* разработка образа-видения *(vision)* будущей компании. На этом этапе компания строит картину того, как следует развивать бизнес, чтобы достичь стратегических целей;

* анализ существующего бизнеса — проводится исследование компании, и составляются схемы ее работы в настоящий момент;

* разработка нового бизнеса — создаются новые и (или) изменяются прежние процессы и поддерживающая их информационная система, тестируются новые процессы;

* внедрение проекта нового бизнеса.

Таким образом, невозможно определить, какой из этих двух путей решения проблем бизнеса (реинжиниринг или оптимизация) лучше, так как это определяется потребностями предприятия, его корпоративной политикой и стилем управления.

*Литература:*

1. Оптимизация и реинжиниринг/ Рябых Д.С. [Электронный ресурс]. Москва, 2006. Режим доступа: http:// www.cfin.ru.

2. Реинжиниринг: сущность и методология/ Баринов В.А. [Электронный ресурс]. Екатеринбург, 2007. Режим доступа: http:// www.ippnou.ru.

3. Реинжиниринг бизнес-процессов: Модное лекарство?/ Шейн Л. [Электронный ресурс]. Режим доступа: http://management.com.

**Кашин А.С., РГППУ**
**гр. КТ-517**
Руководитель: ст. преподаватель кафедры СИС
Н.В. Меньшикова

## МЕРЫ ОБЕСПЕЧЕНИЯ СОХРАННОСТИ ИНФОРМАЦИИ

В настоящее время, вопросы защиты информационных систем являются одним из самых важных моментов, как в период внедрения системы, так и в период ее поддержки. Все более возрастающая стоимость систем, все более значимая роль информационной системы в деятельности предприятия и оценка потенциальных убытков от несанкционированного использования или разрушения информационной системы предприятия, заставляют руководителей уделять все больше внимания вопросам защиты информационных систем.

Для того чтобы быть уверенным в защищенности информации нужно рассмотреть возможные меры защиты ценной информации.

*1. Профилактика атаки.*

Важно гарантировать недоступность информации для лиц, которым эта информация не предназначена. Для важной информации выделить отдельное место на локальном компьютере или целый сервер (если информация должна быть доступна в любое время). Место, где находится компьютер с информацией, должно быть изолировано от посторонних.

Во многих компаниях шаблоны документов находятся в общем доступе для любых сотрудников, что является явной недоработкой людей, занимающихся безопасностью. Шаблоны документов должны находиться на удаленном сервере и быть доступны в режиме «только чтение».

Важно так же уничтожать ненужную или более не использующуюся информацию, так как она может стать наводкой для хакеров. Так же важно ограничить права пользователей, ограничить набор программ на компьютере, обновление программ и компонентов системы осуществлять только с проверенного сервера.

*2. Обнаружение разведки.*

Обязательно нужно осуществлять проверку входящего и исходящего трафика на наличие подозрительных пакетов. Своевременное обнаружение таких пакетов может четко указать, когда и откуда ждать угрозы.

Нужно осуществлять мониторинг системы и проверку на целостность программного обеспечения, так как для удаленного получения данных чаще всего используются именно программные уязвимости.

Обязательна проверка журналов и логов. Нужно регулярно делать резервные копии журналов, обращать внимание на неповторяемость. Наблюдать за постоянной загрузкой системы и обращать внимание на отклонения.

*3. Фильтрация трафика.*

Чтобы обезопасить информацию от удаленных атак нужно использовать специальные программно-аппаратные комплексы для фильтрации (отсечения) входящего/исходящего трафика, называемые межсетевыми экранами.

Сетевой экран или брандмауэр (англ. Firewall) — комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, т. к. их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

На домашних компьютерах и рабочих станциях сетевые экраны используют для защиты информации от кражи, для создания эффекта невидимости компьютера в сети и подобных задач.

Важно запретить прохождение трафика на все известные порты персонального компьютера, кроме нужных портов. Для такой цели подойдет сетевой экран WIPFW – это свободно распространяемый брандмауэр для OS Windows, на основе брандмауэра IPFW, входящего в состав OS FreeBSD. Вы можете использовать и конфигурировать его так же, как и в работе с IPFW.

Для более сложных задач фильтрации, связанных с контролированием трафика системного и производственного программного обеспечения, используются более сложные версии сетевых экранов, например Agnitum Outpost Firewall (AOF). AOF – один из лучших персональных брандмауэров, представленных на рынке. Безопасность информации обеспечивается технологией Anti-Leak (технология предотвращений утечки данных). Agnitum Outpost обнаружит и предотвратит попытки вредоносных приложений передать данные с вашего компьютера в сеть.

Таким образом, рассмотрев разные меры защиты данных, можно сделать вывод, что для сохранения ценной информации необходимо в комплексе применять данные методы. Однако, даже применение всех мер не может дать стопроцентной надежности, поэтому нужно всегда следить за состоянием своей системы, чтобы не потерять информацию.

**Клипа О.В., РГППУ**
**гр. ИО-513**
Руководитель: ст. преподаватель кафедры СИС
С.В. Ченушкина

## ИСПОЛЬЗОВАНИЕ МУЛЬТИМЕДИЙНЫХ ЭНЦИКЛОПЕДИЙ НА УРОКАХ ИСТОРИИ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

За последние годы ситуация в российском образовании сильно изменилась благодаря государственным программам по информатизации, внедрению информационно-коммуникационных технологий в педагогическую практику. Уже очень многие школы подключены к Интернету и оборудованы разнообразной компьютерной техникой. Важная задача — позаботиться о том, чтобы эти новые возможности послужили во