Модуль 5
ТЕХНОЛОГИИ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ РАЗРУШЕНИЯ И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема 5.1
ЦЕЛИ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ. УРОВНИ И МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Целью совершения любого преступления является удовлетворение корыстных целей человека или группы людей, как то материальных, моральных, психических и так далее. Преступления в информационной сфере затрагивают различные аспекты: это и получение информации нелегальным путем (в том числе и с использованием детей), распространение в Интернете материалов порнографического типа (в том числе и детской порнографии), мошенничество в Интернете и т. д.

Основные понятия в области защиты информации от разрушения и несанкционированного доступа рассмотрим исходя из **ГОСТ Р 50922—2006.** Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации. Термины данного стандарта рекомендуется использовать в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание: собственниками информации могут быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации — деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от утечки — защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Примечание: заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации от несанкционированного воздействия — защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия — защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных не целенаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения — защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Примечание: заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Цель защиты информации: заранее намеченный результат защиты информации.

Примечание: результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации — степень соответствия результатов защиты информации цели защиты информации.

Показатель эффективности защиты информации — мера или характеристика для оценки эффективности защиты информации.

Норма эффективности защиты информации — значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.

Замысел защиты информации — основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Система защиты информации — совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Техника защиты информации — средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Объект защиты информации — информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации.

Оценка соответствия требованиям по защите информации — прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации.

Средство защиты информации — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Средство контроля эффективности защиты информации — средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации.

В связи с тем, что информация является предметом собственности (государства, коллектива, отдельного лица (субъекта)), то неизбежно возникает проблема угрозы безопасности этой информации, заключающейся в неконтролируемом ее распространении, в хищении, несанкционированном уничтожении, искажении, передаче, копировании, блокировании доступа к информации. Следовательно, возникает проблема защиты информации от утечки и несанкционированных воздействий на информацию и ее носители, а также предотвращения других форм незаконного вмешательства в информационные ресурсы и информационные системы. В связи с чем, понятие ***«Защита информации»*** становится основополагающим (ключевым) понятием и рассматривается как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Значимость защиты информации увеличивается в связи с возрастанием возможностей иностранных разведок за счет совершенствования технических средств разведки, приближения этих средств к объектам разведки (носителям информации) вследствие развертывания инспекционной деятельности, создания совместных предприятий и производств, сокращения закрытых для иностранцев зон и городов.

Определившись с терминологией защиты информации, переходим на рассмотрение уровней и мер защиты информации. Можно выделить три основных уровня защиты информации. Например, применительно к общеобразовательному учреждению они выглядят следующим образом:

- защита информации на уровне рабочего места ученика и учителя;
- защита информации на уровне компьютерного класса;
- защита информации на уровне образовательного учреждения.

Защита информации на этих различных уровнях будет иметь как общие способы, так и специальные способы, зависящие от уровня.

Одним из способов (мер) по защите информации являются программные средства защиты. В настоящее время создано большое количество операционных систем, систем управления базами данных, сетевых пакетов и пакетов прикладных программ, уже включающих в себя разнообразные средства защиты информации.

С помощью программных средств защиты решаются следующие задачи информационной безопасности:

- контроль загрузки и входа в систему с помощью персональных идентификаторов (имя, код, пароль и т. п.);
- разграничение и контроль доступа субъектов к ресурсам и компонентам системы, внешним ресурсам;
- изоляция программ процесса, выполняемого в интересах конкретного субъекта, от других субъектов (обеспечение работы каждого пользователя в индивидуальной среде);
- управление потоками конфиденциальной информации с целью предотвращения записи на носители данных несоответствующего уровня (грифа) секретности;
- защита информации от компьютерных вирусов;
- стирание остаточной конфиденциальной информации в разблокированных после выполнения запросов полях оперативной памяти компьютера;
- обеспечение целостности информации путем введения избыточности данных;
- автоматический контроль над работой пользователей системы на базе результатов протоколирования и подготовка отчетов по данным записей в системном регистрационном журнале.

Методы обеспечения защиты информации могут быть разные, но основные из них следующие:

- препятствие;
- управление доступом;
- маскировка;
- регламентация;
- принуждение и побуждение.

Тема 5.2
УСТАНОВКА ПАРОЛЕЙ НА ПК И ПАПКИ. МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

Для разграничения доступа на одном компьютере современные операционные системы позволяют разграничивать доступ к информации и другим частям операционной системы (сервисы, программы и т. д.) с помощью учетных записей с задаваемыми правами доступа. На ОС по умолчанию представлены две учетные записи: администратор (полный доступ), гость (минимальный доступ). Также существует такое понятие, как группы пользователей — это

некий набор предустановленных прав, которые можно назначать пользователям. Для того чтобы однозначно авторизовать того или иного пользователя, применяются пароли. Это может быть применимо для ограничения и контроля деятельности работы детей на домашнем компьютере.

С помощью этого же механизма также регламентируется доступ к файловой системе, в частности, к папкам. Необходимым условием работы любого компьютера в сети является установка на нем персонального межсетевого экрана с функцией анализа активности программного обеспечения. По тому же принципу, но более сложными механизмами, связанными с централизованным администрированием, реализуется разграничение прав доступа в доменной структуре учреждения, например, школы.

Самым распространенным путем утечки информации является электронная почта. В настоящее время злоумышленники активно развивают методы социального инжиниринга, которые позволяют проникнуть даже на самый защищенный пользовательский компьютер.

Социальная инженерия — технология использования человеческого фактора для взлома информационной безопасности. Именно человек является наиболее слабым звеном в системах защиты. Один из приемов использования социальной инженерии — методика введения пользователя в заблуждение путем сообщения ему важных для него данных, оказывающихся на самом деле ложными.

Пример подобной методики — фишинг. Фишинг — вид онлайнового мошенничества, целью которого является получение идентификационных данных пользователей. Для этого рассылаются электронные письма от имени популярных брендов и вставляются в них ссылки на фальшивые сайты. Оказавшись на таком сайте, пользователи рискуют сообщить информацию конфиденциального характера.

Злоумышленники рассылают письма с троянскими программами, которые были спрятаны под фотографиями. Для заманивания пользователей на сайты-ловушки текст письма составляется так, чтобы у читающего не возникло сомнения в правдивости написанного.

Основой защиты от таких атак является, как ни странно, «обучение» пользователей. Необходимо информировать пользователей об этом виде угроз.

Для борьбы с фишинг-атаками используются средства контентной фильтрации, такие, как системы контроля электронной почты, фильтры, обеспечивающие фильтрацию сообщений Ин-

тернет-пейджеров. Антивирусная фильтрация и проверка на наличие шпионских программ позволяют значительно снизить уровень воздействия фишинг-атак на сеть. Целью многих подобных атак является установка на компьютере пользователя троянцев или программ-шпионов, дающая возможность злоумышленникам получить доступ к персональным данным пользователя.

Большинство клиентских почтовых программ использует протоколы POP3 и IMAP4 для подключения к пользовательскому почтовому ящику и считывания почты и протокол SMTP — для отправки писем. Веб-доступ к почтовым ящикам осуществляется по протоколу HTTP.

Для обеспечения защиты при приеме и передаче почтовых сообщений рекомендуется использовать *протокол SSL (Secure Sockets Layer)*.

Программа Microsoft Outlook, например, для работы с почтовым сервером Exchange использует *протокол RPC,* включающий в себя встроенные механизмы обеспечения безопасности канала.

При работе с электронной почтой следует обязательно пользоваться современными антивирусными программами и, желательно, средствами защиты от нежелательной почты — *спама*.

Тема. 5.3
БЕЗОПАСНОСТЬ РАБОТЫ В ЛОКАЛЬНОЙ СЕТИ

Рассмотрим безопасность в локальной сети исходя из требований Национального стандарта согласно ГОСТу Р ИСО/МЭК 17799—2005. Для этого вводятся такие понятия, как управление сетевыми ресурсами, средства контроля сетевых ресурсов, контроль сетевого доступа, политика в отношении использования сетевых служб.

Управление сетевыми ресурсами

Цель: обеспечение безопасности информации в сетях и защиты поддерживающей инфраструктуры.

Средства контроля сетевых ресурсов

Для обеспечения требуемого уровня безопасности компьютерных сетей и его поддержки требуется комплекс средств контроля. Руководители, отвечающие за поддержку сетевых ресурсов, долж-

ны обеспечивать внедрение средств контроля безопасности данных в сетях и защиту подключенных сервисов от неавторизованного доступа. В частности, необходимо рассматривать следующие меры и средства управления информационной безопасностью:

- следует распределять ответственность за поддержание сетевых ресурсов и компьютерных операций;
- следует устанавливать процедуры и обязанности по управлению удаленным оборудованием, включая оборудование, установленное у конечных пользователей;
- если необходимо, специальные средства контроля следует внедрять для обеспечения конфиденциальности и целостности данных, проходящих по общедоступным сетям, а также для защиты подключенных систем.

Контроль сетевого доступа

Цель: защита сетевых сервисов.

Доступ как к внутренним, так и к внешним сетевым сервисам должен быть контролируемым. Это необходимо для уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым сервисам, не компрометируют их безопасность, обеспечивая:

- соответствующие интерфейсы между сетью организации и сетями, принадлежащими другим организациям, или общедоступными сетями;
- соответствующие механизмы аутентификации в отношении пользователей и оборудования;
- контроль доступа пользователей к информационным сервисам.

Политика в отношении использования сетевых служб

Несанкционированные подключения к сетевым службам могут нарушать информационную безопасность целой организации. Пользователям следует обеспечивать непосредственный доступ только к тем сервисам, в которых они были авторизованы. Контроль доступа, в частности, является необходимым для сетевых подключений к важным или критичным приложениям или для пользователей, находящихся в зонах высокого риска, например, в общественных местах или за пределами организации вне сферы непосредственного управления и контроля безопасности со стороны организации.

Следует предусматривать меры безопасности в отношении использования сетей и сетевых сервисов.

При этом должны быть определены:

- сети и сетевые услуги, к которым разрешен доступ;
- процедуры авторизации для определения, кому, к каким сетям и сетевым сервисам разрешен доступ;
- мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам.

Необходимо, чтобы эти меры согласовывались с требованиями в отношении контроля доступа.

Рассматривая работу в локальных сетях, необходимую для обеспечения безопасности в школе и дома, остановимся на вопросах основ безопасности при работе в сетях, принципах построения защищенных операционных систем (ОС), основных угрозах при работе в сети, основных мерах безопасности при работе в сети.

Основы безопасности при работе в сетях

В современном информационном мире, когда все компьютеры, объединенные в локальную сеть, имеют доступ в Интернет, актуальными становятся вопросы защиты от взлома злоумышленниками.

Рассмотрим основные принципы построения защищенных операционных систем:

- все современные ОС являются *многопользовательскими* — они рассчитаны на работу в системе (в том числе одновременную) нескольких пользователей;
- чтобы отличить одного пользователя от другого, применяются *учетные записи* (accounts) с уникальными *именами* и *паролями*;
- учетные записи различаются *уровнем полномочий (привилегий, прав)* — набором действий, которые обладатель данной учетной записи может выполнять в системе. Обычно учетные записи разделяют на *административные,* обладающие максимальными привилегиями, и *пользовательские,* набор полномочий для которых позволяет нормально работать в системе, но не разрешает выполнять какие-либо критичные с точки зрения безопасности данных операции, например, форматировать разделы жесткого диска или менять настройки сети.

  В различных версиях ОС Windows дополнительно существуют учетные записи с уровнем прав, средним между административным и пользовательским (участники группы «Опытные пользователи»), а также обладающие минимальными

полномочиями *гостевые учетные записи* (участники группы «Гости», включая встроенную учетную запись «Гость»).

Кроме того, существует два типа учетных записей — *локальные* из базы данных конкретного компьютера с ОС Windows, и *глобальные учетные записи в домене,* которые хранятся на контроллерах домена (подробнее о них будет сказано далее);

- для входа в компьютер обязательно нужно указать имя и пароль учетной записи, зарегистрированной в системе. Следует подчеркнуть, что понятие «вход в систему» подразумевает не только непосредственный доступ, но и другие возможности работы с компьютером, например, *сетевой* или *терминальный* вход, для которых также требуются пользовательские имя и пароль.

  В операционных системах Windows допускается также сетевой вход без указания имени и пароля *(анонимный* вход); такие подключения используются при некоторых взаимодействиях в сетях Microsoft;
- после входа в систему (интерактивного, сетевого и т. д.) пользователь получает доступ к ресурсам того компьютера, в который он вошел (например, доступ к локальным файлам или каталогам). Уровень доступа при этом определяется *списком разрешений,* т. е. возможных действий, которые данный пользователь может осуществлять с защищенным объектом. Например, один пользователь может изменить или удалить файл, другой — только прочитать его, а третьему вообще будет отказано в доступе к этому файлу.

Основные угрозы при работе в сети

Угроз, поджидающих пользователей при подключении компьютера к сети, довольно много. Мы приведем только основные из них:

- *«взлом» компьютера* обычно производится с целью захвата контроля над операционной системой и получения доступа к данным;
- *повреждение системы* чаще всего организуется, чтобы нарушить работоспособность (вызвать отказ в обслуживании — «Denial of Service») каких-либо сервисов или компьютера (чаще сервера) целиком, а иногда — даже всей сетевой инфраструктуры организации;
- *кража данных* из-за неправильно установленных прав доступа, при передаче данных или «взломе» системы позволяет

получить доступ к защищаемой, часто — конфиденциальной информации со всеми вытекающими отсюда неприятными для владельца этих данных последствиями;
- *уничтожение данных* имеет целью нарушить или даже парализовать работу систем, компьютеров, серверов или всей организации.

Атаки на компьютеры или серверы, вирусы, «черви», шпионские и «троянские» программы — все это злонамеренное ПО пишется для того, чтобы осуществить в той или иной степени перечисленные выше угрозы.

Основные меры безопасности при работе в сети

Меры безопасности при работе в сети довольно просты. Их можно сформулировать в виде следующего набора правил:
- отключайте компьютер, когда вы им не пользуетесь. Как любят говорить эксперты по компьютерной безопасности, «самым защищенным является выключенный компьютер, хранящийся в банковском сейфе»;
- своевременно обновляйте операционную систему. В любой ОС периодически обнаруживаются так называемые *«уязвимости»*, снижающие защищенность вашего компьютера. Наличие уязвимостей нужно внимательно отслеживать (в том числе читая «компьютерную» прессу или информацию в Интернете), чтобы вовремя предпринимать меры для их устранения.

Рекомендации по защите компьютеров

Для ОС Windows корпорацией Microsoft создан специальный веб-узел Windows Update, обратившись к которому (например, с помощью программы WUPDMGR.EXE или команды **Windows Update** или **Центр обновлений** в меню **Пуск),** нетрудно просмотреть и скачать список обновлений, рекомендуемых для вашего компьютера:
- используйте ограниченный набор хорошо проверенных приложений, не устанавливайте сами и не разрешайте другим устанавливать на ваш компьютер программы, взятые из непроверенных источников (особенно из Интернета). Если приложение больше не нужно, удалите его;
- без необходимости не предоставляйте ресурсы своего компьютера в общий доступ. Если же это все-таки потребова-

лось, обязательно настройте минимально необходимый уровень доступа к ресурсу только для зарегистрированных учетных записей;

- установите (или включите) на компьютере персональный межсетевой экран (брандмауэр). Если речь идет о корпоративных сетях, установите брандмауэры как на маршрутизаторах, соединяющих вашу локальную сеть с Интернетом, так и на всех компьютерах сети;
- обязательно установите на компьютер специализированное антивирусное и «антишпионское» программное обеспечение. Настройте его на автоматическое получение обновлений как минимум один раз в неделю (лучше — ежедневно или даже несколько раз в день);
- даже если вы единственный владелец компьютера, для обычной работы применяйте пользовательскую учетную запись: в этом случае повреждение системы, например, при заражении вирусом, будет неизмеримо меньше, чем если бы вы работали с правами администратора. Для всех учетных записей, особенно административных, установите и запомните сложные пароли.

Сложным считается пароль, содержащий случайную комбинацию букв, цифр и специальных символов, например, jxglrg$N. Разумеется, пароль не должен совпадать с именем вашей учетной записи.

Пароль в виде случайной последовательности символов нелегко запомнить, поэтому часто используют следующую технику — пароль набирается в английской раскладке русскими буквами. Например, слово «Пароль» тогда будет выглядеть как «Gfhjkm». Однако этот способ следует применять с осторожностью — взломщики давно имеют целые словари подобным образом преобразованных слов, так что желательно вставлять в такие пароли специальные символы и цифры.

Пароли для доступа в различные системы должны быть разными. Недопустимо использовать один и тот же пароль для администрирования вашего компьютера и для входа, например, на игровой веб-сайт;

- при работе с электронной почтой никогда сразу не открывайте вложения, особенно полученные от неизвестных отправителей. Сохраните вложение на диск, проверьте его антивирусной программой и только затем откройте. Если есть такая возможность, включите в вашей почтовой программе защиту от потенциально опасного содержимого и отключите поддержку HTML;

- при работе с веб-сайтами соблюдайте меры разумной предосторожности: старайтесь избегать регистрации, не передавайте никому персональные сведения о себе и внимательно работайте с Интернет-магазинами и другими службами, где применяются онлайновые способы оплаты с помощью кредитных карт или систем типа WebMoney, Яндекс-Деньги и т. д.;
- при проведении оплаты убедитесь, что соединение защищено шифрованием с помощью технологии Secure Sockets Layer (SSL) — в этом случае адресная строка обязательно должна начинаться с «https://»;
- перечисленные выше меры лишь повышают общую защищенность системы и данных, но не дают никакой гарантии от их повреждения или даже полной потери. Поэтому обязательно следует создавать резервные копии системы и данных на съемном жестком диске или на DVD-RW — это позволит вам легко восстановить их в случае утери. При этом одну копию имеет смысл хранить вне дома, например, в сейфе;
- исключительно важную роль играет обучение всех пользователей основам безопасной работы в сетях — как в домашних, так и в корпоративных, — ведь нарушение правил одним пользователем ставит под угрозу всю систему защиты.

Защита локальной сети и данных актуальна на всех уровнях корпоративной инфраструктуры, т. к. затрагивает безопасность серверов и рабочих станций. Microsoft предлагает целостное решение по построению информационной системы, основанной на серверной платформе Windows Server 2008 R2 и рабочих станциях Windows Vista и Windows 7.

В систему защиты сети и данных от несанкционированного доступа входят следующие технологии:

- Система управления доступом.
- Система аудита.
- Система аутентификации пользователей.
- Аутентификация с использованием смарт-карт.
- Политика на ограничение использования программ.
- Служба управления правами.
- Центр сертификации.
- Встроенные средства шифрования.
- Шифрующая файловая система EFS.
- Поддержка протокола IPSec.
- Безопасность беспроводных соединений.
- Организация виртуальных частных сетей (VPN).

Для защиты компьютеров дома или в сети можно использовать брандмауэр.

Брандмауэр — это программное или аппаратное обеспечение, которое блокирует атаки хакеров и не позволяет вирусам и вирусам-червям попасть на компьютер через Интернет.

Если компьютер используется дома, включение брандмауэра —эффективный и важный этап его защиты. Если сеть развернута дома, необходимо защитить каждый входящий в нее компьютер. Для защиты сети служит аппаратный брандмауэр, например, маршрутизатор. Кроме того, на каждом компьютере следует установить программный брандмауэр для блокировки распространения вируса в случае, если один из компьютеров все же будет заражен.

Если компьютер используется в сети школы или другой организации, то соблюдайте политику, заданную администратором сети. Администраторы могут настраивать все компьютеры в сети так, что включить брандмауэр нельзя, пока они подключены к сети. В этом случае о необходимости включения брандмауэра на конкретном компьютере можно узнать у администратора сети.

Брандмауэр входит в состав большинства операционных систем Windows, начиная с Windows XP.

ПРАКТИЧЕСКАЯ ЧАСТЬ МОДУЛЯ 5

Практическое задание

Настройка локальной сети школы с учетом требований по минимизации угроз информационной безопасности.

Рекомендации:

- определите периметр локальной сети и средства его защиты;
- разделите ЛВС на несколько физических и/или логических сегментов (компьютеры администрации, методические объединения, компьютерные классы, библиотека и т. д.);
- выделите общие и разделенные (тематические, групповые и т. д.) информационные ресурсы ЛВС (папки: общие, метод. объединений, компьютерных классов; почтовый сервер; база данных библиотеки; принтеры и т. д.);
- выделите ответственных (собственников) информационных ресурсов и выработайте совместно с ними процедуру предоставления доступа к их ресурсам;

- выделите критичные информационные ресурсы и учебные процессы, тесно интегрированные с информационными технологиями (компьютеры и файлы администрации и т. д.);
- выделите особо уязвимые компоненты (компьютерные классы, точки доступа WiFi, удаленный доступ и т. д.);
- определитесь с необходимыми средствами защиты каждого из компонентов (не забудьте о резервном копировании и централизованном обновлении);
- максимально документируйте все ваши действия, создавайте и актуализируйте схемы;
- разработайте документы, содержащие хотя бы общие планы действий для разных экстренных ситуаций (вирусное заражение, удаление файлов с отчетами с сетевого диска секретариата, недоступность ресурсов Интернета с рабочего места завуча и т. д.);
- совместно с другими преподавателями выработайте модель общения с учениками в разнообразных нестандартных ситуациях, связанных с использованием информационных технологий (ученик скопировал на общий ресурс фотографии с неприличным содержанием, ученик пытается использовать ПО для получения пароля администратора системы и т. д.).

Вопросы

1. Можно ли сообщить хорошо успевающему ученику пароль администратора домена?
2. Стоит ли использовать один пароль для разных информационных систем и почему?
3. Какие преимущества дает централизованное администрирование компьютеров и серверов (домен)?
4. Сколько резервных копий критичных данных нужно иметь и где их хранить?
5. Доступ к каким категориям ресурсов сети Интернет необходимо блокировать в соответствии с законодательством РФ?
6. На всех ли компьютерах можно разрешить использовать внешние устройства (флешки, фотоаппараты, смартфоны и т. д.) и почему?
7. Стоит ли разрешать неконтролируемое подключение мобильных устройств (КПК, смартфонов, ноутбуков и т. д.) к ЛВС школы?
8. Правильно ли располагать компьютеры классов информатики и компьютеры администрации в одном сегменте?
9. Какие действия вы предпримете, если заподозрите что в вашей сети появились зараженные компьютеры?

10. Нужно ли контролировать посещение учениками ресурсов социальных сетей и форумов и в каком объеме (запретить все, разрешить только «доверенные ресурсы», журналировать все действия учеников на этих ресурсах и т. д.)?
11. Использовать в работе школы или нет ЭЦП и если использовать, то для каких целей?

Используемые литература и ресурсы

1. Сайт Федерального агентства по техническому регулированию и метрологии ГОСТ Р 50922—2006 ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Защита информации. Основные термины и определения [Электронный ресурс]. — URL: http://protect.gost.ru/v.aspx?control=8&baseC=6&page=0&month=6&year=2008&search=50922&RegNum=1&DocOnPageCount=15&id=121129&pageK=E10BFA12-ED02—4212—8D58—3F1D91F314A0

2. Основы компьютерных сетей: Учебное пособие. — 3-е изд., испр. и доп. — М.: БИНОМ. Лаборатория знаний, 2007. — 160 с.

3. Национальный стандарт Российской Федерации. ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью. ISO/IEC 17799: 2000 Information technology — Code of practice for information security management (IDT) Издание официальное. Москва Стандартинформ 2006

4. Защитите свой компьютер: брандмауэр, безопасность при работе в Интернете. Что такое брандмауэр? [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/computer/basics/firewall.mspx

5. Защитите свой компьютер: брандмауэр, безопасность при работе в Интернете. Выберите оптимальный брандмауэр для своей версии системы Windows [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/computer/firewall/using.mspx —

6. Взлом и защита локальной сети [Электронный ресурс]. — URL: http://virusinfo.info/showthread.php?t=29760