ПАСПОРТ

Безопасность образовательного учреждения

Автор А. Баданов (badanov1@yandex.ru)

План изложения материала

1. Общее представление о сети и уровнях защиты в организации
2. Обучение персонала (серии семинаров, инструктирование)
3. Меры принимаемые в организации
4. Как вписывается в общие принципы информационной безопасности
5. ИБ на курсах повышения квалификации всех направлений (итоги анкетирования)
6. Оснащение личных компьютеров ПО и рекомендации для сотрудников организации
7. финал (ссылка)

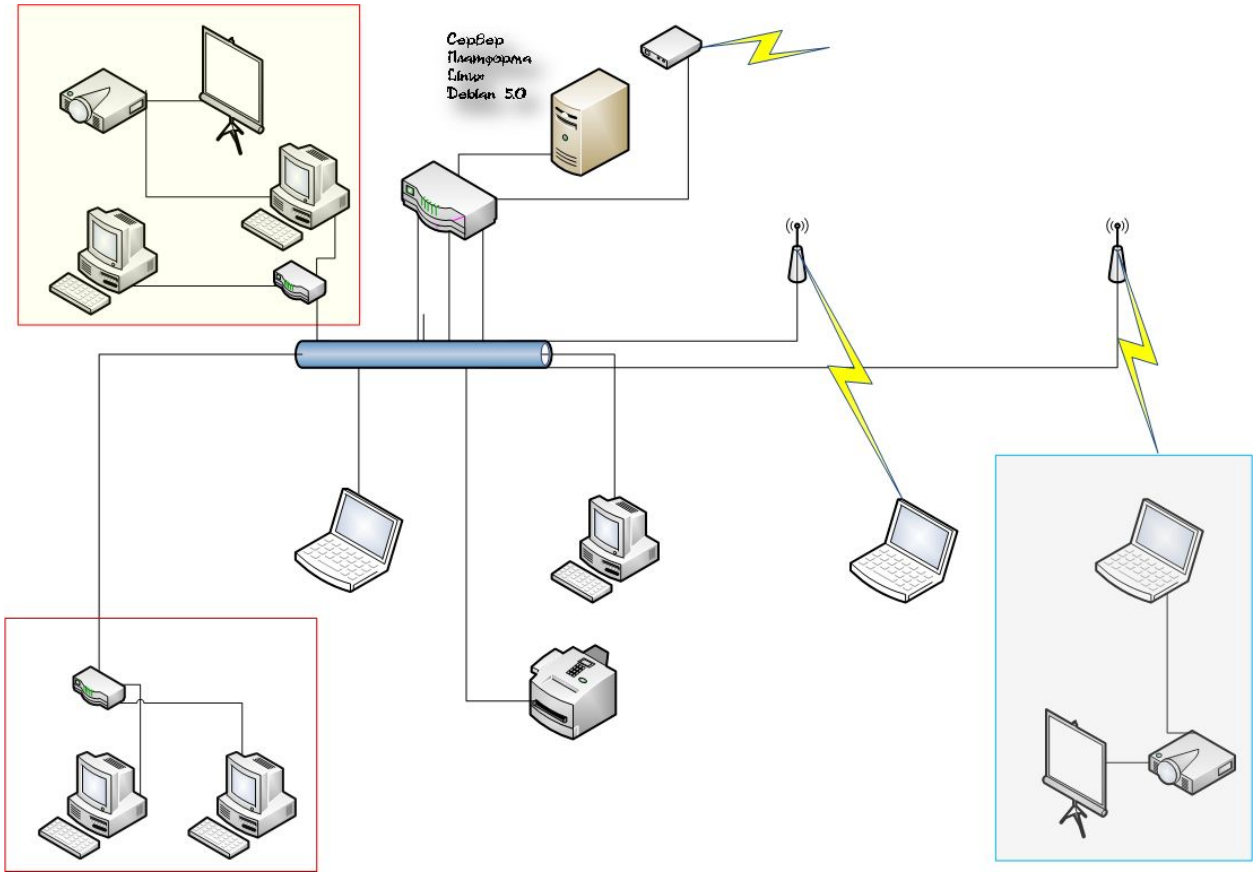

Схема 1. Общее представление об организации информационной среды организации.

Краткая информация:

Локальная сеть организации состоит из серверной и клиентских частей. Клиентская часть организована на базе операционных систем Windows 2000, XP и Vista . И OS Linux 15 рабочих станций. В системе включено разграничение прав пользователей на основе отдельных учётных записей для каждого компьютера. Для обеспечения дополнительной безопасности от вредоносных программ и проникновения из вне в клиентских системах отключены избыточные функции и службы, что в целом не ограничивает пользователей в стандартном функционале. Так же установлено современное антивирусное программное обеспечение, базы которого обновляются автоматически через интернет.

Серверная часть организована на базе ОС Linux Debian 5.0. На основе серверной части построена единая система доступа пользователей в глобальную сеть, а так же реализованы функции защиты от внешних угроз. Надёжная защита организована фаерволом Iptables, ограничивающим доступ к локальной сети из вне, а так же прокси-сервером Squid, ограничивающими посещаемый пользователями интернет-контент. Таким образом, Squid ограничивает пользователей, для предотвращения проникновения вредоносного и шпионского ПО на компьютер пользователей с тех сайтов, вероятность наличия такого ПО на которых очень высока.

В локальной сети создано несколько подсетей.

Зона WiFi- вся территория организации, Существует Файл-сервер с распределенными по различным группам пользователей сетевым ресурсам и дискам

В практической деятельности широко используется свободнораспространяемое ПО

2. Благодаря активной работе по организации защищенной информационной среды удалось добиться некоторых результатов.

Началась работа с тотальной ревизии существующей структуры и пересмотра порядка работы с информацией. Значительное внимание было уделено человеческому фактору. Регулярно проводятся тематические семинары, обучение, инструктирование сотрудников организации. Введены в действие жесткие инструкции, организованы безопасные рабочие места, введены ограничения (контент фильтрация, трафик, различный уровень контроля за порядком использования как информации, так и носителей информации). Первоначально это вызвало некое нежелание и недисциплинированность со стороны сотрудников, но в кратчайшее время плюсы от выполнения правил и инструкций и удобство от работы с организованной информационной средой сыграли решающую роль в принятии и выполнении этих правил. Помимо неких ограничений сотрудники получили ряд дополнительных технологических решений (внутренняя конференц связь, файлообменные сети, технологии для цифрового общения, интернет пришел ко всем без ограничений).

Регулярно знакомим сотрудников с новинками, особенностями использования различных программ, технологий. Проводим обучение по заявкам подразделений. Регулярно обобщается и доводится до сведения сотрудников организации интересная информация. Активно используем работу в сетевых профессиональных сообществах. Технические специалисты немедленно реагируют на проблемы, которые могут возникать в информационно-технически насыщенной среде.
Вирусы- в основном «приходящие гости» с носителей информации «курсантов», студентов. Все сотрудники четко для себя уяснили, что для информационной безопасности нет ничего лучше профилактики и предупреждения возможных угроз.

3. Меры предпринимаемые в организации для успешной работы в информационно-защищенной среде.

- Персонифицированный доступ к информации. Распределение ролей пользователей информации и персональная ответственность за информационную безопасность и работу с персонифицированными данными
- Организация не пересекающихся технических сетевых решений.
- Регулярное обновление Операционных систем
- Наличие на всех рабочих станциях антивирусов с обновляющимися базами
- При работе в сети Интернет- Контентная фильтрация
- Работа фейервола
- Использование альтернативного браузера с настроенными компонентами (дополнениями) по безопасности.
- Использование на наиболее сложно контролируемых (там, где за одной рабочей станцией может работать множество пользователей и посторонних лиц) рабочих станциях операционных систем под управлением Linux
- Автозапуск и автозагрузка отключена на всех рабочих станциях организации
- Важные данные регулярно архивируются (в ручном или автоматизированном режиме)
- Осуществляется ряд инструктивных мер по организации тотального входного контроля за любыми носителями информации (жесткое правило: прежде чем запускать файл, флешку на исполнение- проверь её)
- Постоянное информирование и обучение сотрудников организации

4. Как же все это вписывается в общие принципы организации информационной безопасности?

В основе организации защищенного информационного пространства лежит следующее:

- Личная дисциплина участников образовательного процесса
- Наличие подготовленного специалиста в организации
- Наличие площадки для общения специалистов
- Использование современных технических и технологических решений

Все мы знаем о существовании множества правил, которые нам прививаются с детства: «мойте руки перед едой», «не разговаривай с незнакомцем на улице» и т.д. Но всегда ли мы следуем этим правилам. К сожалению не всегда и при этом у нас находятся какие то оправдания-типа срочно нужно, скорее, обойдется и т.д. Уже давно назрела необходимость возвести правила информационной безопасности в ранг очень жестких правил . Потому что от не соблюдения этих правил может пострадать не только тот, кто нарушает их, а все общество (сообщество). Хотя, как и в любом обществе, всегда будут находиться «неряхи» и просто безответственные люди. Поэтому решение проблем информационной безопасности возможно только комплексно и всеми.

5. ИБ на курсах повышения квалификации всех направлений. Выборка итогов анкетирования работников системы образования.

Ежедневно и 2-3 раза в неделю пользуются компьютером 67% и 23% респондентов (90%). В профессиональных целях -57%

Ежедневно и 2-3 раза в неделю пользуются Интернетом 49% и 29% соответственно (почти 80%). Около 40% имеют дома компьютер и подключение к сети Интернет. Т.е. Большинство используют технику и выход в Интернет на своих рабочих местах. Почти все использующие Интернет педагоги являются участниками различных социальных сетей. И не всегда эти социальные сети профессинальноориентированные.

Вот некоторые вопросы и ответы по вопросам безопасности.

На рабочем (домашнем) компьютере у вас имеются вирусы?

Ответы	График	%
Да		33.33
Нет		61.81
Не знаю		4.86
У меня нет антивируса		0
	Всего ответов:	
	Неответивших:	

Кто решает проблемы потери информации и информационную безопасность от внедрения вирусов?

Ответы	График	%
Самостоятельно		31.94
Коллеги по работе		6.25
Домашние специалисты		15.28
Привлеченные специалисты		30.56
Специалист образовательного учреждения		15.97
Никто		0

Около 40% знают что на компьютере с которым он работает явно имеются вирусы. А сколько их неявно присутствует? И свыше 30 процентов пользователей вынуждены рассчитывать только на помощь сторонних специалистов.

Проблемы защиты от вирусов по вашему мнению должны решать....

Ответы	График	%
Каждый самостоятельно		44.44
Специалисты		54.17
Нет ответа		1.39
	Всего ответов:	
	Неответивших:	

Ответственность за антивирусную защиту должны нести

Ответы	График	%
Пользователи ПК		56.25
Руководитель ОУ		4.17
Специалист ОУ		11.11
Все		20.83
Авторы вируса		7.64
Нет ответа		0

Почти 60 % считают, что ответственность за антивирусную защиту должны нести сами пользователи. И почти пополам проблемы защиты от вирусов должны решать либо сами пользователи, либо специалисты.

Есть ли необходимость регулярная организация курсов, семинаров по вопросам безопасности?

Ответы	График	%
В очной форме в ОУ		50.69
В очной форме в районе		23.61
В очной форме в Республике		4.17
В дистанционной форме		11.81
Нет необходимости		2.78
Это проблема руководителя ОУ		0.69
Это личные проблемы каждого из пользователей		5.56
Нет ответа		0.69

Какие курсы должны иметь модуль по вопросам безопасности информации?

Ответы	График	%
Только на специально организованных для специалистов по вопросам безопасности		10.06
Все курсы		55.62
По информационным технологиям		26.63
Для учителей информатики		7.69
Нет необходимости		0

Всего ответов:
Неответивших:

Полученные данные позволяют сделать вывод о том вопросы информационной безопасности важны для всех и даже наиболее продвинутая часть учительства в ИТ также осознает, что организация защищенного информационного пространства дело общее и учиться этому необходимо постоянно. Очень важно иметь в своем образовательном учреждении специалиста, тьютора (возможно из числа учителей, старшеклассников) который поможет организовать эту деятельность, обучение в ОУ. Предлагается активнее привлекать учреждения повышения квалификации.

В организации разработаны специальные модули по вопросам информационной безопасности, которые используются в системе повышения квалификации. Большую поддержку оказало сотрудничество с Академией повышения квалификации и профессиональной переподготовки.

6. Оснащение личных компьютеров ПО и рекомендации для сотрудников организации

Для сотрудников организации, слушателей курсов подготовлены наборы программного обеспечения, которое свободно распространяется и которое можно использовать как в личных целях, так и на работе. Подготовлены видеоуроки, подробные иллюстрированные инструкции для самых начинающих. Ведь мало организовать безопасное информационное пространство в организации, вирусы и угрозы могут прийти и с домашних компьютеров, компьютеров партнерских организаций и т.д. Есть необходимость ввести термин в понятие

информационная безопасность – коллективная безопасность. И каждый на своем уровне будет помогать друг другу работать в мире без угроз. Кстати Издательство Бином через своих партнеров компанию Линуксцентр (ЗАО "Мезон.РУ") активно распространяет свободнораспространяемое ПО для использования его в школе. Активную позицию занимает и компания Касперского (проекты Школа Безопасности и академия Касперского) Это интересные шаги к организации коллективной безопасности.

Ссылка.
Интерактивный плакат «Основы безопасности» с множеством ссылок, информации, пособий и проч. http://dostizenie.ucoz.ru/index/spravochnik_bezopasnost_it/0-33 . Как правило, самое интересное находится в разделе плаката «Дополнительная информация» http://dostizenie.ucoz.ru/index/dopolnitelnaja_informacija/0-34 . Предлагаю использовать в своей работе эти материалы. Удачи и всего самого доброго