяются | Продолжайте реализовывать классификацию данных с |

| | | |
|---|---|---|
| | схема классификации данных и рекомендации по защите данных, разработанные на основе подобной схемы. | соответствующими рекомендациями по защите. |
| **Классификация данных** | Ответ указывает на то, что в организации отсутствуют схема классификации данных или рекомендации по защите данных, разработанные на основе подобной схемы. | Определите схему классификации корпоративных данных и организуйте соответствующие инструктаж и обучение всего персонала. Определите требования к обработке и защите данных в соответствии с уровнями их классификации. |
| **Классификация данных** | Вы указали, что не знаете ответа на этот вопрос. | Проверьте открытые компоненты вместе в ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). |
| **Подкатегория** | **Передовые методики** | |
| **Утилизация данных** | Продолжайте реализовывать процедуры удаления данных | |
| **Утилизация данных** | Определите и внедрите процедуры управления данными и их утилизации как для бумажных копий, так и для данных в электронном виде (например данных, хранящихся на дискетах и жестких дисках). | |
| **Утилизация данных** | Проверьте открытые компоненты вместе в ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). | |
| **Утилизация данных** | Необходимо реализовать формальные процедуры, регламентирующие утилизацию пользователями данных как в бумажном, так и в электронном виде. В случае отсутствия рекомендаций и процедур безопасного уничтожения данных конфиденциальные сведения могут оказаться в опасности. | |
| | **Полученные данные** | **Рекомендации** |
| **Утилизация данных** | Ответ указывает на то, что организация следует документально закрепленным процессам утилизации данных. | Продолжайте реализовывать процедуры удаления данных |
| **Утилизация данных** | Ответ указывает на то, что организация не следует документально закрепленным процессам утилизации данных. | Определите и внедрите процедуры управления данными и их утилизации как для бумажных копий, так и для данных в электронном виде (например данных, хранящихся на дискетах и жестких дисках). |

| | | |
|---|---|---|
| **Утилизация данных** | Вы указали, что не знаете ответа на этот вопрос. | Проверьте открытые компоненты вместе в ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). |
| **Подкатегория** | **Передовые методики** | |
| **Протоколы и службы** | Следует четко задокументировать стандарты и процедуры, чтобы отразить, какие протоколы и службы можно использовать в организации. Необходимо проверить списки управления доступом, чтобы убедиться, что уровень предоставленного доступа для всех разрешенных служб действительно необходим в компании. При возможности необходимо определить определенный IP-адрес/диапазон. На серверах должны быть установлены только те службы, которые необходимы для нужд компании. Кроме того, в этих инструкциях должны содержаться данные версии протокола и минимальной стойкости шифрования. Следует обеспечить более надежную защиту при использовании протокола за счет устройств внешнего доступа (маршрутизаторов, шлюзов, межсетевых экранов и т.д.), строгой проверки подлинности и шифрованных соединений. | |
| | **Полученные данные** | **Рекомендации** |
| **Протоколы и службы** | Ваш ответ указывает на то, что у вас имеются документированные указания, которые предписывают, какие протоколы и службы разрешены в корпоративной сети. | Проведите аудит документации, выясните, какие протоколы и службы разрешены, и убедитесь, что документация соответствует настроенным спискам управления доступом и правилам межсетевого экрана на соответствующих устройствах.<br>Опубликуйте эти сведения в корпоративной интрасети и реализуйте политики, регулирующие внесение изменений в правила. |
| **Подкатегория** | **Передовые методики** | |
| **Правильное использование** | Политика правильного использования предназначена для обеспечения надлежащего использования корпоративных сетей, приложений, данных и систем. Эта политика также должна регулировать данные мультимедиа, печатные носители и другую интеллектуальную собственность. | |
| | **Полученные данные** | **Рекомендации** |
| **Правильное использование** | Ваш ответ указывает на то, что в вашей организации | Все сотрудники и клиенты, использующие корпоративные |

| | | |
|---|---|---|
| | существует корпоративная политика правильного использования. | ресурсы, должны быть ознакомлены с этими политиками. Разместите политики в корпоративной интрасети и рассмотрите необходимость ознакомления с ними всех новых сотрудников при приеме их на работу. |
| **Подкатегория** | **Передовые методики** | |
| **Управление учетными записями** | Для всех пользователей, которым требуется доступ к ресурсам ИТ, необходимо создать отдельные учетные записи. Нельзя использовать общие учетные записи для нескольких пользователей. По умолчанию учетные записи должны создаваться с минимальными необходимыми привилегиями. Администраторы сетей и серверов должны иметь привилегированные (администраторские) и непривилегированные учетные записи. Стойкость пароля необходимо повышать и регулярно проверять, а все изменения учетной записи должны регистрироваться. По мере изменения роли отдельного пользователя все привилегии учетной записи должны быть пересмотрены и изменены при необходимости. В случае увольнения все учетные записи должны быть отключены или удалены. | |
| | **Полученные данные** | **Рекомендации** |
| **Управление учетными записями** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Подкатегория** | **Передовые методики** | |
| **Управление** | Необходимо регулярно выполнять сторонние проверки, чтобы гарантировать соответствие всем требованиям законодательства (например HIPAA для здравоохранения, Sarbanes-Oxley для фирм, деятельность которой регулируется положениями КЦББ). | |
| | **Полученные данные** | **Рекомендации** |
| **Управление** | Вы указали, что в вашей организации существуют политики для управления вычислительной средой. | Продолжите разработку и внедрение политик управления компьютерной средой в соответствии с действующими стандартами (ISO17799, CoBIT, HIPAA, SOX и т.д.) |
| **Подкатегория** | **Передовые методики** | |
| **Политика безопасности** | Политики безопасности должны разрабатываться с участием руководителей, ИТ-специалистов и сотрудников отдела кадров, а также высшего руководства корпорации. Эти политики должны часто обновляться с учетом текущих передовых методик (например CoBIT). | |
| | **Полученные данные** | **Рекомендации** |

| | | |
|---|---|---|
| **Политика безопасности** | Вы указали, что у вас существует политика безопасности информации, направленная на регулирование деятельности организации, связанной с безопасностью. | Продолжите использование политики информационной безопасности, однако периодически пересматривайте и обновляйте ее в соответствии с последними технологическими изменениями и изменениями среды. |
| **Политика безопасности** | Вы указали, что политика была разработана совместно отделом ИТ и представителями бизнеса. | При последующих обновления и изменениях политики по-прежнему должны разрабатываться как ИТ-специалистами, так и специалистами других отделов. |

| **Управление средствами исправления и обновления** | | |
|---|---|---|
| **Подкатегория** | **Передовые методики** | |
| **Документация о сети** | Всегда должны использоваться оперативные и точные физические и логические схемы внешних и внутренних сетей. Любые изменения, выполненные в этой среде, должны своевременно отражаться на соответствующей схеме.<br><br>К последним схемам должны иметь доступ только члены рабочей группы ИТ-специалистов. | |
| | **Полученные данные** | **Рекомендации** |
| **Документация о сети** | Ваш ответ указывает на то, что в вашей среде существуют логические сетевые схемы, и они обновлены. | Пересмотрите политику, регулирующую обновление схем сети.<br>Если для среды существует политика управления изменениями, укажите обновление схем в качестве формального шага, подлежащего выполнению в рамках политики управления изменениями.<br><br>Обеспечьте, чтобы доступ к самым последним схемам имел только ограниченный круг ИТ-специалистов и специалистов по безопасности. |
| **Документация о сети** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. |

| | | |
|---|---|---|
| | | Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Подкатегория** | **Передовые методики** | |
| **Поток данных приложений** | Схемы архитектуры приложений должны отображать основные компоненты и потоки важных данных в конкретной среде, включая системы, через которые проходят данные, а также способы их обработки.<br>По мере выполнения обновления приложения или системы, содержащей это приложение, необходимо своевременно обновлять схемы. | |
| **Подкатегория** | **Передовые методики** | |
| **Управление средствами исправления** | Необходимо своевременно разворачивать изменения системы безопасности и конфигурации (в соответствии с корпоративной политикой безопасности) по мере их выхода. Исправления и обновления (разработанные собственными силами или предоставленные сторонними поставщиками) должны тщательно проверяться в лабораторных условиях до развертывания. Кроме того, необходимо проверить все системы после установки исправления, чтобы определить наличие конфликтов в конкретной системе, из-за которых может потребоваться выполнить откат исправления.<br>Необходимо распределить системы по категориям, чтобы можно было осуществлять планирование на основе распределения по группам, — важные системы и системы с повышенным трафиком, должны исправляться в первую очередь. | |
| | **Полученные данные** | **Рекомендации** |
| **Управление средствами исправления** | Вы указали, что исправления и обновления проверяются перед их применением во всех системах. | Продолжайте практику проверки всех исправлений и обновлений перед их развертыванием в рабочей среде. |
| **Управление средствами исправления** | Ваш ответ указывает на то, что политика исправлений и обновлений существует как для приложений, так и операционных систем. | Продолжайте осуществлять текущие процедуры и пересмотрите сведения, доступные в разделе, посвященном передовым методикам, чтобы внести все необходимые изменения в используемые политики.<br>Оцените возможность использования серверов SMS и служб WSUS для автоматического администрирования и развертывания исправлений для серверов Windows. |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| Подкатегория | Передовые методики | |
|---|---|---|
| **Управление изменениями и конфигурация** | Любые изменения в рабочей среде сначала должны проверяться с точки зрения безопасности и совместимости перед запуском в производство, кроме того должна вестись полная документация по конфигурации всех производственных систем. | |
| | **Полученные данные** | **Рекомендации** |
| **Управление изменениями и конфигурация** | Вы указали, что в вашей организации существует процесс управления изменениями и конфигурацией. | По-прежнему используйте процесс официального управления изменениями и конфигурацией для проверки и документирования всех обновлений перед развертыванием. |
| **Управление изменениями и конфигурация** | Вы указали, что конфигурации документируются для дальнейших справок. | Продолжайте документировать все конфигурации для упрощения поиска и устранения неисправностей и восстановления систем. |
| **Управление изменениями и конфигурация** | Вы указали, что изменения, внесенные в конфигурации, проверяются до развертывания в производственных системах. | Продолжайте практику проверки всех изменений конфигурации перед их развертыванием в производственных системах. |
| **Управление изменениями и конфигурация** | Вы указали, что соответствие конфигурации проверяется и принимается в централизованном порядке. | Продолжайте практику проверки и обеспечения соответствия через центральную систему управления. |

| Управление средствами исправления и обновления - Ресурсы | | |
|---|---|---|
| Microsoft Update | Microsoft provides an automatic way for you to get the latest product updates and security patchs on regular basis through our Microsoft Update service. | http://www.update.microsoft.com/microsoftupdate/v6/vistadefault.aspx?ln=en-us |
| Microsoft Windows Server Update Services | Microsoft Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates to computers running the Windows operating system. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network. | http://technet.microsoft.com/en-us/wsus/default.aspx |
| Systems Center Configuration Manager | System Center Configuration Manager 2007 is the solution to comprehensively assess, deploy, and update your servers, clients, and devices across physical, virtual, distributed, and mobile environments. Optimized for Windows and extensible beyond, it is the best choice for gaining | http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx |

| | |
|---|---|
| | enhanced insight into and control over your IT systems. |

| **Архивация и восстановление** | | |
|---|---|---|
| **Подкатегория** | **Передовые методики** | |
| **Файлы журнала** | Файлы журналов настроены на запись всех запланированных действий без перезаписи элементов. Необходимо настроить автоматическую процедуру чередования файлов журналов на ежедневной основе и разгрузить журналы на защищенный сервер в сети управления.<br>Необходимо ограничить доступ к файлам журнала и настройкам конфигурации для предотвращения их изменения и удаления.<br><br>Необходимо регулярно проверять файлы журналов на предмет подозрительной или аномальной активности. Проверка должна включать в себя работу системы, обслуживание и систему безопасности. Для расширения возможностей проверки необходимо использовать программное обеспечение корреляции событий и анализ тенденций. | |
| | **Полученные данные** | **Рекомендации** |
| **Файлы журнала** | Вы указали, что в вашей среде файлы журналов чередуются. | Рассмотрите необходимость хранения файлов журналов в базе данных, чтобы служба безопасности при необходимости могла провести анализ тренда и получить доступ к защищенным журналам. |
| **Файлы журнала** | Вы указали, что в вашей среде файлы журналов просматриваются не регулярно. | Служба безопасности должна ежедневно просматривать файлы журналов на предмет подозрительной или аномальной активности. Рассмотрите необходимость мониторинга файлов журналов из DMZ и основных сетевых серверов с помощью MOM (Microsoft Operations Manager). В случае создания критических записей журнала, MOM отправит предупреждения соответствующим сотрудникам. |
| **Файлы журнала** | Вы указали, что в вашей среде доступ к файлам журналов защищен. | Рассмотрите необходимость переноса файлов журналов на защищенный сервер в сети управления для архивирования. Доступ к архивированным файлам журналов следует |

| | | |
|---|---|---|
| | | предоставить только службе безопасности для анализа происшествий. |
| **Файлы журнала** | Вы указали, что журналы ведутся на централизованном сервере журналов. | Продолжайте ведение журнала на централизованном сервере журналов. |

| **Подкатегория** | **Передовые методики** |
|---|---|
| **Планирование аварийного восстановления и возобновления деятельности предприятия** | Продолжайте поддерживать и тестировать планы аварийного восстановления и возобновления деятельности предприятия. |
| **Планирование аварийного восстановления и возобновления деятельности предприятия** | Требуйте разработки, документирования, реализации, а также периодических проверки, тестирования и обновления планов аварийного восстановления. Разработайте планы непрерывной работы предприятия, предусматривающие действия персонала, места размещений, а также системы и другие технологические проблемы. |
| **Планирование аварийного восстановления и возобновления деятельности предприятия** | Проверьте открытые компоненты вместе в ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). |
| **Планирование аварийного восстановления и возобновления деятельности предприятия** | Планы аварийного восстановления и возобновления деятельности предприятия должны быть документально оформлены и соответствовать современным требованиям. Это позволит обеспечивать восстановление в приемлемые сроки. Планы (включая планы восстановления приложений из резервных копий) должны регулярно тестироваться на полноту и правильность.<br>Планы непрерывной работы должны охватывать всю среду предприятия, включая ее физические и технологические составляющие, а также персонал. |

| | **Полученные данные** | **Рекомендации** |
|---|---|---|
| **Планирование аварийного восстановления и возобновления деятельности предприятия** | Ответ указывает на то, что организация выполняет процедуры аварийного восстановления и возобновления деятельности предприятия. | Продолжайте поддерживать и тестировать планы аварийного восстановления и возобновления деятельности предприятия. |
| **Планирование аварийного восстановления и возобновления деятельности предприятия** | Вы указали, что в вашей среде файлы журналов просматриваются регулярно. | Рассмотрите необходимость мониторинга файлов журналов из DMZ и основных сетевых серверов с помощью MOM (Microsoft Operations Manager). В случае создания критических записей журнала, MOM отправит предупреждения соответствующим сотрудникам. |
| **Планирование аварийного восстановления и** | Ответ указывает на то, что организация не применяет | Требуйте разработки, документирования, |

| | | |
|---|---|---|
| **возобновления деятельности предприятия** | процедуры аварийного восстановления и возобновления деятельности предприятия. | реализации, а также периодических проверки, тестирования и обновления планов аварийного восстановления. Разработайте планы непрерывной работы предприятия, предусматривающие действия персонала, места размещений, а также системы и другие технологические проблемы. |
| **Планирование аварийного восстановления и возобновления деятельности предприятия** | Вы указали, что не знаете ответа на этот вопрос. | Проверьте открытые компоненты вместе в ИТ-специалистами своей компании или деловым партнером по обеспечению безопасности. Чтобы получить более подробные сведения, введите наиболее подходящий ответ на вопрос в средстве MSAT (Microsoft Security Assessment Tool). |
| **Планирование аварийного восстановления и возобновления деятельности предприятия** | Вы указали, что не знаете, с какой периодичностью просматриваются файлы журналов. | Служба безопасности должна ежедневно просматривать файлы журналов на предмет подозрительной или аномальной активности. Рассмотрите необходимость мониторинга файлов журналов из DMZ и основных сетевых серверов с помощью MOM (Microsoft Operations Manager). В случае создания критических записей журнала, MOM отправит предупреждения соответствующим сотрудникам. |
| **Подкатегория** | **Передовые методики** | |
| **Архивация** | Регулярно следует выполнять полную архивацию. Если возможно, необходимо выполнять частичную промежуточную архивацию между полными архивациями. В стратегии архивации должны рассматриваться наихудшие сценарии полного восстановления системы и приложения. Для важных приложений процесс восстановления должен полностью восстановить функции приложения за минимальное время. | |
| | **Полученные данные** | **Рекомендации** |
| **Архивация** | Ваш ответ указывает на то, что важные материалы в вашей среде архивируются на регулярной основе. | Проведите аудит механизмов архивации и обеспечьте регулярное архивирование всех важных активов. Периодически проверяйте работоспособность функций восстановления, чтобы контролировать возможность |

| | | |
|---|---|---|
| | | восстановления с резервных носителей. |
| **Подкатегория** | **Передовые методики** | |
| **Резервные носители** | Для управления хранением и работой резервных носителей должны применяться подробные политики. Эти политики должны касаться следующих проблем:+ Хранение на месте/за пределами сети<br>+ Чередование носителей<br>+ Элементы управления безопасностью<br>+ Элементы управления доступом персонала<br><br>Съемные резервные носители необходимо хранить в запертых, несгораемых корпусах, доступ к которым имеет только уполномоченный персонал.<br><br>Необходимо использовать хранение данных за пределами сети для повышения возможности их восстановления после сбоя. | |
| | **Полученные данные** | **Рекомендации** |
| **Резервные носители** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Подкатегория** | **Передовые методики** | |
| **Архивация и восстановление** | Необходимо выполнять регулярные проверки процедур архивации и восстановления, чтобы определить сбойные носители и повысить вероятность успешного восстановления в случае сбоя.<br>Необходимо подробно задокументировать все процедуры восстановления различных систем, включая приложения.<br><br>Следует проверить все документы, посвященные архивации и восстановлению, чтобы убедиться, что в них описаны все критические системы, необходимые для непрерывного ведения бизнеса. | |
| | **Полученные данные** | **Рекомендации** |
| **Архивация и восстановление** | Ваш ответ показал, что для процедур архивации и восстановления существует хорошо документированная политика. | Следует проверить все документы, посвященные архивации и восстановлению, чтобы убедиться, что в них описаны все критические системы, необходимые для непрерывного ведения бизнеса. Регулярно проверяйте процедуры архивации и восстановления, |

| | |
|---|---|
| | чтобы контролировать надлежащее функционирование всех аппаратных и программных компонентов. |

## Персонал

Усилия, направленные на обеспечение безопасности, часто не включают организационные аспекты, которые важны для поддержания общей безопасности в организации. В этом разделе оценки рассматриваются внутренние процессы предприятия, определяющие корпоративную политику безопасности, процессы, связанные с персоналом, осведомленность сотрудников о безопасности и их обучение. В области анализа, связанной с персоналом, также рассматривается безопасность применительно к повседневным операциям, относящимся к назначениям и определению ролей. Оценка предусматривает проверку процедур высокого уровня, которые организация может выполнять для снижения угрозы со стороны персонала, сосредоточившись на следующих областях безопасности, связанных с персоналом:

- Требования и оценки — Планирование, Сторонние оценки
- Политика и процедуры — Кадровая политика, Сторонние взаимосвязи
- Обучение и осведомленность — Осведомленность о безопасности

| **Требования и оценки** | | |
|---|---|---|
| **Подкатегория** | **Передовые методики** | |
| **Требования по безопасности** | Организации следует определить круг лиц, обладающих достаточной квалификацией по системам безопасности, которые должны участвовать во всех обсуждениях и принятии решений, связанных с безопасностью. Организация должна определить необходимые составляющие защиты на основе ценности имущества, а также уровень безопасности, требуемый для его защиты. Все векторы угроз включаются в анализ. Выработанная стратегия должна быть уравновешена с точки зрения расходов и преимуществ защиты. Кроме того, она может включать передачу или принятие рисков. Требования по безопасности, полученные от представителей бизнеса и технических специалистов, должны быть задокументированы и опубликованы с целью ознакомления и будущего использования всеми сторонами. Различия между классами приложений и данных может привести к определению других конечных требований. | |
| | **Полученные данные** | **Рекомендации** |
| **Требования по безопасности** | Вы указали, что в вашей организации имеется модель для назначения уровней критичности каждому компоненту вычислительной среды. | Продолжите назначение уровней важности для компонентов и обязательно обновляйте модель при добавлении нового оборудования. |
| **Требования по безопасности** | Ваш ответ указывает на то, что в определение требований по безопасности вовлечены группы по безопасности и бизнесу. | Группа, отвечающая за обеспечение безопасности, должна участвовать во всех мероприятиях, связанных с разработкой требований, проектированием и |

| | | |
|---|---|---|
| | | развертыванием технологий. Требования по безопасности должны быть четко задокументированы и являться частью функциональных требований. |
| **Подкатегория** | **Передовые методики** | |
| **Оценки безопасности** | Необходимо провести стороннюю оценку, чтобы получить полезную и объективную точку зрения на состояние системы безопасности организации.<br>Сторонние оценки могут быть также полезны для обеспечения соответствия требованиям нормативов, клиентов, партнеров и поставщиков.<br><br>Оценки должны затрагивать инфраструктуру, приложения, политики, а также процедуры аудита. Целью этих оценок должно быть не только определение проблем безопасности, но также проверка небезопасных конфигураций и прав внешнего доступа. Необходимо проверить и оценить политики и процедуры безопасности на предмет пробелов. | |
| | **Полученные данные** | **Рекомендации** |
| **Оценки безопасности** | Ваш ответ указывает на то, что в вашей организации в данный момент производится независимая оценка безопасности. | Независимые оценки очень полезны для любой организации. Обязательно организуйте проведение регулярных независимых оценок. В случае значительного изменения схемы и конфигурации существующей среды запланируйте и при первой возможности проведите оценку системы безопасности. |
| **Оценки безопасности** | Вы указали, что оценки безопасности для вашей организации выполняются внутренним персоналом. | Продолжайте практику частых проверок безопасности внутренним персоналом, но в дополнение к этому привлекайте заслуживающую доверия стороннюю организацию. |
| **Оценки безопасности** | Вы указали, что оценки выполняются ежеквартально. | Продолжайте практику ежеквартальной оценки безопасности. |

| **Политика и процедуры** | |
|---|---|
| **Подкатегория** | **Передовые методики** |
| **Проверка в фоновом режиме** | Для определения любых потенциальных проблем необходимо проводить проверки в фоновом режиме, тем самым снижая риск для организации и других служащих. Этот шаг также позволяет |

| | | |
|---|---|---|
| | определить любые потенциальные проблемы и пробелы в резюме кандидата.<br>Процесс найма должен включать обзор предыдущих мест работы кандидата и сведения о привлечении к юридической ответственности.<br><br>Необходимо оценить навыки кандидата с точки зрения подробных должностных инструкций и требований, чтобы оценить его сильные и слабые стороны. | |
| | **Полученные данные** | **Рекомендации** |
| **Проверка в фоновом режиме** | Ваш ответ указывает на то, что проверка в фоновом режиме выполняется по отношению ко всем сотрудникам. | Отлично, продолжайте реализацию этой политики. Проверка биографических данных должна включать обзор предыдущих мест работы кандидата, сведений об образовании и привлечении к юридической ответственности. |
| **Подкатегория** | **Передовые методики** | |
| **Политика отдела кадров** | Формальная процедура увольнения должна гарантировать, что предприняты все необходимые шаги при завершении трудового соглашения.<br>Должны существовать процедуры для увольнения как по обычным причинам, так и в результате конфликтов.<br><br>Эти процедуры должны включать следующее:<br>+ Уведомление всех отделов — отдела кадров, ИТ, физической защиты, службы поддержки, финансового отдела и т.д.<br>+ Выдворение служащего за пределы компании<br>+ Удаление всех учетных записей и прекращение доступа к сети<br>+ Сдача собственности, принадлежащей компании — переносные и карманные компьютеры, электронные носители, конфиденциальные документы и т.д. | |
| | **Полученные данные** | **Рекомендации** |
| **Политика отдела кадров** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| **Подкатегория** | **Передовые методики** | |
| **Сторонние взаимосвязи** | Чтобы снизить риск разглашения данных, необходимо применять формальные политики и процедуры для урегулирования взаимоотношений со сторонними компаниями. Эти политики и процедуры позволяют определить проблемы безопасности и ответственность каждой из сторон при их | |

| | | |
|---|---|---|
| | устранении.<br>Эти политики должны включать следующее:<br>+ Уровень соединения и доступа<br>+ Представление данных и работа с ними<br>+ Роли и ответственность (включая полномочия) каждой стороны<br>+ Управление взаимоотношениями — установка, продолжение и прекращение. | |
| | **Полученные данные** | **Рекомендации** |
| **Сторонние взаимосвязи** | Вы указали, что конфигурирование систем выполняется внутренним персоналом. | Системы должны настраиваться внутренним персоналом в соответствии с проверенным образом. |
| **Сторонние взаимосвязи** | Вы указали, что ваша организация самостоятельно осуществляет управление вычислительной средой. | В зависимости от потребностей бизнеса, подходящим решением будет самоуправление или привлечение внешних ресурсов. Если управление осуществляется с использованием внешних ресурсов, требования по безопасности необходимо оговорить в контракте, а соглашения об уровне сервиса (SLA) предназначены для обеспечения соответствия этим требованиям. |
| **Сторонние взаимосвязи** | Вы указали, что не знаете ответа на этот вопрос. | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |

| **Обучение и осведомленность** | |
|---|---|
| **Подкатегория** | **Передовые методики** |
| **Осведомленность о безопасности** | Программа уведомления о вопросах безопасности позволяет служащим внести свой вклад в общее состояние системы безопасности компании благодаря информированию их о последних угрозах безопасности. Хорошо осведомленные служащие могут немедленно сообщить о проблемах безопасности.<br>В эффективной программе осведомленности должны учитываться все аспекты безопасности, включая приложение, сеть и физические устройства, а также содержаться четкие инструкции относительно обязанностей служащих в случае обнаружения ими того, что может подвергнуть опасности любой из этих элементов. |

| | | |
|---|---|---|
| | Следует реализовать политики, которые регулируют использование служащими ресурсов компании.<br><br>Программа осведомленности должна стать составной частью обучения нового персонала. Необходимо регулярно проводить курсы повышения квалификации и обновления, чтобы гарантировать, что все служащие знакомы с последними практиками и рисками.<br><br>Чтобы гарантировать полное понимание служащими этого материала, необходимо проводить регулярные проверки. | |
| | **Полученные данные** | **Рекомендации** |
| **Осведомленность о безопасности** | Вы указали, что в вашей организации в отношении безопасности существует индивидуальная или групповая ответственность. | Продолжайте поддерживать в компании специалиста или группу специалистов, ответственных за безопасность, и требуйте обязательной консультации с этими сотрудниками перед изменением вычислительной среды. |
| **Осведомленность о безопасности** | Вы указали, что группа, обеспечивающая безопасность в вашей организации, участвует в определении требований для новых и существующих технологий. | Продолжайте практику консультации со специалистом/группой специалистов по безопасности перед изменением вычислительной среды. Консультироваться с группой специалистов по безопасности необходимо на ранних стадиях планирования. |
| **Осведомленность о безопасности** | Ваш ответ указывает на то, что в вашей организации все же существует программа осведомленности о вопросах безопасности. | Все сотрудники должны участвовать в обучении по вопросам осведомленности. Осведомленность о вопросах безопасности должна стать обязательной составной частью обучения нового персонала.<br>Хорошо осведомленные служащие могут немедленно сообщить о проблемах безопасности. |
| **Осведомленность о безопасности** | Вы указали, что обучение проводится ежегодно. | Обучение по вопросам безопасности должно проводиться для всех сотрудников ежеквартально. |
| **Осведомленность о** | Вы указали, что в программе | Продолжайте практику |

| | | |
|---|---|---|
| **безопасности** | уведомления о вопросах безопасности участвовало более 75% всех служащих. | обязательного участия всех сотрудников в обучении по вопросам осведомленности о безопасности.<br>Осведомленность о вопросах безопасности должна стать обязательной составной частью обучения нового персонала.<br>Хорошо осведомленные служащие могут немедленно сообщить о проблемах безопасности. |

| **Подкатегория** | **Передовые методики** |
|---|---|
| **Обучение в области безопасности** | В сотрудничестве с владельцами предприятий определите приемлемую продолжительность времени простоя для критически важных приложений. Основываясь на полученных данных, примите необходимые меры, чтобы обеспечить полное соответствие выработанным требованиям. Доступность и производительность веб-приложений можно улучшить за счет развертывания подсистем балансировки нагрузки перед веб-серверами. Принцип работы подсистемы балансировки нагрузки заключается в распределении запросов на разные узлы в кластере серверов с целью оптимизации производительности системы. Если на одном веб-сервере в кластере серверов происходит сбой, запрос перенаправляется для обработки на другой сервер, что обеспечивает высокий уровень доступности.<br>В сотрудничестве с владельцами предприятий определите приемлемую продолжительность времени простоя для критически важных файловых ресурсов и баз данных. Протестируйте механизмы перехода приложений на другие ресурсы при сбое и определите соответствие продолжительности времени простоя приемлемым значениям. |

| | **Полученные данные** | **Рекомендации** |
|---|---|---|
| **Обучение в области безопасности** | Ваш ответ указывает на то, что в данный момент проводится тематическое обучение для служащих в зависимости от их роли в организации. | Ролевое и непрерывное обучение - это неотъемлемый элемент, обеспечивающий понимание всеми служащими того, что от них требуется и как они должны выполнять эти требования. Продолжайте обучение сотрудников на всех уровнях в организации и по всем аспектам безопасности в зависимости от требований к должности. |

## Обучение и осведомленность - Ресурсы

| | | |
|---|---|---|
| Microsoft Security Certifications | The MCSE: Security for Windows Server2003 certification provides you the skill set to secure a Windows Server environment. | http://www.microsoft.com/learning/mcp/mcse/security/windowsserver2003.mspx |
| Industry Security Certifications | (ISC)2 - CISSP, SSCP Certifications ISACA - CISM, CISA Certifications CompTIA - Security+ | http://www.isc2.org<br><br>http://www.isaca.org<br><br>http://www.comptia.org |
| Microsoft Security Awareness Toolkit | Microsoft recognizes that information security awareness and training is critical to any organization's information security strategy and supporting security operations. People are in many cases the last line of defense against threats such as malicious code, disgruntled employees, and malicious third parties. Therefore, people need to be educated on what your organization considers appropriate security-conscious behavior, and also what security best practices they need to incorporate in their daily business activities. This kit was created to provide guidance, samples, and templates for creating your own security awareness program. | http://technet.microsoft.com/en-us/security/cc165442.aspx |

# Список приоритетных действий

Ниже в порядке приоритета расположены рекомендации, предложенные в разделе Подробная оценка. Для получения дополнительных сведений об этих элементах см. соответствующую запись в том разделе.

Партнер корпорации Майкрософт по обеспечению безопасности может оказать помощь в создании программы обеспечения безопасности, включающей эти действия.Подробная оценка. Для получения дополнительных сведений об этих элементах см. соответствующую запись в том разделе.

| **Список приоритетных действий** | |
|---|---|
| ***Предмет анализа*** | ***Рекомендация*** |
| **Высокий приоритет** | |
| Инфраструктура > Проверка подлинности > Пользователи с удаленным доступом | Если это еще не было сделано, рассмотрите необходимость использования многофакторной проверки подлинности для удаленного доступа и предоставьте доступ только тем сотрудникам, у которых реально существует потребность в удаленном подключении. |
| Приложения > Развертывание и использование > Независимый сторонний поставщик программного обеспечения | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения |

| | |
|---|---|
| | дальнейших сведений. |
| Приложения > Развертывание и использование > Уязвимые места в системе | Эти процедуры включают проверку исправлений в лабораторных условиях, а также проверку приложений после установки исправления, чтобы определить наличие конфликтов, из-за которых может потребоваться выполнить откат исправления. Периодически повторяйте эти процедуры, чтобы убедиться, что они соответствуют текущим требованиям приложения. |
| Операции > Архивация и восстановление > Планирование аварийного восстановления и возобновления деятельности предприятия | Продолжайте поддерживать и тестировать планы аварийного восстановления и возобновления деятельности предприятия. |
| Персонал > Политика и процедуры > Сторонние взаимосвязи | Системы должны настраиваться внутренним персоналом в соответствии с проверенным образом. |
| **Средний приоритет** | |
| Инфраструктура > Управление и контроль > Защищенная сборка | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| Инфраструктура > Проверка подлинности > Административные пользователи | Чтобы еще более снизить риск взлома пароля в административных учетных записях, выполните следующие рекомендации:<br>+ Истечение срока действия пароля<br>+ Блокировка учетной записи после 7 - 10 попыток неправильного ввода пароля<br>+ Ведение журнала системы |
| Инфраструктура > Защита по периметру > Удаленный доступ | Выполните проверку этого открытого элемента с участием ИТ-персонала или специалиста по безопасности. Введите наиболее подходящий ответ на это вопрос в средстве MSAT для получения дальнейших сведений. |
| Приложения > Схема приложения > Методологии разработки систем безопасности программного обеспечения | Продолжайте обучать разработчиков принципам разработки систем безопасности программного обеспечения. |
| Инфраструктура > Защита по периметру > Система определения вторжения (IDS) | Продолжайте практику развертывания сетевой системы определения вторжения. Следите за регулярным обновлением сигнатур вирусов, а также изучайте технологии предотвращения |

| | |
|---|---|
| | вторжения, так они становятся широко востребованными. |
| **Низкий приоритет** | |
| Операции > Среда > Узел управления - Серверы | Рассмотрите необходимость использования SSH или VPN для защиты текстовых протоколов. |
| Операции > Среда > Узел управления - Сетевые устройства | Следует протестировать все системы управления, в которых используется SNMP, чтобы убедиться, что в них используются последние версии исправлений и не используются настройки сообщества по умолчанию. |
| Операции > Политика безопасности > Правильное использование | Все сотрудники и клиенты, использующие корпоративные ресурсы, должны быть ознакомлены с этими политиками. Разместите политики в корпоративной интрасети и рассмотрите необходимость ознакомления с ними всех новых сотрудников при приеме их на работу. |
| Операции > Архивация и восстановление > Архивация | Проведите аудит механизмов архивации и обеспечьте регулярное архивирование всех важных активов. Периодически проверяйте работоспособность функций восстановления, чтобы контролировать возможность восстановления с резервных носителей. |
| Инфраструктура > Защита по периметру > Антивирус - Настольные компьютеры | Продолжайте использовать такую практику. Реализуйте политику, в соответствии с которой пользователям необходимо регулярно обновлять сигнатуры вирусов. Рассмотрите необходимость установки клиента антивирусной программы с использованием настроек для рабочей станции по умолчанию. |

# Приложения

## Вопросы и ответы

В рамках этой оценки были предоставлены следующие ответы.

| Вопрос оценки | Ваш ответ |
|---|---|
| **Business Risk Profile** | |
| Число используемых настольных и переносных компьютеров в компании: | Более 500 |
| Число используемых серверов в компании: | Более 25 серверов |
| Используется ли в вашей компании постоянное подключение к Интернету? | Да |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| Получают ли клиенты и поставщики доступ к сети или внутренним системам по Интернету? | Да |
| Предоставляет ли ваша компания на своем узле такие службы приложений, как портал или веб-узел, для внешних клиентов или партнеров? | Да |
| Развертывает ли ваша организация службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте? | Да |
| Подключаются ли внешние партнеры или клиенты непосредственно к внутренним серверным системам компании с целью получения доступа к данным, записи обновлений или обработки информации? | Да |
| Развертывала ли ваша организация идентичные компоненты серверной инфраструктуры, например базы данных, для поддержки как внешних приложений, так и внутренних корпоративных служб? | Да |
| Разрешено ли сотрудникам или подрядчикам вашей организации пользоваться удаленным доступом для подключения к внутренней корпоративной сети? | Да |
| Разрешено ли сотрудникам в вашей организации развертывать непроизводственные системы, например личные веб-серверы или компьютеры, на которых хранятся "любимые проекты", в общей корпоративной сети? | Нет |
| Разрешена ли в вашей организации, помимо резервных носителей/ленточных носителей, обработка конфиденциальных или принадлежащих компании данных за пределами сети? | Нет |
| Сильно ли повлияет дискредитация безопасности систем в вашей среде на способность компании вести дела? | Не знаю |
| Пользуется ли ваша компания офисным пространством совместно с другими организациями? | Нет |
| Разрабатывает ли ваша компания приложения? | Да |
| Разрешено ли разработчикам программного обеспечения в вашей организации пользоваться удаленным доступом для подключения к корпоративным ресурсам, связанным с разработкой, или удаленно разрабатывать код приложения? | Да |
| Разрабатывает ли ваша компания и поставляет ли программные продукты клиентам, партнерам или на рынок широкого потребления? | Да |
| Разрешено ли разработчикам в вашей организации вести разработку или тестировать системы удаленно или в каких-либо местах в незащищенных условиях? | Нет |
| Выступает ли ваш персонал ИТ в роли хранителя (в отличие от разработчика) важных бизнес-приложений? | Да |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| Требуется ли использовать в бизнес-процессах данные, которые хранятся, обрабатываются или распределяются третьей стороной? | Нет |
| Хранит или обрабатывает ваша компания данные клиента в общей среде совместно с корпоративными ресурсами? | Нет |
| Полагаетесь ли вы на сторонних партнеров по разработке программных продуктов с целью поддержки предложений, связанных с бизнес-службами? | Да |
| Получает ли ваша компания доход от предложения услуг, требующих обработки данных или информационной проходки? | Не знаю |
| Считает ли ваша организация данные, обработанные службами приложений компании, конфиденциальными или важными для деловых операций клиентов? | Да |
| Доступны ли основные бизнес-приложения компании через Интернет-соединения? | Нет |
| Кто является целевыми пользователями основных приложений в вашей среде? | Внутренние сотрудники и внешние клиенты, поставщики и партнеры |
| Каким образом основные приложения становятся доступны пользователям? | Из внутренней сети и с использованием удаленного доступа |
| Подключена ли корпоративная сеть к сетям клиента, партнера или сторонним сетям по сетевым соединениям - общедоступным или частным? | Нет |
| Получает ли ваша компания доход от услуг, в основе которых лежит хранение или распределение данных в электронном виде, например файлов мультимедиа или документации? | Не знаю |
| Прошла ли ваша организация через изменение "копирование и замена", касающееся любого основного компонента технологии, за последние 6 месяцев? | Не знаю |
| Полагается ли ваша компания на данные, полученные от партнеров, поставщиков или из сторонних источников, или данные, обработанные ими? | Да |
| Повлияет ли на доходность событие, нанесшее вред приложениям или инфраструктуре клиента, например бездействие узла, отказ оборудования или сбой в приложении? | Да |
| Хранит ли ваша компания конфиденциальные или важные данные клиентов? | Да |
| Зависит ли работа компонентов или приложений инфраструктуры клиентов от доступа к ресурсам в вашей среде? | Да |
| Используется ли инфраструктура и компоненты приложений вашей компании несколькими | Да |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| клиентами? | |
| Развертывает ли ваша организация новые службы или приложения до выполнения их оценки, относящейся к возможным проблемам безопасности? | Нет |
| Регулярно ли ваша организация меняет учетные данные для привилегированных учетных записей? | Да |
| Меняет ли ваша организация учетные данные для привилегированных учетных записей после увольнения персонала с привилегированным доступом? | Да |
| Считаете ли вы, что информационные технологии являются необходимым условием для вашей компании? | Да |
| Все ли сотрудники в вашей компании используют компьютеры для бизнеса? | Нет |
| Привлекает ли ваша компания внешний ресурс, управляющий или владеющий любой частью инфраструктуры? | Да |
| Существует ли у вашей компании среднесрочный или долгосрочный план для выбора и развертывания компонентов новых технологий? | Да |
| Считаете ли вы, что ваша организация является ранним последователем в новых технологиях? | Нет |
| Выбирает и разворачивает ли ваша организация новые технологии на основе существующих партнерских или лицензионных соглашений? | Да |
| Ограничивается ли ваша организация в выборе технологий только теми технологиями, которые известны текущему ИТ-персоналу? | Да |
| Расширяет ли ваша компания свою сеть посредством приобретения новых компаний и существующих в них сред? | Не знаю |
| Разрешено ли сотрудникам в вашей организации загружать конфиденциальные данные клиентов или корпоративные данные на свои рабочие станции? | Нет |
| Ограничивает ли ваша организация доступ пользователей к данным в зависимости от их роли в компании? | Да |
| Выберите вариант, который наиболее точно описывает отраслевой сегмент вашей компании: | Прочее |
| Выберите размер организации: | Более 500 сотрудников |
| Располагается ли ваша компания в разных местах? | Да |
| Относится ли деятельность вашей компании к чрезвычайно конкурентной или сосредоточенной на исследованиях отрасли, в которой кража интеллектуальной собственности или шпионаж может стать серьезной проблемой? | Да |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| Существует ли в вашей компании высокая текучесть среди специалистов по технологиям, а также изнурительные условия работы? | Да |
| Обладает ли ваша компания продуктом, имеющим важное значение, или широко известной торговой маркой? | Да |
| Используется ли вашей компании программное обеспечение самых ранних версий (которое уже не поддерживается поставщиком)? | Нет |
| Приобретает ли ваша организация программное обеспечение у известных и надежных поставщиков или источников? | Да |
| **Инфраструктура** | |
| Используются ли в вашей организации на границах сети межсетевые экраны или другие элементы управления доступом на сетевом уровне для защиты корпоративных ресурсов? | Да |
| Развертывает ли ваша организация эти элементы управления в каждом офисе? | Да |
| Использует ли ваша организация нейтральную зону (также широко известную как демилитаризованная зона или ДМЗ), отделяющую внутренние и внешние сети, в которых размещены службы? | Да |
| Размещены ли в вашей организации службы, связанные с Интернетом? | Да |
| Используется ли в вашей организации программное обеспечение межсетевого экрана на хост-компьютере для защиты серверов? | Да |
| Используется ли в вашей организации оборудование или программное обеспечение для определения вторжения, помогающее выявить злонамеренные атаки? | Да |
| Выберите тип(ы) используемой системы определения вторжения (IDS): | Сетевая система определения вторжения (NIDS) |
| Реализованы ли в среде антивирусные решения? | Да |
| Выберите системы, в которых развернуты антивирусные решения: | Настольные компьютеры |
| Возможен ли удаленный доступ к сети компании? | Да |
| Выберите тех, кто может удаленно подключаться к сети: | Сотрудники<br>Подрядчики |
| Используется ли технология виртуальной частной сети (VPN) для обеспечения возможности безопасного подключения удаленных пользователей к корпоративным ресурсам? | Да |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| Способна ли VPN ограничивать подключение к карантинной сети до прохождения клиентом всех необходимых проверок безопасности? | Не знаю |
| Проводится ли многофакторная проверка подлинности (маркеры, смарт-карты и т.п.) для удаленных пользователей? | Да |
| Существует ли в сети более одного сегмента? | Да |
| Используется ли сегментация сети для отделения внешнего клиента и служб внешней сети от корпоративных ресурсов? | Да |
| Группируются ли хост-компьютеры в вашей организации в сегменты сети исходя из схожих ролей или предложения схожих услуг? | Да |
| Группируются ли хост-компьютеры в вашей организации в сегменты сети исходя из предоставления только необходимых для подключающихся пользователей услуг? | Да |
| Был ли создан и документирован план, позволяющий управлять выделением адресов TCP/IP для систем в зависимости от требуемых сегментов? | Да |
| Существует ли возможность беспроводного подключения к сети? | Да |
| Какие из приведенных элементов управления безопасностью используются для упорядочения подключений к беспроводной сети? | Изменение заданного (по умолчанию) сетевого имени (известного также как идентификатора наборов служб или SSID) в точке доступа<br><br>Отключение широковещательной рассылки SSID<br><br>Включение шифрования WEP (Wired Equivalent Privacy)<br><br>Включение защищенного доступа Wi-Fi (WPA)<br><br>Включение аппаратных ограничений MAC-адреса<br><br>Подключение точки доступа к сети за пределами межсетевого экрана или в отдельном сегменте из проводной локальной сети |
| Существуют ли средства контроля для применения политик паролей к учетным записям разного типа? | Да |
| Выберите учетные записи, для которых существуют средства контроля для применения политик паролей: | Администратор<br><br>Пользователь<br><br>Удаленный доступ |
| Укажите вариант проверки подлинности, используемый для административного доступа к управлению устройствами и хост-компьютерами: | Многофакторная проверка подлинности |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| Укажите вариант проверки подлинности, используемый для доступа внутренних пользователей к внутренней сети и хост-компьютеру: | Многофакторная проверка подлинности |
| Укажите вариант проверки подлинности, используемый для удаленного доступа пользователей: | Многофакторная проверка подлинности |
| Разрешена ли блокировка учетной записи для блокирования доступа после определенного числа неудачных попыток входа в систему? | Да |
| Разработаны ли в организации процессы наблюдения за неактивными учетными записями администраторов, сотрудников, поставщиков и удаленных пользователей? | Не знаю |
| Конфигурирование систем выполняется самой компанией или поставщиком оборудования/продавцом? | Конфигурируется внутренним персоналом |
| Что из приведенного создается на основе образа или формальной документированной конфигурации? | Рабочие станции и переносные компьютеры<br><br>Серверы |
| Включает ли в себя эта конфигурация процедуры 'укрепления узла'? | Не знаю |
| Какие из приведенных решений были установлены на рабочих станциях и переносных компьютерах сотрудников? | Программа обнаружения и удаления шпионских средств |
| Разработаны ли в организации формальные процедуры реагирования на нарушения безопасности? | Да |
| Разработаны ли в организации политики и процедуры создания отчетов в случаях нарушения безопасности или возникновения проблем, имеющих отношение к безопасности? | Да |
| Развернуты ли элементы управления физической безопасностью для защиты имущества компании? | Да |
| Какие из приведенных элементов управления безопасностью используются? | Система сигнализации, установленная для обнаружения незаконного вторжения и оповещения<br><br>Сетевое оборудование (коммутаторы, кабельные системы, Интернет-соединение) находится в закрытом помещении с ограниченным доступом<br><br>Сетевое оборудование находится также в запираемом шкафу/стойке<br><br>Серверы находятся в закрытом помещении с ограниченным доступом<br><br>Серверы находятся также в запираемых шкафах/стойках |
| Какие из перечисленных мер контроля физического | Идентификационные карточки для сотрудников и |

| | |
|---|---|
| доступа используются? | посетителей |
| | Журналы регистрации посетителей |
| | Контрольно-пропускные пункты |

| **Приложения** | |
|---|---|
| Существуют ли в вашей компании важные бизнес-приложения (LOB)? | Не знаю |
| Используются ли у вас специально разработанные макросы для офисных приложений (например для Word, Excel или Access)? | Не знаю |
| Какие механизмы действуют на местах для обеспечения высокой доступности приложений? Выберите в приведенном списке все развернутые механизмы: | Балансировка нагрузки |
| | Кластеризация |
| | Регулярная проверка приложения и восстановление данных |
| Собственная группа разрабатывала какие-либо основные приложения, развернутые в вашей среде? | Не знаю |
| Были ли какие-либо из основных приложений, развернутых в инфраструктуре предприятия, разработаны сторонними консультантами или поставщиками? | Да |
| Предоставляет ли сторонний консультант или поставщик регулярное обновление программного обеспечения, исправления для системы безопасности и сведения о способах обеспечения безопасности? (Действует ли такая поддержка в настоящее время?) | Проектирование |
| | Написание кода |
| | Тестирование/контроль качества |
| | Окончательная проверка |
| Регулярно ли сторонний поставщик предоставляет программные обновления и исправления, повышающие безопасность, а также документацию по механизмам безопасности? (существует ли еще поддержка) | Да |
| Какие методологии разработки систем безопасности программного обеспечения применяются в компании? (Отметьте все подходящие варианты) | Другие |
| Располагает ли ваша организация сведениями о проблемах безопасности, существующих в каком-либо приложении, используемом в среде? | Да |
| Имеются ли в вашей организации процедуры, направленные на устранение проблем безопасности? | Да |
| Проводит ли компания обучение в области безопасности для разработчиков и испытателей? | Да |
| Какой процент разработчиков и испытателей компании прошел практическое обучение разработке | 75 % |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| систем безопасности? | |
| Проводит ли компания ежегодное обновление программы обучения персонала по разработке систем безопасности? | Да, необязательно |
| Применяет ли компания программные средства в качестве инструмента тестирования и аудита при разработке защищенного программного обеспечения? | Да, для некоторых проектов |
| Существуют ли средства контроля для применения политик паролей в основных приложениях? | Да |
| Выберите элементы управления, предусматривающие наличие паролей и применяемые для основных приложений: | Сложные пароли<br>Истечение срока действия пароля<br>Блокировка учетной записи |
| Выберите в приведенном списке наиболее распространенный метод проверки подлинности, используемый для основных приложений: | Многофакторная проверка подлинности |
| Существуют ли механизмы для основных приложений в вашей среде, позволяющие ограничивать доступ к критическим данным и функциональным возможностям? | Да |
| Записываются ли сообщения основных приложений в вашей среде в файлы журналов для проведения анализа и проверки? | Да |
| Выберите тип регистрируемых событий: | Неудачные попытки проверки подлинности<br>Успешные проверки подлинности<br>Ошибки приложения<br>Отказ в доступе к ресурсам<br>Успешный доступ к ресурсам<br>Изменения в данных<br>Изменения в учетных записях пользователей |
| Проверяются ли входные данные развернутыми приложениями? | Да |
| Выберите в приведенном списке входные данные приложения, в отношении которых проводится проверка: | Конечные пользователи<br>Клиентские приложения<br>Передачи данных |
| Шифруются ли основными приложениями обрабатываемые ими конфиденциальные и важные | Не знаю |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02
данные для бизнеса?

| **Операции** | |
|---|---|
| Управление средой осуществляется самой компанией или внешним ресурсом? | Средой управляет компания |
| Используются ли в организации выделенные узлы управления для безопасного управления системами и устройствами в вашей среде? | Да |
| Выберите системы, для которых существуют выделенные узлы управления: | Сетевые устройства<br>Серверы |
| Используются ли учетные записи для отдельного входа в систему в обычной или административной/управленческой деятельности? | Да |
| Предоставляет ли организация пользователям административные права доступа к их рабочим станциям и переносным компьютерам? | Да |
| Регулярно ли тестируется межсетевой экран в целях обеспечения ожидаемой производительности? | Да |
| Разработаны ли в организации планы аварийного восстановления и возобновления деятельности предприятия? | Да |
| Проходят ли эти планы регулярное тестирование? | Не знаю |
| Существует ли модель для назначения уровней критичности каждому компоненту вычислительной среды? | Да |
| Существуют ли политики для управления вычислительной средой? | Да |
| Существует ли политика безопасности информации, направленная на регулирование деятельности организации, связанной с безопасностью? | Да |
| Выберите тех, кто разрабатывал политику: | Совместно отделом ИТ и представителями бизнеса |
| Существует ли корпоративная политика правильного использования? | Да |
| Существуют ли политики для управления учетными записями отдельных пользователей? | Не знаю |
| Существует ли документированный процесс для сборок хост-компьютеров? Если да, то укажите, какого типа. (Для каких типов хост-компьютеров существует документированный процесс для сборок?) | Устройства инфраструктуры<br>Серверы<br>Рабочие станции и переносные компьютеры |
| Существуют ли документированные указания, которые предписывают, какие протоколы и службы разрешены в корпоративной сети? Выберите используемый вариант. | Указания существуют и документированы |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| Разработана ли в организации формальная и документально оформленная процедура утилизации данных на электронных и бумажных носителях? | Да |
| Разработана ли в компании схема классификации данных с соответствующими рекомендациями по их защите? | Да |
| Существует ли процесс управления изменениями и конфигурацией? | Да |
| Существуют ли в организации конфигурации, которые документируются для дальнейших справок? | Да |
| Проверяет ли организация изменения, внесенные в конфигурации, до развертывания в производственных системах? | Да |
| Проверяется и принимается ли соответствие конфигурации в централизованном порядке (например, в соответствии с групповой политикой для средств Active Directory)? | Да |
| Существует ли установленная политика исправлений и обновлений, а также сам процесс? | Да |
| Выберите компоненты, для которых они существуют: | Операционные системы и приложения |
| Проверяет ли организация исправления и обновления до их развертывания? | Да |
| Укажите, что из приведенного используется для развертывания и управления исправлений: | Автоматическое обновление Windows<br>Веб-узел Windows Update<br>Windows Server Update Services (WSUS)<br>Сервер Systems Management Server (SMS)<br>System Center Configuration Manager (SCCM) |
| На хост-компьютерах какого типа используется автоматизированное управление исправлениями? | Рабочие станции и переносные компьютеры<br>Серверы |
| Существует ли установленная политика, направленная на обновление продуктов обнаружения по сигнатуре? | Антивирус<br>Система определения вторжения (IDS) |
| Существуют ли точные логические схемы и справочная документация по конфигурации для сетевой инфраструктуры и хост-компьютеров? | Да |
| Существуют ли точные схемы архитектуры приложений и потоков данных для основных приложений? | Не знаю |
| Ведутся ли журналы в среде для записи событий на хост-компьютерах и устройствах? | Да |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| Предпринимает ли организация меры для защиты сведений, содержащихся в журналах? | В конфигурации операционной системы и приложений отключена возможность перезаписи событий<br><br>Доступ к файлам журнала разрешен только для учетных записей уровня администратора<br><br>Журналы ведутся на централизованном сервере журналов |
| Регулярно ли в организации просматриваются файлы журналов? | Да |
| С какой периодичностью просматриваются файлы журналов? | Не знаю |
| Регулярно ли резервируются важные и критические данные? | Да |
| Существуют ли политики и процедуры для хранения резервных носителей и работы с ними? | Не знаю |
| Существуют ли политики для регулярной проверки процедур архивации и восстановления? Документированы ли эти политики? | Да, и они документированы |
| **Персонал** | |
| Существует ли в вашей компании в отношении безопасности индивидуальная или групповая ответственность? | Да |
| Обладает ли такое лицо или группа должным опытом в области безопасности? | Да |
| Участвует ли это лицо или группа в определении требований по безопасности для новых и существующих технологий? | Да |
| На каких стадиях жизненного цикла технологий привлекается данная группа или лицо, обеспечивающее безопасность? | Планирование и проектирование<br><br>Реализация<br><br>Тестирование<br><br>Развертывание |
| Определены ли роли и обязанности для каждого лица, связанного с информационной безопасностью? | Да |
| Используются ли независимые сторонние специалисты для организации оценки безопасности среды? | Да |
| С какой периодичностью выполняются такие оценки безопасности? | Ежегодно |
| Выберите области анализа, которые охватываются этими оценками: | Инфраструктура<br><br>Приложение<br><br>Политика |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

| | |
|---|---|
| | Проверка |
| Выполняют ли оценки безопасности среды внутренние специалисты организации? | Да |
| С какой периодичностью выполняются такие оценки безопасности? | Ежеквартально |
| Выберите области анализа, которые охватываются этими оценками: | Инфраструктура |
| | Приложение |
| | Политика |
| | Проверка |
| Выполняются ли в организации проверки в фоновом режиме, являющиеся составной частью процесса найма? | Да |
| Выберите наиболее подходящий вариант: | Проверка в фоновом режиме выполняется по отношению ко всем должностям |
| Существует ли официальная политика в отношении служащих, покидающих компанию? | Не знаю |
| Существует ли официальная политика регулирования сторонних взаимосвязей? | Не знаю |
| Существует ли в вашей компании программа уведомления о вопросах безопасности? | Да |
| Сколько процентов сотрудников участвовало в программе уведомления о вопросах безопасности? | Более 75% |
| Какие темы охватывает обучение, связанное с осведомленностью? | Средства контроля и политики безопасности компании |
| | Оповещение о подозрительной активности |
| | Конфиденциальность |
| | Безопасность электронной почты, включая контроль спама и работу с вложениями |
| | Безопасность средств Интернета, включая веб-просмотр и загрузку файлов с узлов |
| | Безопасность компьютера, включая использование персональных межсетевых экранов и шифрование |
| С какой периодичностью проводится обучение? | Ежегодно |
| Проводится ли тематическое обучение для служащих в зависимости от их роли в организации? | Да |
| Выберите в приведенном списке все темы, которые | Безопасность операций |

можно отнести к данному случаю:

Безопасность инфраструктуры

Безопасность приложений

Готовность к происшествиям и реагирование

## Глоссарий

В глоссарии рассматриваются стандартные термины и понятия, используемые в отрасли обеспечения безопасности и включенные в данный отчет. Кроме того, могут быть включены и другие термины, не использованные в этом отчете.

| Термин | Определение |
|---|---|
| **AoAs** | Области анализа, которые являются инфраструктуры, приложений, операции, и люди. |
| **Приложения** | Прикладная программа, функциональные возможности которой использует конечный пользователь. Работает в загруженной операционной системе. В качестве примера приложения можно привести текстовый редактор, электронные таблицы и программы управления базами данных. |
| **антивирус** | Программные и аппаратные технологии, защищающие вычислительную среду от злонамеренных программных средств. |
| **профиль риска для бизнеса (ПРБ)** | Величина измерения риска, которому подвергается организация, в зависимости от бизнес-среды и отрасли, в условиях которых она конкурирует. |
| **индекс эшелонированной защиты (DiDI)** | Величина измерения защитных мер по обеспечению безопасности, используемых в отношении персонала, процессов и технологий для снижения рисков, выявленных на предприятии. |
| **демилитаризованная зона (ДМЗ)** | Часть сети, отделенная от внутренней сети межсетевым экраном, а также подключенная к Интернету через другой межсетевой экран. |
| **межсетевой экран** | Аппаратное или программное устройство, обеспечивающее защиту хост-компьютеров от несанкционированного доступа через сеть. |
| **Инфраструктура** | Сетевые функции, возможности управления ими и их поддержки для обеспечения защиты сети, реагирования на нештатные ситуации, безотказной работы сети и анализа ошибок. Включены поддержка внутренних и внешних бизнес-процессов, а также способы создания и развертывания узлов. |
| **многофакторная проверка подлинности** | Проверка подлинности, требующая сочетания как минимум двух из следующих условий: что известно; что имеем; или кто вы. Например, дебетовая |

| | |
|---|---|
| | банковская карта - это двухфакторная проверка подлинности. Для нее требуется то, что имеем (сама карта), и то, что известно (ПИН-код). Необходимость ввода кем-то нескольких паролей для проверки подлинности - это лишь однофакторная проверка подлинности, поскольку это как раз "то, что известно". Вообще, чем больше факторов, тем выше уровень безопасности при проверке подлинности. Таким образом, система, для которой требуется карта с идентификатором (то, что имеем), ПИН-код (то, что известно) и сканер отпечатков пальцев (кто вы), является более безопасной, чем система, которой требуется лишь имя пользователя/пароль (один фактор) или карта с идентификатором и ПИН-код. |
| **Операции** | The policies, processes, procedures, and practices related to the protection |
| **Персонал** | Члены организации, а также политики, процессы, процедуры и методы, относящиеся к защите сотрудников и организации. |
| **инфраструктура открытых ключей (PKI)** | Комплексный набор технологий, требуемых для обеспечения шифрования с использованием открытых ключей и цифровых подписей. Для обеспечения распределения ключей, целостности и конфиденциальности данных используется шифрование с комбинированием открытых и закрытых ключей. |
| **процесс** | Документированная серия последовательных задач, используемых для выполнения бизнес-функции. |

Средство Microsoft для оценки риска, связанного с безопасностью
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»
Завершено: 19-ноя-23 15:02

## Интерпретация графиков

- Показатель ПРБ находится в диапазоне от 0 до 100, где более высокая оценка подразумевает более высокий показатель потенциального риска для бизнеса в данной специфической области анализа (AoA). Важно отметить, что нулевое значение в данном случае невозможно, так как деловая деятельность сама по себе подразумевает наличие какого-то уровня риска. Кроме того, важно понимать, что существуют определенные аспекты ведения бизнеса, для которых отсутствует прямая стратегия снижения риска.

- Индекс DiDI также находится в диапазоне от 0 до 100. Высокий показатель свидетельствует о среде, в которой было принято множество мер для развертывания стратегий эшелонированной защиты (DiD) в конкретной области (AoA). Показатель DiDI не отражает общей эффективности безопасности или же ресурсы, затраченные на безопасность. Это, скорее, отражение общей стратегии, использованной для защиты среды.

- На первый взгляд, может показаться, что низкий показатель ПРБ и высокий показатель DiDI - это хороший результат, но это не всегда так. Масштаб данной самооценки не предусматривает все факторы, которые следует принять во внимание. При значительной диспропорции между показателями ПРБ и DiDI в конкретной области анализа рекомендуется изучить ее (AoA) как можно глубже. При анализе результатов важно учитывать индивидуальные показатели, как для ПРБ, так и DiDI, по отношению друг к другу. Стабильная среда, вероятно, будет представлена сравнительно одинаковыми показателями во всех областях. Разница между показателями DiDI - это явный признак того, что общая стратегия безопасности базируется на одной методике снижения риска. Если стратегия обеспечения безопасности не уравновешивает аспекты, связанные с персоналом, процессами и технологиями, то для среды существует вероятность повышенной уязвимости для злонамеренных атак.