Структура политики безопасности организации

Общие меры безопасности

Политика безопасности – формальное изложение правил, которых должны придерживаться пользователи при доступе к технологическим и информационным ресурсам.

Политика безопасности – **совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации**.

Политика может сводиться к простым правилам пользования или может занимать сотни страниц с детализацией каждого аспекта правил подключения и пользования сетью.

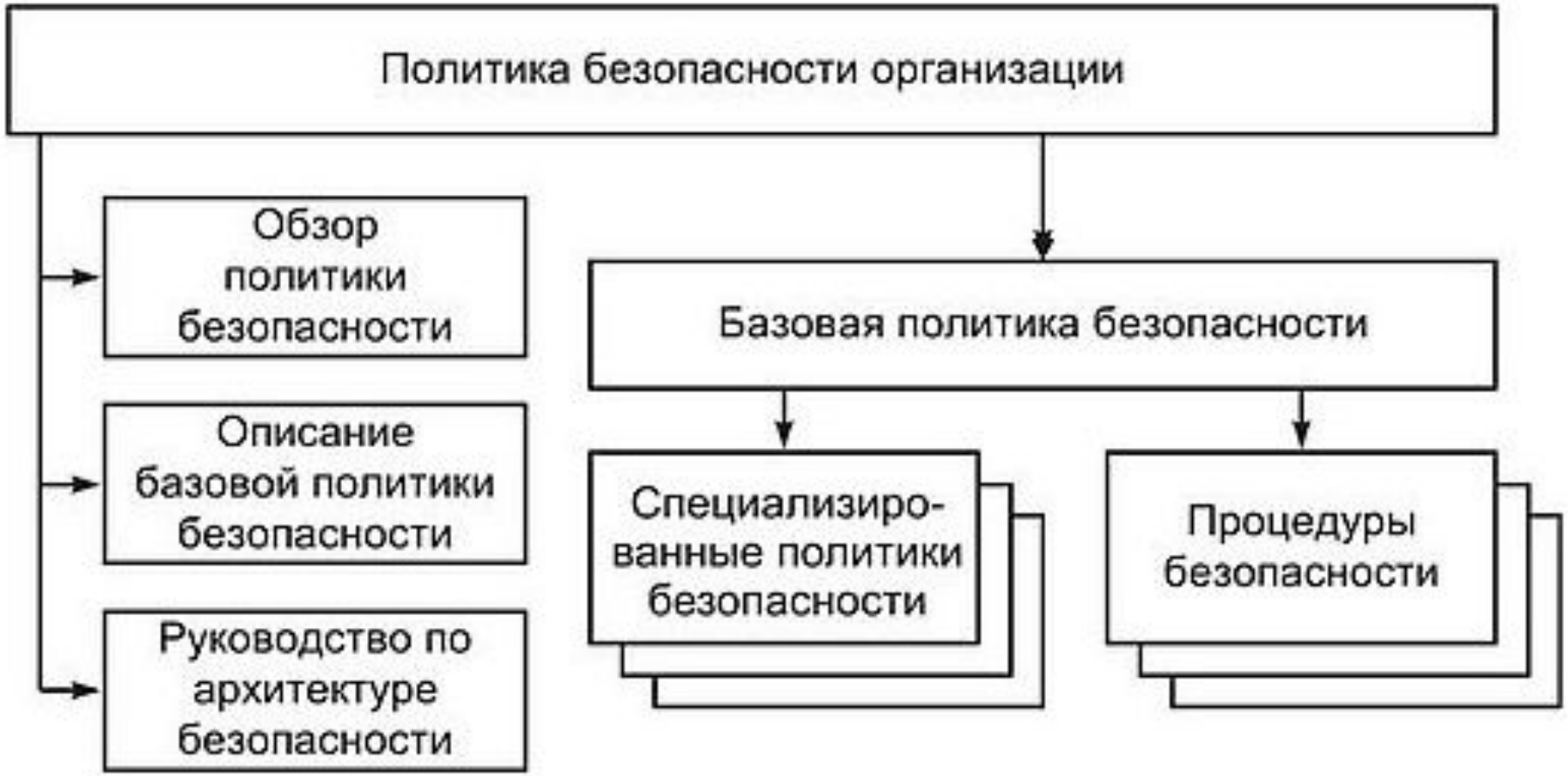
Политика безопасности должна обеспечить централизацию мер по защите, контролю, испытанию и развитию сети.

Разработанная политика безопасности будет эффективна только в том случае, если она будет поддерживаться и соблюдаться всеми пользователями сети.

Обычно политика безопасности организации включает:

- базовую политику безопасности
- специализированные политики безопасности
- процедуры безопасности

Структура политики безопасности организации



Понятия

- *обзор политики безопасности* — раскрывает цель политики безопасности, описывает структуру политики безопасности, подробно излагает, кто и за что отвечает, устанавливает процедуры и предполагаемые временные рамки для внесения изменений. В зависимости от масштаба организации политика безопасности может содержать больше или меньше разделов;
- *описание базовой политики безопасности* — определяет разрешенные и запрещенные действия, а также необходимые средства управления в рамках реализуемой архитектуры безопасности;
- *руководство по архитектуре безопасности* — описывает реализацию механизмов безопасности в компонентах архитектуры, используемых в сети организации

Потенциально существуют десятки специализированных политик, которые могут применяться большинством организаций среднего и большого размера. Некоторые политики предназначаются для каждой организации, другие — специфичны для определенных компьютерных окружений.

С учетом особенностей применения специализированные политики безопасности можно разделить на две группы:

- политики, затрагивающие значительное число пользователей;
- политики, связанные с конкретными техническими областями.

К специализированным политикам, затрагивающим значительное число пользователей, относятся:

- политика допустимого использования;
- политика удаленного доступа к ресурсам сети;
- политика защиты информации;
- политика защиты паролей и др.

К специализированным политикам, связанным с конкретными техническими областями, относятся:

- политика конфигурации межсетевых экранов;
- политика по шифрованию и управлению криптоключами;
- политика безопасности виртуальных защищенных сетей VPN;
- политика по оборудованию беспроводной сети и др.

Политика допустимого использования.

Цель

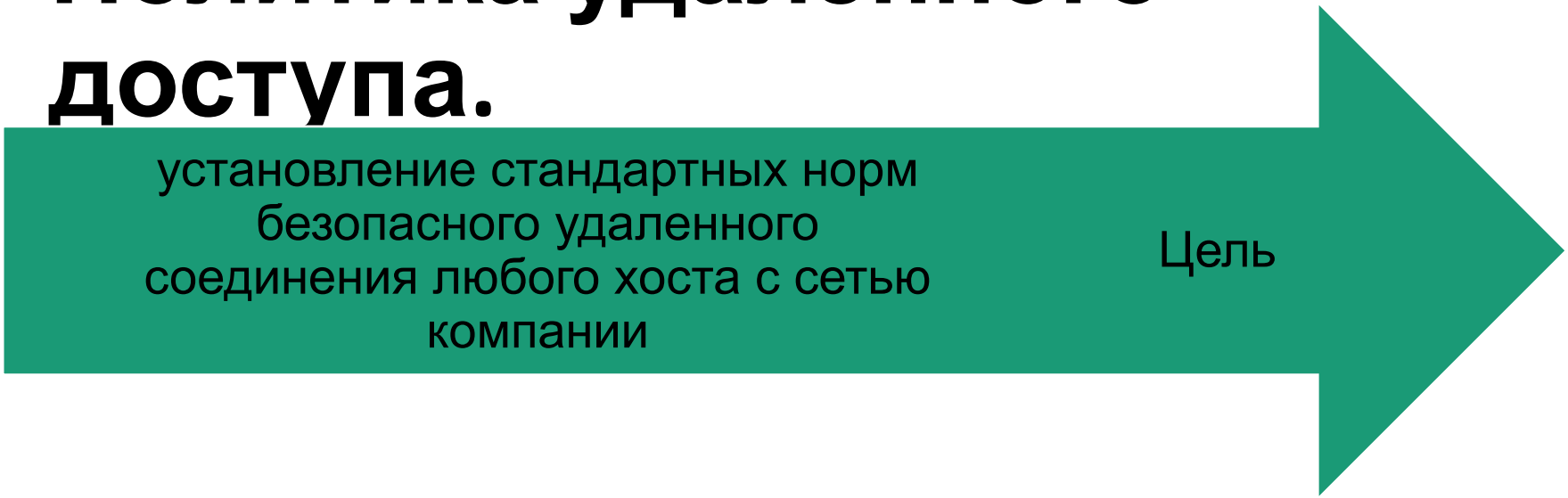
установление стандартных норм безопасного использования компьютерного оборудования и сервисов в компании

установление соответствующих мер безопасности сотрудников для защиты корпоративных ресурсов и собственной информации.

Политика допустимого использования устанавливает:

- ответственность пользователей за защиту любой информации, используемой и/или хранимой их компьютерами
- правомочность пользователей читать и копировать файлы, которые не являются их собственными, но доступны им
- уровень допустимого использования электронной почты и Web-доступа

Политика удаленного доступа.



Стандартные нормы призваны минимизировать ущерб компании из-за возможного неавторизованного использования ресурсов компании. К такому ущербу относятся: утрата интеллектуальной собственности компании, потеря конфиденциальных данных, искажение имиджа компании, повреждения критических внутренних систем компании и т. д.

Политика удаленного доступа:

- ✔ намечает и определяет допустимые методы удаленного соединения с внутренней сетью;
- ✔ существенна в большой организации, где сети территориально распределены;
- ✔ должна охватывать по возможности все распространенные методы удаленного доступа к внутренним ресурсам.

Политика удаленного доступа определяет:

- какие методы разрешаются для удаленного доступа;
- ограничения на данные, к которым можно получить удаленный доступ;
- кто может иметь удаленный доступ.

Политика безопасности

1. Правила идентификации и аутентификации
2. Правила назначения паролей
3. Правила допустимого использования
4. Правила использования удаленного доступа
5. Правила технического обслуживания сети
6. Правила поведения в аварийных ситуациях

Правила идентификации и аутентификации

- Используются для указания лиц, имеющих право доступа к ресурсам сети, и для описания процедур верификации.
- Сюда относится физический доступ в коммутационные отсеки и к основным сетевым ресурсам, таким как серверы, коммутаторы, маршрутизаторы и точки доступа.

Политика безопасности

1. Правила идентификации и аутентификации
2. Правила назначения паролей
3. Правила допустимого использования
4. Правила использования удаленного доступа
5. Правила технического обслуживания сети
6. Правила поведения в аварийных ситуациях

Правила назначения паролей

- Убедитесь, что пароли соответствуют минимальным требованиям и регулярно изменяются.

Политика безопасности

1.	Правила идентификации и аутентификации
2.	Правила назначения паролей
3.	Правила допустимого использования
4.	Правила использования удаленного доступа
5.	Правила технического обслуживания сети
6.	Правила поведения в аварийных ситуациях

Правила допустимого использования

- Описывают допустимые сетевые приложения и формы использования сети.

Политика безопасности

1. Правила идентификации и аутентификации
2. Правила назначения паролей
3. Правила допустимого использования
4. Правила использования удаленного доступа
5. Правила технического обслуживания сети
6. Правила поведения в аварийных ситуациях

Правила использования удаленного доступа

- Описывают, каким образом удаленные пользователи могут получить доступ к сети, а также к чему получает доступ пользователь, использующий удаленное подключение.

Политика безопасности

1. Правила идентификации и аутентификации
2. Правила назначения паролей
3. Правила допустимого использования
4. Правила использования удаленного доступа
5. Правила технического обслуживания сети
6. Правила поведения в аварийных ситуациях

Правила технического обслуживания сети

- Описывает процедуры обновления операционных систем сетевых устройств и приложений конечных пользователей.

Политика безопасности

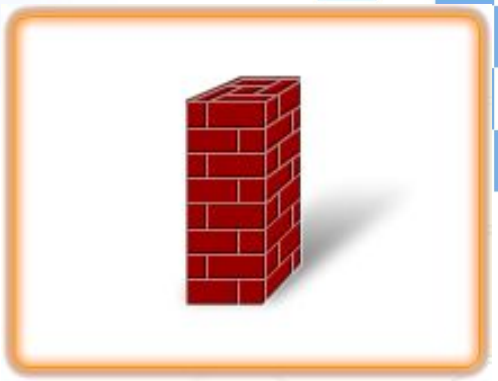
1.	Правила идентификации и аутентификации
2.	Правила назначения паролей
3.	Правила допустимого использования
4.	Правила использования удаленного доступа
5.	Правила технического обслуживания сети
6.	Правила поведения в аварийных ситуациях

Правила поведения в аварийных ситуациях

- Описывают правила поведения в аварийных ситуациях.

Средства безопасности

Межсетевой экран
Средство обеспечения безопасности для контроля входящего и исходящего трафика для данной сети.



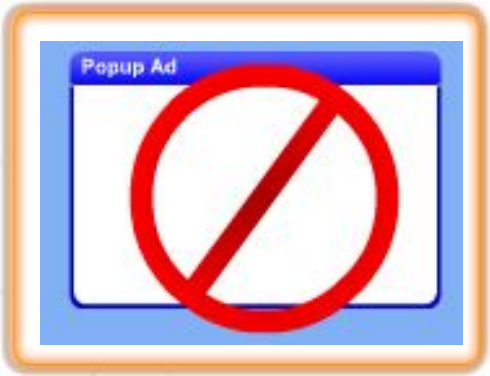
Спам-фильтр
Программное обеспечение, устанавливаемое на рабочей станции конечного пользователя или на сервере, для выявления и удаления нежелательной почты.

Патчи и обновления
Программное обеспечение, дополняющее операционную систему или приложение и устраняющее уязвимые для атаки места или добавляющее дополнительные функции.

Средства безопасности

Защита от шпионского ПО
Программное обеспечение, устанавливаемое на рабочей станции конечного пользователя для выявления и удаления шпионского и рекламного ПО.

Средство блокирования всплывающих окон
Программное обеспечение, устанавливаемое на рабочей станции конечного пользователя, для предотвращения появления всплывающих окон, содержащих рекламу.



Антивирусная программа
Программное обеспечение, устанавливаемое на рабочей станции конечного пользователя или сервере, для выявления и удаления вирусов, червей или "Троянских коней" из файлов или электронных сообщений.

Процедуры безопасности

Политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты.

Процедуры безопасности определяют, как защитить ресурсы и каковы механизмы исполнения политики, т. е. как реализовывать политики безопасности.

Назначение

Процедуры безопасности детально определяют действия, которые нужно предпринять при реагировании на конкретные события; обеспечивают быстрое реагирование в критической ситуации; помогают устранить проблему единой точки отказа в работе, если, например, во время кризиса работник неожиданно покидает рабочее место или оказывается недоступен.

Примеры

В качестве примеров можно указать процедуры для резервного копирования и внесистемного хранения защищенных копий,

процедуры для вывода пользователя из активного состояния и/или архивирования логина и пароля пользователя, применяемые сразу, как только данный пользователь увольняется из организации.

Процедура реагирования

Процедура реагирования на события является необходимым средством безопасности для большинства организаций. Организация особенно уязвима, когда обнаруживается вторжение в ее сеть или когда она сталкивается со стихийным бедствием.

Иногда называют процедурой обработки событий или процедурой реагирования на инциденты.

Данная процедура определяет:

- обязанности членов команды реагирования;
  - какую информацию регистрировать и прослеживать;
  - как обрабатывать исследование отклонений от нормы и атаки вторжения;
  - кого и когда уведомлять;
  - кто может выпускать в свет информацию и какова процедура выпуска информации;
  - как должен выполняться последующий анализ и кто будет в этом участвовать.

Процедура управления конфигурацией

Обычно определяется на корпоративном уровне или уровне подразделения. Эта процедура должна определить процесс документирования и запроса изменений конфигурации на всех уровнях принятия решений. В принципе должна существовать центральная группа, которая рассматривает все запросы на изменения конфигурации и принимает необходимые решения.

Процедура управления конфигурацией определяет:

- кто имеет полномочия выполнить изменения конфигурации аппаратного и программного обеспечения;
- как тестируется и инсталлируется новое аппаратное и программное обеспечение;
- как документируются изменения в аппаратном и программном обеспечении;
- кто должен быть проинформирован, когда случаются изменения в аппаратном и программном обеспечении.