Dr.WEB®
www.drweb.com

Создание надежной системы безопасности, сбалансированной по критерию безопасность-стоимость

Защити созданное

Формулировка задач, стоящих перед бизнесом в области безопасности

Обеспечение надежной защиты бизнеса при условии минимизации затрат на обеспечение безопасности, включая минимизацию затрат и усилий на поддержание системы безопасности в актуальном состоянии.

Формулировка задач, стоящих перед бизнесом в области безопасности

- Минимальное количество используемых продуктов и систем при оптимальном уровне защиты
- Выполнение требований законодательства – построение системы защиты в соответствии с требованиями Федерального закона № 152-ФЗ и другими стандартами
- Централизованное управление всеми компонентами защиты

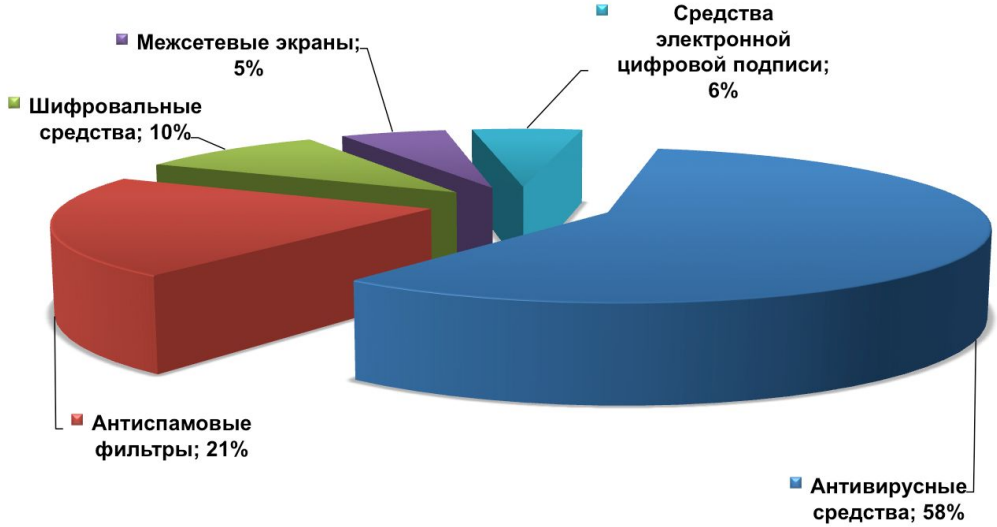
Формулировка задач, стоящих перед бизнесом в области безопасности

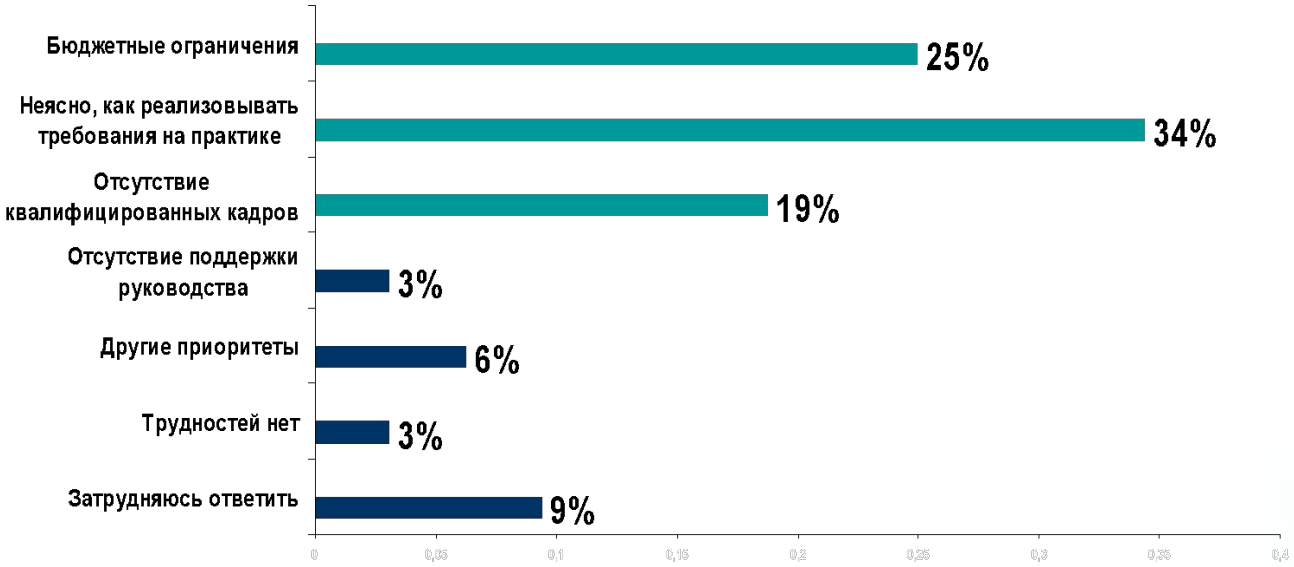
Все вышесказанное обеспечивает:

- минимизацию затрат на приобретение и сопровождение продуктов,
- минимизацию требуемого уровня квалификации обслуживающего персонала и сокращение его количества,
- высвобождение ресурсов для других задач.

Dr.WEB®
www.drweb.com

Текущая ситуация в области безопасности





Защити созданное

www.drweb.com

Dr.WEB®
www.drweb.com

Текущая ситуация в области безопасности

Федеральный закон № 152-ФЗ — шанс для бизнеса
или груз на шее?

Цель проведения аудита информационной безопасности

Получить независимую и объективную оценку текущего уровня информационной безопасности для:

- систематизации и упорядочивания существующих мер защиты информации;
- обоснования инвестиций в информационную безопасность;
- подготовки ТЗ на разработку и создание системы безопасности, в том числе для приведения системы информационной безопасности в соответствие требованиям международных или российских стандартов и требований;
- оценки уровня эффективности имеющейся системы безопасности.

Аудит СУИБ по стандарту ISO 27001

1. Политика безопасности
2. Организационные меры безопасности
3. Учет и категорирование информационных ресурсов
4. Кадровые аспекты ИБ
5. Физическая защита информационных ресурсов
6. Управление технологическим процессом
7. Управление доступом
8. Закупка, разработка и сопровождение компонентов ИС
9. Управление инцидентами в области информационной безопасности
10. Обеспечение непрерывности работы и восстановления
11. Соответствие нормативным и руководящим документам

Перечень типов объектов защиты

- Линии связи и сети передачи данных
- Сетевые программные и аппаратные средства, в том числе сетевые серверы
- Файлы данных, базы данных, хранилища данных
- Носители информации, в том числе бумажные носители
- Прикладные и общесистемные программные средства
- Программно-технические компоненты автоматизированных систем
- Помещения, здания, сооружения
- Платежные и информационные технологические процессы
- Бизнес-процессы

Конечные потребители результатов аудита

Внутренние пользователи:

- Руководство компании
- Служба информационной безопасности
- Служба автоматизации предприятия
- Служба внутреннего контроля/аудита

Внешние пользователи:

- Акционеры компании
- Регулирующие органы
- Страховые компании
- Клиенты компании

Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 Обеспечение ИБ организаций банковской системы РФ. Общие положения

Все процедуры должны быть задокументированы.

Должны существовать процедуры действий на все возможные инциденты.

Все действия и инциденты должны отслеживаться и протоколироваться.

Все документы должны быть утверждены.

Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 Обеспечение ИБ организаций банковской системы РФ. Общие положения

5.24. Для реализации и поддержания ИБ в организации БС РФ необходима реализация четырех групп процессов:

- планирование СОИБ организации БС РФ («планирование»);
- реализация СОИБ организации БС РФ («реализация»);
- мониторинг и анализ СОИБ организации БС РФ («проверка»);
- поддержка и улучшение СОИБ организации БС РФ («совершенствование»).

Стандарт ISO/IEC 27001:2005 Требования к системе менеджмента информационной безопасности

Организация должна управлять активами:

- Должна проводиться инвентаризация активов в соответствии с разработанными принципами классификации активов по их значимости, правовым требованиям, важности и критичности для организации.
- Должны быть определены ответственные за активы.

Стандарт ISO/IEC 27001. Обязательное приложение А. Требование А.7

Стандарт ISO/IEC 27001:2005 Требования к системе менеджмента информационной безопасности

Организация должна выявлять угрозы для существующих и новых бизнес-процессов и идентифицировать риски:

- Идентифицировать активы.
- Идентифицировать угрозы этим активам.
- Идентифицировать уязвимости, которые могут быть использованы этими угрозами.
- Определить воздействие, которое может привести к потере конфиденциальности, целостности и доступности ресурсов.

Стандарт ISO/IEC 27001. Пункт 4.2.1 г)

Стандарт ISO/IEC 27001:2005 Требования к системе менеджмента информационной безопасности

Организация должна оценивать риски и принимать решения как на основе известных рисков, так и существующих бизнес-целей:

- Оценить ущерб бизнесу.
- Оценить вероятность возникновения нарушения.
- Оценить уровни рисков.
- Определить, является ли риск приемлемым, или требуется обработка риска с использованием критериев принятия риска.

Стандарт ISO/IEC 27001. Пункт 4.2.1 д)

Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 Обеспечение ИБ организаций банковской системы РФ. Общие положения

5.4. Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности.

Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации БС РФ.

Незлоумышленные действия собственных работников создают либо уязвимости ИБ, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности актива или параметры системы, которая этот актив поддерживает.

Стандарт ISO/IEC 27001:2005 Требования к системе менеджмента информационной безопасности. Риск-менеджмент

Вероят-ность / Ущерб	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Низкий	1	3	5	7	9
Средний	3	9	15	21	27
Высокий	5	15	25	35	45
Очень высокий	7	21	35	49	63

Пример частной модели угроз

Частная модель угроз безопасности
информационной системы персональных данных

_____
(наименование информационной системы персональных данных)

Исходная степень защищенности информационной системы персональных данных: _____

Показатель защищенности Y_1 = _____(0 – для высокой степени исходной защищенности, 5 – для средней, 10 – для низкой)

Справочно:		
Вероятность реализации Y_2 = 0 для маловероятной угрозы; 2 для низкой вероятности угрозы; 5 для средней вероятности угрозы; 10 для высокой вероятности угрозы.	Коэффициент реализуемости угрозы $Y = (Y1 + Y2)/20$.	Возможность реализации угрозы $0 < Y < 0,3$, - низкая; $0,3 < Y < 0,6$, - средняя; $0,6 < Y < 0,8$, - высокая; $Y > 0,8$, - очень высокая.

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
Угрозы преднамеренного электромагнитного воздействия на ее элементы					Экранирование зданий и помещений, технических средств.	Удаление от границы контролируемой зоны
Угрозы от утечки по техническим каналам						
Угрозы утечки акустической информации	**Мало вероятная**	**Низкая**	**Низкая**	**Неактуальная**	Виброгенераоры, генераторы шумов, звукоизоляция.	Инструкция пользователя Технологический процесс
Угрозы утечки видовой информации						
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных						Инструкция пользователя
Просмотр информации на дисплее посторонними лица, находящимися в помещении в котором ведется обработка персональных данных						Инструкция пользователя Пропускной режим

Пример методики определения актуальных угроз

По документу ФСТЭК России БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ	Внешний	Категории внутренних нарушителей							
	1	1	2	3	4	5	6	7	8
	физич. лица	без дост. к ПДн	лок.польз ПДн	уд.польз ПДн	адм.ИБ сегмента	сист. админ	АИБ	програм. сопр.ПП	ремонт ТС
иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;			как 1	как 2	как 3	как 4	как 5		
располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;									
располагать именами и вести выявление паролей зарегистрированных пользователей;									
изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.									
знает по меньшей мере одно легальное имя доступа;									
обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;									
располагает конфиденциальными данными, к которым имеет доступ.									
располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн;									
имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.									
обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;									
обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;									
имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;									
имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;									

Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 Обеспечение ИБ организаций банковской системы РФ. Общие положения

Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ организации БС РФ — разработать политику ИБ организации БС РФ и в соответствии с ней реализовать, эксплуатировать и совершенствовать СОИБ.

Стандарт ISO/IEC 27001:2005 Требования к системе менеджмента информационной безопасности. Риск-менеджмент

Согласно методике управления рисками:

1. Работаем над снижением наиболее опасных рисков

Операционная система	Системный администратор	**Вирусная атака**	Уязвимость компьютерной системы	5	5	**25**	1. Установка антивирусного ПО 2. Регулярное обновление АВ
Рабочий журнал МП-45	Руководитель информационной службы	**Нерегулярное заполнение**	Неисполнительность персонала	3	9	**27**	1. Обучение 2. Система мотивации

2. Принимаем остаточные риски

Сменное задание	Мастер …	**Сбой в компьютерной сети предприятия**	Несвоевременное техническое обслуживание	3	5	**15**	Согласно процедуре принятия рисков
		Ошибка оператора при вводе данных	Чел. фактор	3	5	**15**	Согласно процедуре принятия рисков

3. Утверждаем

Стандарт ISO/IEC 27001:2005 Требования к системе менеджмента ИБ. Работа СМИБ по требованиям ISO 27001

Пункт 5.1.c Установка ролей и ответственности

Пункт A.8.1 Приоритеты найма служащих
A.8.1.1 Роли и ответственность
A.8.1.2 Подбор и прием персонала
A.8.1.3 Условия работы

Пункт A.10.10.4 Действия системного администратора
Действия системного администратора и
системного оператора также должны записываться в журнал.

Dr.WEB®
www.drweb.com

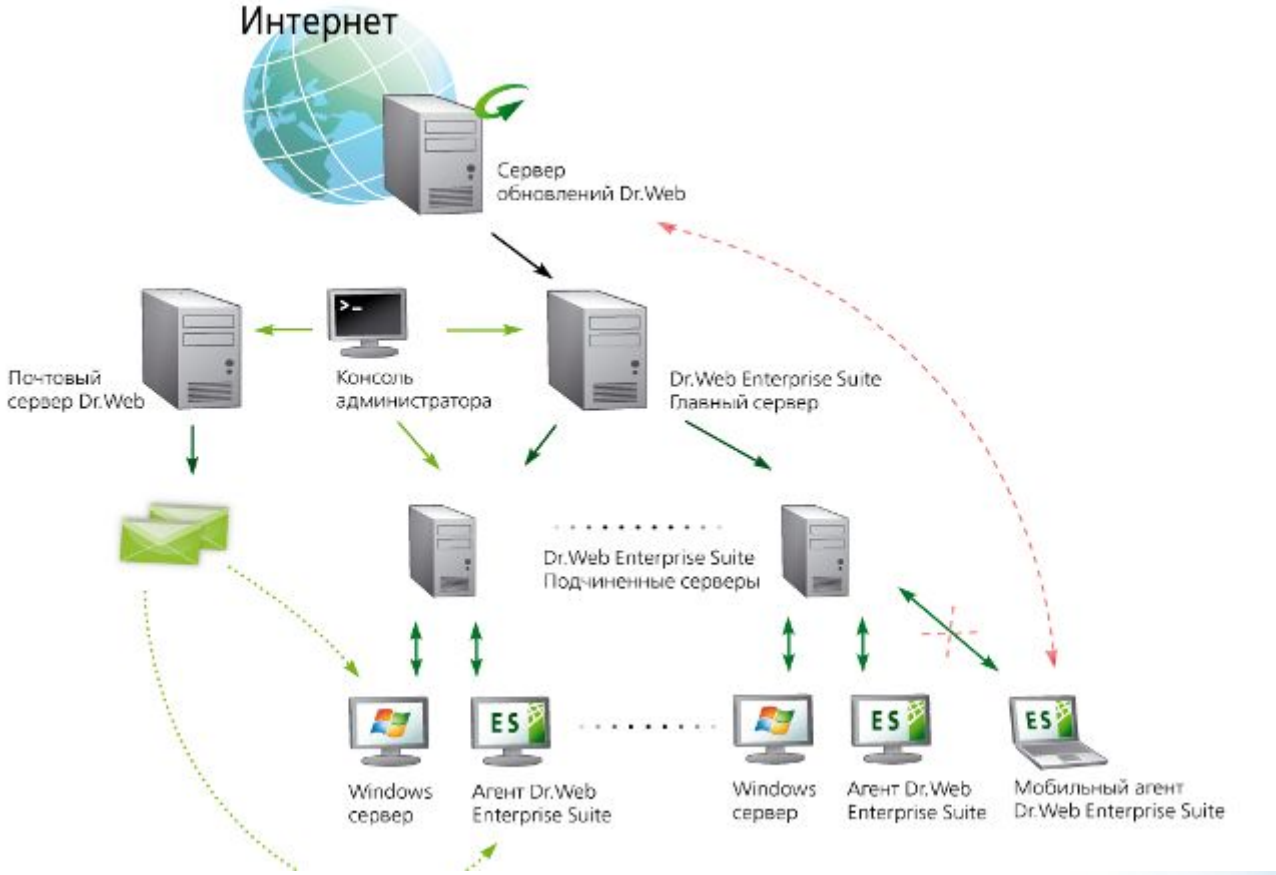
Оптимизация стоимости защиты

Закон — это повод упорядочить бизнес-процессы. Правильное определение угроз и необходимых для работы компании персональных данных позволяет сократить стоимость реализации закона в разы.

Обезличивание
Правильное определение действующих угроз
Правильный выбор ПО с исключением дублирования функций
Максимальное использование возможностей уже имеющихся в ИС средств защиты информации, возможностей ОС и прикладного ПО.
Сокращение количества АРМ, обрабатывающих ПДн.
Разделение ИС межсетевыми экранами на отдельные сегменты.
Организация терминального доступа к ИСПДн.
Исключение из ИСПДн части ПДн, хранение их на бумажных или иных носителях.

И это не все!

Пример структуры системы защиты с централизованным управлением (на примере Dr.Web Enterprise Security Suite)



Оптимизация стоимости защиты

Обезличивание ПДн — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту.

Ст. 3 Федерального закона № 152-ФЗ «О персональных данных», NIST SP800-122, Стандарт ISO 25237-2008

- Абстрагирование ПДн — превращение их в менее точные — например, путем группирования общих или непрерывных характеристик.
- Скрытие ПДн — удаление всей или части записи ПДн — ПДн не должны быть избыточными по отношению к цели.
- Внесение шума в ПДн — добавление небольшого количество посторонней информации в ПДн.
- Замена ПДн — перестановка полей одной записи ПДн теми же самыми полями другой аналогичной записи.
- Разделение ПДн на части — использование таблиц перекрестных ссылок. Например, две таблицы: одна с Ф. И. О. и идентификатором субъекта ПДн, вторая — с тем же идентификатором субъекта ПДн и остальной частью ПДн
- Использование специальных алгоритмов — например, маскирование ПДн или подмена отдельных символов другими. Идеальным вариантом является использование алгоритмов криптографического хеширования.
- Псевдонимизация — удаление ассоциации с субъектом ПДн и добавление ассоциации между набором особенностей, касающихся субъекта ПДн, и одним или более псевдонимами.

Оптимизация стоимости защиты

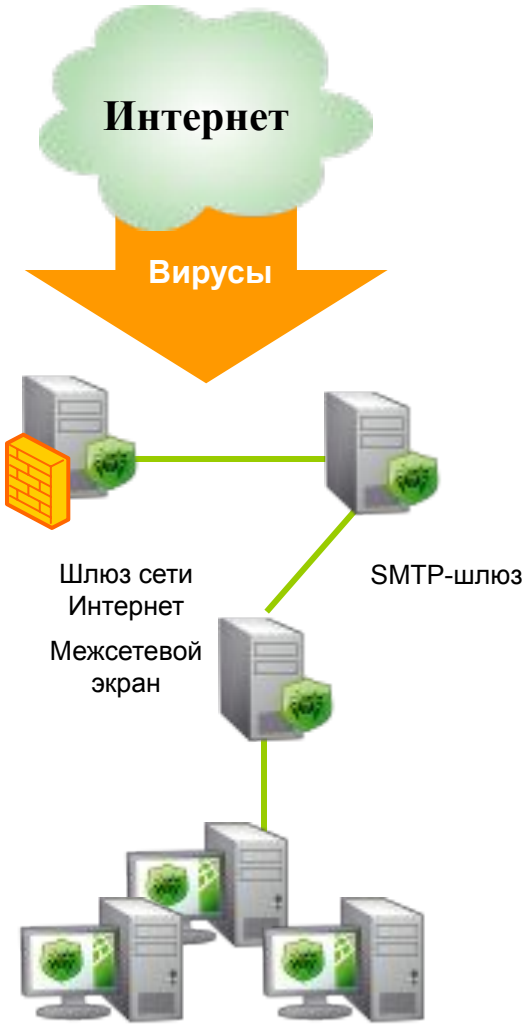
- Выделение отдельного сегмента сети для обработки ПД

Dr.WEB®
www.drweb.com

Оптимизация стоимости защиты — Требования к продуктам и системам

- Комплексная защита от вирусов и спама
- Выполнение требований законодательства — построение системы защиты в соответствии с требованиями Федерального закона № 152-ФЗ
- Централизованное управление всеми компонентами защиты
- Удобство и простота администрирования
- Богатый функционал
- Нетребовательность к ресурсам
- Совместимость приложений

Способы организации антивирусной защиты



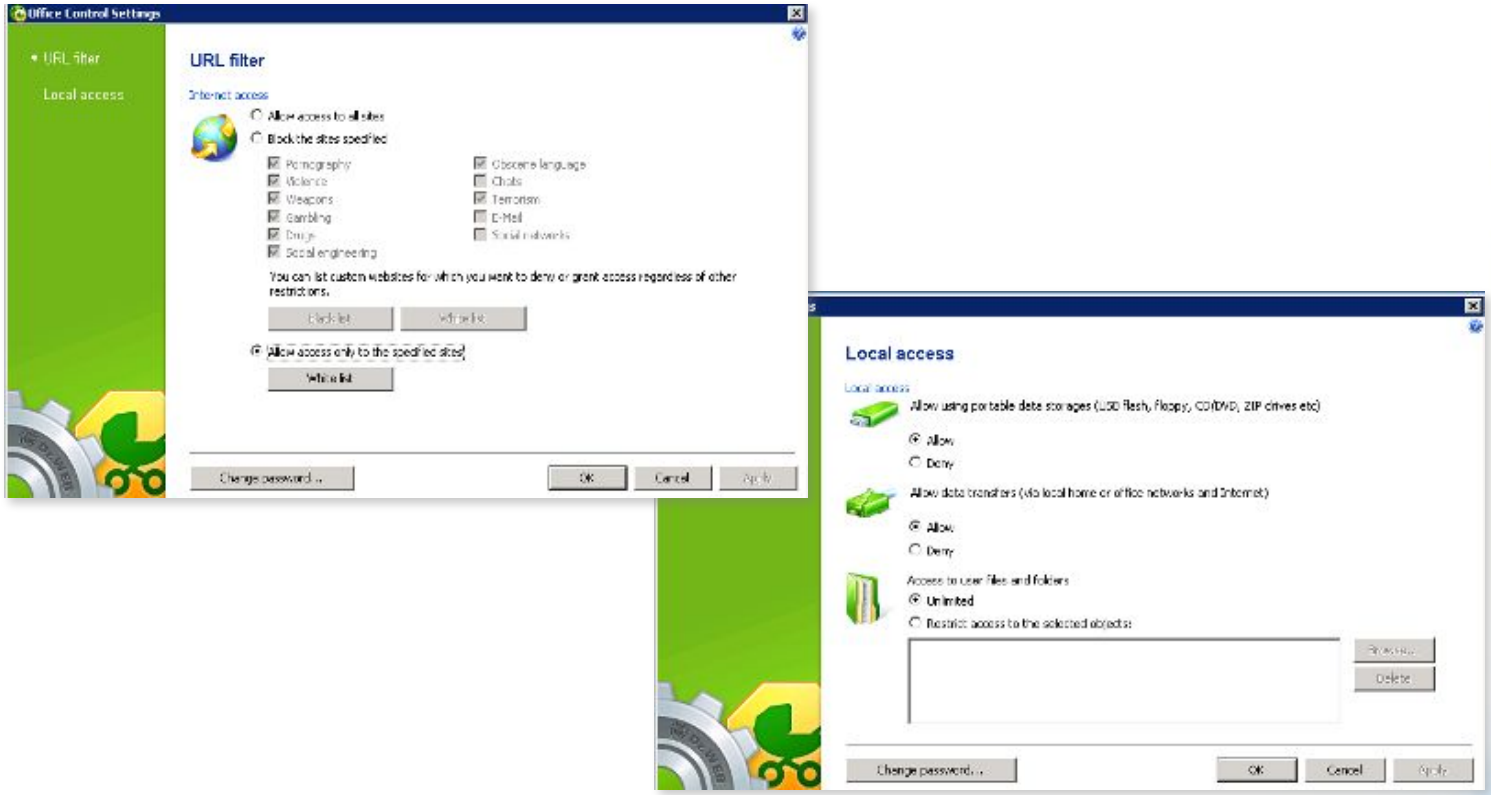
Антивирусная защита, соответствующая требованиям закона о персональных данных, должна включать защиту всех узлов локальной сети:

- рабочих станций;
- файловых и терминальных серверов;
- шлюзов сети Интернет;
- почтовых серверов.

Использование демилитаризованной зоны и средств проверки почтового трафика на уровне SMTP-шлюза повышает уровень защиты.

Dr.WEB®
www.drweb.com

Оптимизация функций защиты конфиденциальной информации



Защити созданное

www.drweb.com

Dr.WEB®
www.drweb.com

Передача функций защиты на аутсорсинг

Dr.Web Av-desk

Защити созданное

Dr.WEB®
www.drweb.com

Программно-аппаратные комплексы

- Уменьшение зависимости предприятий от уровня квалификации ИТ-персонала
- Снижение потерь рабочего времени, простоев оборудования и персонала за счет уменьшения количества вирусных инцидентов в корпоративной сети
- Повышение производительности труда путем снижения количества отвлекающих факторов
- Оптимизация расходов на интернет-трафик и контроль за деятельностью сотрудников в сети Интернет

Защити созданное

www.drweb.com

Dr.WEB®
www.drweb.com

Вопросы?

Благодарим за внимание!
Желаем вам процветания и еще больших успехов!

www.drweb.com