ДОКУМЕНТАЦИЯ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО ТРЕБОВАНИЯМ ISO/IEC 27001:2005

Дмитриев Александр Анатольевич
Учредитель, главный редактор
журнала "Das Management",
ведущий аудитор ISO 9001, ISO/IEC 27001, BS 25999

ЧТО ТАКОЕ СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

Система менеджмента информационной безопасности (СМИБ) необходима любому предприятию для сохранения целостности, конфиденциальности и доступности информационных активов предприятия. Современные практики по управлению СМИБ базируются на международном стандарте ISO/IEC 27001. Объектами СМИБ являются все информационные активы: бумажные и электронные документы, компьютеры, информационные системы, сети, а также персонал, хранящий и обрабатывающий информацию в своих головах. Для всех информационных активов существуют угрозы различной степени важности. Основная выгода внедрения СМИБ – выявление наиболее опасных угроз и экономия средств на создание эффективной системы обеспечения информационной безопасности.

КРАТКИЙ АЛГОРИТМ ВНЕДРЕНИЯ

Порядок внедрения СМИБ подробно не описан ни в одной, имеющейся на рынке, книге или стандарте. Каждый консультант имеет собственную методику внедрения, которая базируется на его навыках и опыте работе. Однако для понимания необходимости разработки документации рекомендуется рассмотреть общий (рамочный) алгоритм внедрения СМИБ с указанием примерных сроков, необходимых для реализации каждого этапа.

Этап	Срок	Описание
I	1 месяц	Получение поддержки со стороны высшего руководства в виде приказа и определения ответственных за внедрение и поддержку СМИБ.
II	*2-3 месяца*	Проведение анализа существующей СМИБ и определение перечня работ по доработке существующей СМИБ.
III	1-2 месяца	Определение перечня мероприятий для достижения требований стандарта. Подготовка плана работ по внедрению СМИБ.
IV	3-9 месяцев	Разработка документации **1. Внедрение системы управления рисками** • Разработать процедуру по идентификации рисков • Создать реестр активов с учетом требований стандарта • Рассчитать и описать риски • Разработать положение о применимости контролей **2. Разработка основного пакета документации** • Создать перечень документов (процедур, записей, инструкций) для разработки • Разработать процедуры и другие документы (*управленческие процедуры, технические процедуры, записи управленческие, записи технические, инструкции, положения)*
V	5-12 месяцев	Обучение персонала и принятие мер по обеспечению работы СМИБ
VI	1-2 месяца	Внутренний аудит СМИБ и анализ СМИБ со стороны высшего руководства

Приведенный алгоритм демонстрирует необходимость разработки пакета документации для реализации требований стандарта. Разработка документации, как правило, продолжительный процесс. Данная статья поможет Вам в его реализации.

РАЗРАБОТКА ДОКУМЕНТАЦИИ – ТРУДОЕМКИЙ ЭТАП ВНЕДРЕНИЯ СМИБ

В процессе внедрения СМИБ требуется разработать объемный пакет документации. На внедрение эффективной СМИБ может уйти от 1-го до 2-х лет. В этом процессе на разработку документации СМИБ может потребоваться от 3 до 9 месяцев. Это огромный, но необходимый объем работы. Неправильно организованный процесс разработки документации может привести к серьезному перерасходу ресурсов и, более того, может снизить до минимума эффект от внедрения СМИБ. Поэтому данная статья ставит целью увести разработчика СМИБ от долгих и ошибочных путей.

СТРУКТУРА ДОКУМЕНТАЦИИ СМИБ

Документация СМИБ может иметь любую удобную для Вас структуру. Исходя из практического опыта предлагаем Вам условно разделить документацию СМИБ на четыре группы, как представлено на рисунке 1: административные документы, документы верхнего уровня, документы среднего уровня и документы нижнего уровня.

Предлагаемая структура позволит Вам разделить трудоемкую работу на несколько логических частей. Разработка документации ведется с верхней точки пирамиды до нижней.

Административные документы являются отправной точкой для внедрения СМИБ. Их разработку и издание осуществляет высшее руководство. С помощью административных документов будет установлена соответствующая организационная структура для управления информационной безопасностью на предприятии. Уполномоченное лицо по информационной безопасности получит основания для внедрения и поддержания СМИБ. Должность уполномоченного по информационной безопасности в странах ЕС при-

нято называть «офицер по ИТ-безопасности». Важнейшим результатом выпуска административных документов является определение офицера по ИТ-безопасности и наделение его соответствующими полномочиями. С этого момента начинается работа над созданием основной документации самой СМИБ.

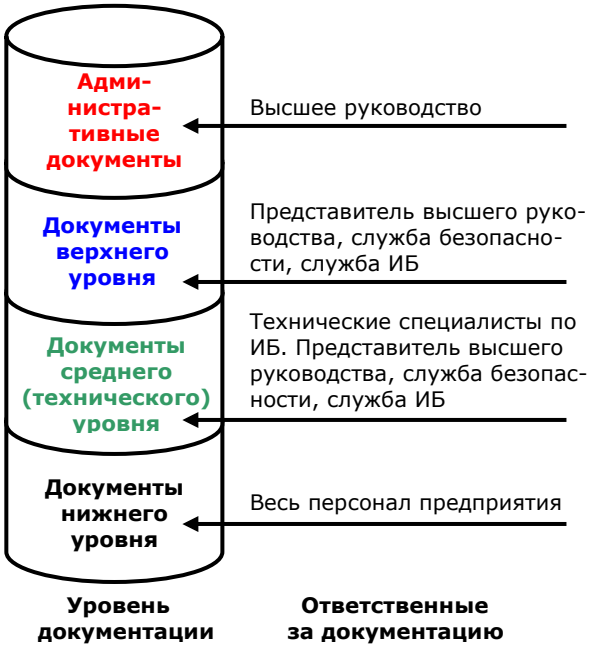

Рисунок 1. Структура документации СМИБ

Документы верхнего уровня позволяют построить на предприятии основу СМИБ – систему управления рисками, а также реализовать основные управленческие процессы. Любые процессы управления базируются на документации. Управленческие процессы СМИБ не являются исключением. Документы верхнего уровня разрабатываются службой информационной безопасности и являются основой для ее работы.

Документы среднего (технического) уровня помогают реализовать конкретные действия по защите всех важных информационных активов от угроз различного происхождения. Это наиболее объемная часть документации. Именно в этом блоке происходит описание конкретных операций каждого участника СМИБ. В разработке технической документации принимают участие специалисты по ИБ, специалисты отдела кадров, управления ИТ, службы физической защиты, юридический отдел и др. На этом уровне документации решаются вопросы распределения ответственности по каждой операции, устанавливаются сроки, готовятся шаблоны договоров (соглашений) для работы с внутренними и внешними сторонами. Основными пользователями данной группы документов являются руководители подразделений, системные администраторы, ответственные за обеспечение информационной безопасности конкретных активов.

Документы нижнего уровня предназначены для конечных пользователей. Они являются эффективным инструментом для сокращения количества угроз, связанных с человеческим фактором. Как правило документы нижнего уровня являются выжимками из документов технического уровня. При их разработке следует четко понимать для кого они рассчитаны. Стоит отказаться от сложных формулировок и незнакомых терминов.

Таким образом, условное деление всей документации СМИБ на четыре группы позволит заниматься разработкой постепенно, переходя от верхнего уровня до нижнего.

РАЗРАБОТКА ДОКУМЕНТАЦИИ

Первый этап – определение перечня

Для определения перечня необходимой документации может использоваться один из трех подходов.

- Первый подход – на основе требований стандарта ISO/IEC 27001. Алгоритм подготовки перечня базируется на проработке требований стандарта. В первом столбце таблицы перечисляются все требования стандарта. Каждое требование стандарта рассматривается с точки зрения необходимости разработки документов или записей. Во втором столбце таблицы записываются наименования документов и записей, необходимых предприятию для реализации этих требований. После заполнения всех строк во втором столбе таблице будет сформирован перечень документации СМИБ. Этот подход можно использовать при любом алгоритме внедрения СМИБ.
- Второй подход – на основе плана по обработке рисков. Для создания перечня предварительно нужно выполнить трудоемкую цепочку действий: идентифицировать активы, определить угрозы и уязвимости, оценить ущерб и вероятность каждого риска, просчитать риски, ранжировать риски. После этого напротив каждого риска необходимо прописать требуемые меры по обработке риска. Среди этих мер будут встречаться документы и записи. Таким образом сформируется перечень документов СМИБ с учетом уровня рисков. Т.е. для рисков с высоким значением возможно потребуется создать отдельные документы, для нескольких малых рисков можно применить единый краткий документ. Этот подход позволяет создать более точный перечень необходимой документации СМИБ.
- Третий подход – на основе предложенного перечня. Предложенный ниже перечень документации можно взять за основу собственного. Необходимо проработать его с точки зрения полноты и избыточности. Этот подход является самым быстрым, но требует от разработчика хорошего знания стандарта, знания проблем в области ИБ собственного предприятия и понимания сути каждого предложенного документа.

Примечание: «З.» обозначает «Запись» или «Журнал»

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ СМИБ

	Административные документы СМИБ
1.	Оргструктура предприятия
2.	Приказ о назначении представителя ВР по СМИБ
3.	Положение о службе безопасности
4.	Положение о службе информационной безопасности
5.	Должностная инструкция представителя ВР по СМИБ
6.	Должностная инструкция системного администратора
7.	Приказ ВР о внедрении и поддержке СМИБ

	Документы верхнего уровня
1.	Область действия СМИБ
2.	Политика СМИБ внешняя
3.	Политика СМИБ внутренняя
4.	Цели СМИБ по процессам
5.	З. Анализ достижения целей
6.	Оргструктура СМИБ
7.	Положение о применимости направлений ИБ
Работа с рисками	
8.	Методика оценки рисков
9.	Критерии принятия рисков
10.	З. Отчет об оценке рисков
11.	З. План по обработке рисков
12.	З. Заявление ВР о принятии остаточных рисков
Работа с документами	

13. Процедура управления документацией
14. Процедура управления записями

Внутренние аудиты

15. Процедура проведения внутренних аудитов
16. З. Группа внутреннего аудита
17. З. Программа внутренних аудитов на год
18. З. План аудита
19. З. Отчет об аудите
20. З. Протокол несоответствия
21. З. План корректирующих и предупреждающих действий

Корректирующие и предупреждающие действия

22. Процедура управления корректирующими и предупреждающими действиями

Анализ со стороны ВР

З. Анализ СМИБ со стороны ВР

Документы среднего (технического) уровня

А6. Общая организация ИБ

Оргструктура СМИБ
З. Журналы регистрации новостей в области ИБ
З. Договор с третьим лицом по работе с ИА
З. Журнал регистрации действий с ИА третьих лиц

А7. Управление Активами

З. Реестр активов
- классификация ИА
- ответственность за ИА
- маркировка ИА
- оценка ИА

А8. Управление персоналом

Процедура управления персоналом
Критерии приема персонала
Программа обучения персонала

Прием на работу

ПРАВИЛА ИБ для конкретной должности
Соглашение о соблюдении правил ИБ
Соглашение о конфиденциальности

Во время работы

Записи об обучении (аттестации)

При переходе на другую должность или увольнении

ПРАВИЛА ИБ для конкретной должности
Соглашение о соблюдении правил ИБ
Соглашение о конфиденциальности

А9. Физическая безопасность

Процедура физической защиты предприятия
Схема периметра безопасности
Схема расположения зданий, помещений
Схема расположения средств обработки информации
Паспорта зон особой безопасности

А10. Управление компьютерами и сетями

Правила обслуживания средств обработки информации
Процедура управления изменениями в СОИ
Процедура антивирусной защиты
Процедура резервного копирования
Процедура сетевой защиты
Процедура работы с носителями информации
Процедура обмена информацией
Процедура управления электронной коммерцией
З. Журнал регистрации действий пользователей
З. Журналы регистрации действий администраторов
Руководства по обслуживанию СОИ

А11. Управление доступом

Физический доступ

Процедура доступа к помещениям
Процедура доступа к персоналу
Процедура доступа к бумажным архивам

Электронный и физический доступ

Процедура доступа к СОИ и ИА за пределами предприятия
Процедура доступа к электронным архивам
Процедура доступа к СОИ
Процедура доступа к ПО
Процедура доступа к ИС
Процедура доступа к ОС
Процедура доступа к сетям
Правила парольной защиты
Правила чистого стола и экрана
З. Журнал регистрации доступов
З. Анализ зарегистрированных доступов

А12. Приобретение, разработка и поддержание ИС

Процедура принятия нового СОИ, ПО, ИС, сети
Процедура разработки(доработки) ПО, ИС
Процедура управления техническими уязвимостями
Процедура криптографической защиты
Правила ввода данных в ПО, ИС, СОИ

А13. Управление инцидентами

Процедура выявления и регистрации инцидентов
З. Журнал регистрации инцидентов ИБ
З. Журнал регистрации жалоб и предложений ИБ

А14. Управление непрерывностью бизнеса

Процедура управления непрерывностью бизнеса
З. Риски серьезного прерывания бизнеса
З. Планы восстановления бизнеса
З. Записи о тестировании планов восстановления

А15. Управление соответствием требованиям

З. Перечень применимого законодательства
Документы на ПО, ИС (лицензии)
З. Перечень законодательных и контрактовых требований по наличию и хранению записей
Процедура защиты персональных данных
Перечень законодательных требований по криптозащите

Документы нижнего уровня

1. Копии внешней политики во всех помещениях
2. Копии Процедур управления документацией во всех подразделениях
3. Копии Процедуры управления записями во всех подразделениях
4. Памятка по антивирусной защите
5. Памятка по резервному копированию
6. Памятка по работе с паролями
7. Памятка при работе на ПК
8. Памятка по обмену информацией
9. Памятка по вводу информации в ИС
10. Памятка по работе с электронными документами
11. Памятка по работе с бумажными документами
12. Действия в случае нестандартной ситуации
13. Действия в случае катастрофы
14. Памятка по защите персональных данных
15. Указатели на входах в зоны особой защиты

Второй этап – подготовка правил написания документов

Стандарт ISO/IEC 27001:2005 (пункт 4.3.1) относительно документации требует:

Документация СМИБ должна включать:
a) документированную политику и цели СМИБ (см. 4.2.1b));
b) сферу функционирования СМИБ (см. 4.2.1a));
c) процедуры и средства управления для поддержки СМИБ;
d) описание методики оценки рисков (см. 4.2.1c));
e) отчет об оценке рисков (см. с 4.2.1c) до 4.2.1g));
f) план обработки рисков (см. 4.2.2b));
g) документированные процедуры, необходимые организации для обеспечения эффективного планирования, управления и контроля за ее процессами в сфере информационной безопасности и описания способа измерения результативности средств управления (см. 4.2.3c));
h) записи, предусмотренные данным Международным стандартом (см. 4.3.3);
i) декларацию соответствия (применимости).

Среди перечисленных требований есть конкретные и четкие: политика СМИБ, методика оценки рисков и др. Эти требования достаточно легко реализовать разработав данные документы. Гораздо сложнее работать с общими «неконкретными» требованиями, такими как: необходимые процедуры и записи, требуемые стандартом. Реализовать их возможно только после изучения всех требований стандарта и написания плана по реализации этих требований.

Использование существующих правил

Хорошей практикой считается использование существующих на предприятии документов и записей. Возможно более легким вариантом будет доработка существующих процедур или журналов с учетом требований ISO/IEC 27001. Нужно помнить что документы создаются для сотрудников предприятия, которые уже привыкли к определенным формам. Создание кардинально новых документов потребует дополнительного времени для обучения сотрудников и времени для привыкания к ним. Поэтому не стоит прибегать к введению новых документов только из-за того, что вы увидели более красивый шаблон у вашего конкурента.

Правила написания процедур

Для написания процедур (политик) необходимо решить два вопроса.

Первый - разработать правила по написанию процедур. Этот документ регламентирует все важные моменты, которые должен помнить разработчик процедур. Эти правила часто называют «стандартом на стандарт».

Второй – разработать шаблон для написания любой процедуры. Этот шаблон может выглядеть следующим образом:

0. Титульный лист (наименование процедуры, дата выпуска, данные об утверждении)
1. Цель (для чего нужна процедура)
2. Область действия (для каких подразделений)
3. Термины, определения, сокращения
4. Ссылки на другие процедуры и стандарты
5. Операции процесса (четкий порядок действий, ответственные, время на выполнения каждого действия)
6. Приложения (бланки журналов, схемы)
7. Лист рассылки (кому направлен документ)
8. Лист регистрации изменений

Третий этап. Разработка документов

Общие рекомендации при разработке документации

При разработке документации СМИБ рекомендую пользоваться 10-ю золотыми правилами:

1. По возможности отказаться от объемного и часто присутствующего на предприятиях документа «лирического» содержания - концепции ИБ. Лучше все кратко изложить в политике ИБ (1 стр.) и целях ИБ (1-2 стр).
2. Все документы должны быть выполнены в едином стиле. Для этого необходимо разработать правила написания документов.
3. Документы должны быть простыми для понимания и максимально краткими. В этом поможет использование блок-схем и употребление коротких фраз.
4. Визуализируйте правила по ИБ. Используйте блок-схемы, таблицы и рисунки.
5. По возможности интегрируйте (вставляйте) документы СМИБ с существующими документами, работающими в рамках других систем менеджмента (качества, ИТ, общей безопасности).
6. Разрабатывайте правила для пользователя в отношении ИБ в рамках одного документа.
7. По возможности объединяйте правила для пользователя с должностными инструкциями.
8. Выбирайте оптимальный вид носителя документов СМИБ между электронным и бумажным. Электронные документы далеко не всегда имеют преимущества над бумажными.
9. Постоянно пересматривайте перечень документации с целью его сокращения и уменьшения объемов конкретных документов.
10. Создавайте журналы для ведения записей только там, где требует стандарт и существующие правила бизнеса. По возможности автоматизируйте процесс ведения записей.

Источники шаблонов документов

Зачем изобретать велосипед? Прежде, чем приступать к самостоятельной разработке документации полезно увидеть уже существующие документы и использовать их в качестве шаблонов для собственных политик, процедур и инструкций. В результате экономится драгоценное время и другие ресурсы предприятия.

Шаблоны документов СМИБ в настоящее время можно получить следующими способами:

1. Участие на практических учебных курсах по стандарту ISO/IEC 27001. Многие учебные организации в рамках практических курсов выдают шаблоны документов в печатном или электронном виде. Если ваша основная цель – шаблоны, необходимо предварительно уточнить этот вопрос у организаторов учебного курса.
2. Шаблоны документов можно получить обратившись к знакомому коллеге. Для этого необходимо обратиться к такому человеку, у которого уже ведется или завершена работа по внедрению СМИБ.
3. Самый быстрый, но дорогой способ овладения шаблонами – приобрести их у конкретной компании. Русский Интернет предлагает широкий спектр компаний, предлагающих приобрести отдельные процедуры или объемный пакет документов.
4. Самый дешевый способ стать обладателем шаблонов – англоязычный Интернет. Опыт европейских стран и США в разработке документов СМИБ достаточно большой. Многие политики и процедуры выкладываются на Интернет-сайтах в открытом доступе. Рекомендую посетить следующие сайты:

   - *http://www.dir.state.tx.us/security/policies/templates.htm*
   - *http://csrc.nist.gov/groups/SMA/fasp/archive.html*
   - *http://www.sans.org/resources/policies/*
   - *http://www.brookes.ac.uk/infosec/*
   - *http://www.vita.virginia.gov/library/default.aspx?id=537*
   - *http://www.it.ufl.edu/policies/security/*
   - *http://www.yourwindow.to/security-policies/*
   - *http://www.hp.com/sbso/productivity/howto/security/*
   - *http://www.wustl.edu/policies/*
   - *http://www.dhs.state.or.us/policy/admin/infosecuritylist.htm*
   - *http://www.tcd.ie/ITSecurity/policies/infosec.php*
   - *http://www.fs.uiuc.edu:1503/fsindex.html?col=cam&qc=cam*
   - *http://campus.leeds.ac.uk/isms/*
   - *http://it.ouhsc.edu/policies/*
   - *http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014f945.shtml*
   - *http://www.sans.org/reading_room/whitepapers/policy issues/*
   - *http://www.windowsecurity.com/pages/security-policy.pdf*

Примеры документов различных уровней

Пример документа административного уровня. Образец приказа о внедрении СМИБ и назначении ответственного

Приказ № _____
г. Донецк __.__.____г.

О разработке и внедрении СМИБ

С целью повышения уровня информационной безопасности предприятия и улучшения взаимодействия между отдельными структурными подразделениями предприятия

ПРИКАЗЫВАЮ:

1. Разработать, внедрить и сертифицировать систему менеджмента информационной безопасности в соответствии с требованиями международного стандарта ИСО/МЭК 27001:2005.
2. Назначить уполномоченным по информационной безопасности заместителя директора (ФИО) с возложением на него следующих дополнительных функций:
   - организация и координация работ по разработке, внедрению и поддержанию в рабочем состоянии процедур и процессов системы менеджмента информационной безопасности (СМИБ),
   - периодическое представление отчетов о функционировании СМИБ и предложений об улучшении ее функционирования,
   - поддержание связи с внешними организациями по вопросам, относящимся к СМИБ,
   - разъяснение персоналу внутренних требований по информационной безопасности.
3. Установить доплату заместителю директора (ФИО) в размере _____ грн за выполнение дополнительных обязанностей, связанных с разработкой СМИБ и ее функционированием.
4. Разработку и внедрение СМИБ завершить в _____ 200_ года, предъявить ее к сертификации в признанной на мировом рынке системе сертификации ТЮФ СЕРТ.
5. Контроль выполнения приказа оставляю за собой.

Директор ОАО «Предприятие» Подпись

Пример документа высшего уровня. Образец политики СМИБ

ПОЛИТИКА

в области информационной безопасности
ОАО «Предприятие»
__._____.2007

- Наша компания берет обязательства по внедрению, поддержке и улучшению системы управления информационной безопасности в соответствии с требованиями международного стандарта ISO/IEC 27001.
- Наш персонал соблюдает законодательные требования и внутренние требования к обеспечению информационной безопасности.
- Информация о наших клиентах хранится в условиях строгой конфиденциальности.

Генеральный директор _____
(Подпись)

Пример документа технического уровня. Образец процедуры

Титульный лист

ОАО "Предприятие"
СТП_ИБ_002_07
Процедура
"Резервное копирование информации"
Разработал: Ф.И.О. Согласовал: Ф.И.О. Утвердил: Ф.И.О.
г. Донецк, 2009

Цель. Установить процесс резервного копирования информации в ООО "Предприятие" в соответствии с требованиями ISO/IEC 27001.

Область действия. Документ предназначен для системного администратора управления ИТ, пользователей подразделений ОМ, ОС, ОПРП.

Сокращения

ИБ – информационная безопасность
ЭД – электронный документ

Ссылки

ЭД. ИБ_источники_РК на ПК "Serv03", "D:\ISMS\"
сетевой диск «Rezerv » на ПК "Serv03"

Операции процесса

1. Ответственный за процесс резервного копирования – офицер по ИБ
2. Резервное копирование осуществляет системный администратор.
3. Процесс резервного копирования осуществляется путем копирования электронных документов из папок-источников в папки-приемники.
4. Перечень источников резервного копирования обозначен в электронном документе ИБ_источники_РК, который находится на ПК "Serv03" по адресу "D:\ISMS\».
5. Общим приемником резервного копирования является сетевой диск «Rezerv », который находится на ПК "Serv03".
6. Резервное копирование осуществляется 1 раз в неделю по пятницам с 17:00 до 18:00.
7. При возникновении проблем при резервном копировании системный администратор немедленно сообщает о них офицеру по ИБ.
8. Офицер по ИБ контролирует процесс резервного копирования путем внезапной проверки журнала резервного копирования (приведен в приложении) и сравнения случайно выбранной папки-источника с папкой-приемником. Проверка осуществляется не реже, чем 1 раз в 2 месяца.

Приложение. Журнал резервного копирования

№	Источник	Приемник	Дата	Подпись

Пример документа нижнего уровня. Образец правил для пользователя

ПАМЯТКА ПО ВЫБОРУ ПАРОЛЯ

Хороший пароль:	**Плохой пароль:**
• Длина 6-10 символов • Содержит и заглавные и прописные латинские буквы • Содержит цифры • Никак не связан с владельцем • Его можно запомнить	• Короткий, меньше 6 символов • Содержит русские буквы • Не содержит цифр • Каким-либо образом связан с владельцем • Его невозможно забыть