МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ (АТИТиМОТД)

СОЗДАНИЕ И УПРАВЛЕНИЕ СЛУЖБОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Магистерская диссертация
44.04.04 Профессиональное обучение по направлению
Управление информационной безопасностью в профессиональном образовании

Выполнила:
магистрант группы ОФ-209/210-2-1
Каюкова Любовь Яковлевна
Научный руководитель:
зав.кафедрой АТИТиМОТД ППИ
к.т.н, доцент.
Руднев Валерий Валентинович

Проверка на объем заимствований:
___68___% авторского текста

Работа рекомендована к защите
«____» _____2017г.
зав. кафедрой АТИТиМОТД ППИ
_____к.т.н., доцент В.В.Руднев

Челябинск 2017

Оглавление

Введение

В последние годы в образовательных организациях (ОО) участились попытки несанкционированного получения информации, в т. ч. персональных данных преподавателей и студентов. Для того, чтобы противодействовать такой тенденции можно, создать в ОО систему информационной безопасности. Нынешний век характеризуется особенностью перехода от индустриального к информационному обществу. В этих условиях тот, кто владеет информацией и умело ее использует, способен решить поставленные задачи, организовать деятельность подчиненных, обеспечить успешное развитие учреждения. Информация и обеспечивающие ее системы и сети являются ценными ресурсами. Владельцы информации сталкиваются с возрастающей угрозой нарушения режима безопасности детей в ОО, которая поступает из различных источников. Информационным системам и сетям могут угрожать такие опасности, как: компьютерное мошенничество, компьютерные вирусы, хакеры, повреждение, хищение, разглашение конфиденциальной информации и другие виды угроз. В процентном отношении, по различным оценкам специалистов, эти угрозы, в среднем распределяются следующим образом: разглашение информации работниками – 43%; копирование программ и данных – 24%; проникновение в компьютер – 18%; подслушивание переговоров – 5%. Анализ состояния дел в области информационной безопасности позволяет сделать вывод, что система мер, обеспечивающая защиту информации, значительно уменьшает возможность ее утечки, несанкционированного доступа, разглашения и потери информации. Главное, чтобы обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности информации. Однако, опыт показывает, что число попыток, направленных на несанкционированное

получение информации, не падает, а имеет устойчивую тенденцию роста. Для осуществления успешной борьбы с этой тенденцией необходима стройная и управляемая система информационной безопасности (СИБ).

СИБ должна обеспечивать:

- конфиденциальность (защита информации от несанкционированного раскрытия или перехвата);

- целостность (достоверность и полноту информации и компьютерных программ);

- доступность (возможность получить пользователям информацию, в пределах своей компетенции).

С учетом зарубежного и отечественного опыта обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

- организационная защита – это регламентация производственной деятельности и отношений исполнителей на нормативно-правовой основе, исключить или ослабляющая нанесение ущерба;

- инженерно-техническая защита-это использование различных технических средств, которые предотвращают нанесение ущерба.

При построении системы информационной безопасности решающую роль играет организационная защита.

В первую очередь необходимо учитывать следующие аспекты: Безопасность информации может быть обеспечена при комплексном использовании всего арсенала имеющихся средств защиты. Никакая система защиты информации не может обеспечить требуемого уровня безопасности информации без соответствующей подготовки пользователей и соблюдения ими установленных правил. Процесс построения системы

информационной безопасности не является разовым мероприятием. Он должен постоянно совершенствоваться, быть управляемым. Такой подход является основным стратегическим звеном всей системы информационной безопасности, а информация – основным элементом защиты. Следует помнить, что информация существует в различных формах. Ее можно хранить на компьютерах, передавать по локальным сетям и через

Интернет, распечатывать на бумажных носителях, копировать, сканировать, а также озвучивать в разговорах. В целях безопасности все виды носителей информации (документы, пленки, магнитные ленты, дискеты, диски и др.), используемые для ее хранения, должны быть надлежащим образом защищены. Очень часто, рассматривая информационную безопасность, путают и отождествляют два понятия: "компьютерная безопасность" и "информационная безопасность". Это неверно. "Компьютерная безопасность" очень важна, но она является только одной из составляющих "информационной безопасности". Какую же работу необходимо проделать ОУ для обеспечения информационной безопасности? Во-первых, целесообразно обеспечить защиту компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.). Решение данной проблемы возможно только при условии, исключающем вывод локальных сетей ОО на Интернет, либо размещение своего сайта у удаленного провайдера. Во-вторых, необходимо иметь как минимум два сервера. Наличие хороших серверов позволит протоколировать любые действия работников ОО в вашей локальной сети. В-третьих, необходимо установить строгий контроль за электронной почтой, обеспечив постоянный контроль за входящей и исходящей корреспонденцией. А так же применение аппаратных средств защиты информации. В свою очередь, ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях по защите информации" определяет

порядок защиты информации. В соответствии с данной статьей защита информации представляет собой принятие правовых, организационных и технических мер. Меры должны быть направлены на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации. Кроме того, определяется и ответственность граждан за защиту информации. Так, п. 5 ст. 9 Закона № 149-ФЗ гласит: "Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению такой информации". Такая обязанность возлагается Трудовым кодексом РФ (далее – ТК РФ), гл. 14 которого определяет защиту персональных данных работника. В соответствии со ст. 90 ТК РФ: "Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами". Для развития данных положений в РФ 27.07.2006 принят Федеральный закон № 152-ФЗ "О персональных данных", который вступил в силу с 1 января 2008 г. Его основной целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в т. ч. защиты прав на неприкосновенность частной жизни, личную и семейную тайны. Статья 3 данного закона определяет: "Персональные данные – любая информация, относящаяся к определенному или неопределенному на основании такой информации лицу (субъекту персональных данных), в т. ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы,

другая информация". Оценивая законодательную базу, следует обратить внимание, что к объектам информационной безопасности в Минобрнауки России, региональных министерствах (департаментах) образования, муниципальных органах управления образованием и в ОО относят: сведения, составляющие государственную тайну, в соответствии с выписками из перечня сведений, подлежащих засекречиванию в министерствах, ведомствах и организациях; информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера; информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. и персональные данные; средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом. Таким образом, можно сделать вывод, что информационная безопасность является одним из составных элементов комплексной безопасности ОО. Уже сегодня назрела необходимость рассматривать ее как одну из основных составляющих безопасности ОО.

Отечественная и зарубежная наука уделяет большое внимание информационной безопасности. Многие зарубежные социологи и политологи активно исследуют вопросы информационного противоборства и информационной безопасности. Среди наиболее известных трудов можно отметить работы Д.Альбертса, Г.С.Джоуэта, М.Либицки, Д.А.Мальтизи, Р.Д.Маклорина, Р.Л.Пфальцграффа, А.Шафрански, Р.Х.Шульца, А.Эделыптейна и других, где рассматриваются различные аспекты влияния информации на политические, экономические, военные и культурные процессы в современных международных отношениях.

Научное осмысление различных аспектов информационной безопасности активно проводились отечественными учеными А.В.Возженниковым, Ю.Ф.Нуждиным, Е.Н.Пасхиным, Е.Е.Перчук, А.И.Поздняковым, Г.Г.Почепцовым, А.А.Прохожевым, С.П.Расторгуевым, А.А.Стрельцовым, Г.Л.Смоляным, Д.С.Черешкиным, А.С.Шийко, В.Н.Цыгичко и другими.

Рассмотрению проблем защиты личности от вредного информационного воздействия в современном мире посвящены работы Г.В.Грачева, Ю.А.Ермакова, В.Е.Лепского, И.К.Мельника, И.Н.Панарина и других исследователей.

Различным аспектам правовой защиты интересов личности в информационной сфере общества посвящены работы В.А.Анниковой, А.А.Антопольского, А.Л.Балыбердина, И.Л.Бачило, М.С.Григорьева, В.И.Кирина, О.А.Колобова, В.А.Копылова, В.Н.Ясенева, В.Н.Лопатина, Д.В.Огородова, В.Д.Попова, Ю.Г.Просвирина, А.А.Фатьянова.

Техническим аспектам защиты информации в информационных системах и сетях посвящены работы В.А.Герасименко, С.Н.Гриняева, М.П.Зегжды, В.Н.Лопатина, В.А.Никитова, Е.И.Орлова, Г.И.Савина.

Различным аспектам проблемы защиты информации посвящены работы Д.А.Андрианова, Н.А.Брусницына, В.Н.Кузнецова, Е.Ю.Митрохина, С.З.Павленко, И.Н.Панарина, С.В.Рабовского, С.П.Расторгуева, А.В.Федорова, А.С.Шийко.

Проблема исследования:

Объект исследования: Информационная безопасность организации профессионального образования.

Предмет исследования: Программные средства защиты информации, обеспечивающие информационную безопасность организации профессионального образования.

Цель исследования: Выяснить, какие программные средства защиты информации наиболее эффективны и доступны.

Гипотеза: Программные средства защиты информации играют большую роль в обеспечении информационной безопасности образовательной организации.

Задачи исследования:

- раскрыть понятия информация, информационная безопасность, информационная безопасность образовательной организации;

- выявить основные угрозы;

- проанализировать основные способы обеспечения информационной безопасности в организации;

- рассмотреть программные средства защиты информации;

- проанализировать программные средства защиты информации;

- выяснить, какие более доступны и надежны.

Для решения поставленных задач и проверки выдвинутой гипотезы нами использованы теоретические и эмпирические методы исследования. **Теоретические методы**: анализ научной, психолого-педагогической, методической, технической литературы, монографических и диссертационных работ, материалов и публикаций периодической печати по теме исследования, сравнение, аналогия. Теоретические методы в процессе организации исследования дополнялись **эмпирическими методами**: наблюдение, анализ программных средств.

Научная новизна:

-определено влияние на социальное и культурное развитие детей и подростков информационного влияния (ИВ) в сети Интернет;

-этот новый смысл концепции ИБУ, рассматривается как состояние защищенности основных интересов учащихся от угроз, создаваемых информации воздействуют на психику и социально-культурное развития детей разнообразными социальными субъектами и информационной

средой общества, в том числе образовательной средой. Под основными интересами учащихся в данном контексте относится к реализации конституционного права на получение качественного образования, направленного на формирование информационной культуры (ИК) студентов, их физического, духовного и интеллектуального развития, на обеспечение личной безопасности, на повышения качества и уровня жизни;

- разработана концепция ИБУ, включая понятийный аппарат проблемы, основные источники информационной опасности и виды угроз.

Теоретическая значимость исследования определяется расширением научных знаний в области информационной безопасности ОО.

Практическая значимость диссертации определяется тем, что ее результаты позволяют повысить степень защиты информации в ОО путем использования предложенных программных средств и рекомендаций по их применению при формировании системы информационной безопасности, направленной на снижение информационных рисков.

Структура работы:

Работа состоит из введения, двух глав, заключения, список использованной литературы.

В первой главе рассматриваются основные понятия информационной безопасности, существующие угрозы информационной безопасности, средства защиты информации, программные средства защиты информации в ОО, алгоритмы работы и существующие уязвимости.

Вторая глава посвящена информационной безопасности ОО, комплексу программных средств защиты информации.

ГЛАВА 1 ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Информация. Информационная безопасность.

Информация— сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы в процессе жизнедеятельности и работы.

Под *информационной безопасностью* понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Информационная безопасность – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только системный, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность - возможность за разумное время получить требуемую информационную службу;

Целостность - актуальность и целостность информации, ее защита от разрушения и несанкционированного изменения;

Конфиденциальность – защита от несанкционированного доступа к информации. Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

В российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

- **информация** - сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

- **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
- **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

В статье 4 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2. установление ограничений доступа к информации только федеральными законами;
3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4. равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5. обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6. достоверность информации и своевременность ее предоставления;

7. неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся *информация* делится на **общедоступную** и ограниченного **доступа**. К общедоступной информации относятся общеизвестные сведения и иная *информация*, *доступ* к которой не ограничен. В законе, определяется *информация*, к которой нельзя ограничить *доступ*, например, *информация* об окружающей среде или деятельности государственных органов. Оговаривается также, что *ограничение доступа* к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, *доступ* к которой ограничен федеральными законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

1. информацию, свободно распространяемую;

2. информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3. информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4. информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее *определение* защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2. соблюдение конфиденциальности информации ограниченного доступа;

3. реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1. предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2. своевременное обнаружение фактов несанкционированного доступа к информации;

3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6. постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ "Об информации, информационных технологиях и о защите информации" создает правовую основу информационного обмена в РФ и определяет *права* и обязанности его субъектов.

1.2. Основные угрозы безопасности информации.

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или повредиться. Компоненты автоматизированной информационной системы можно разделить на следующие группы:

Оборудование - это компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства - принтеры, контроллеры, кабели, линии связи, и т. д.);

Программное обеспечение - это приобретенные программы, исходные, объектные, загрузочные модули;

Операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;

Данные, хранимые временно и постоянно, на дисках, флэшках, печатные, архивы, системные журналы и т. д.;

Персонал. Пользователи, администраторы, разработчики и т. д.

Опасные воздействия на компьютерную информационную систему можно разделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Из причин случайных воздействия во время эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и аварий;
- неисправности и сбои оборудования;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи с влиянием внешней среды.

Преднамеренные воздействия - это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник.

Можно составить гипотетическую модель потенциального нарушителя:

- квалификация нарушителя на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- преступнику известна информация о принципах работы системы;

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ. Несанкционированный доступ и использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Проведем классификацию каналов несанкционированного доступа, по которым можно осуществить хищение, изменение или уничтожение информации (Рис.1):

- Через человека

- Программа

- Через аппаратуру

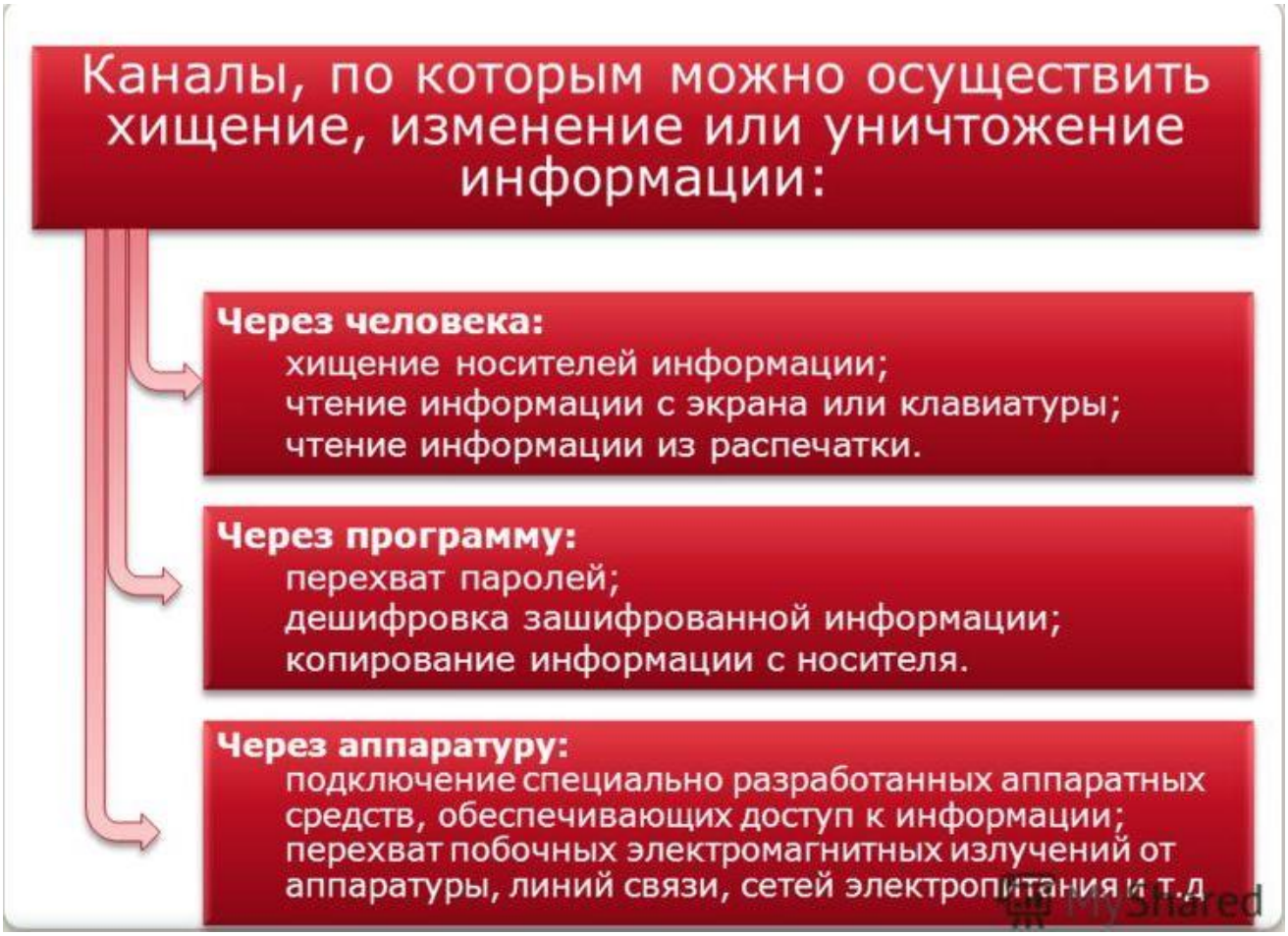

Рис.1

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основной характеристикой любой компьютерной сети является то, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программ с помощью механизма сообщений. При этом сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характеризуется тем, что в отношении них принимают так называемых удаленных атак. Преступник может находиться за тысячи километров от атакуемого объекта, при этом нападению может быть не только конкретный компьютер, но и информация, передающаяся по сети каналов связи.

1.3. Обеспечение безопасности информации

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1. *Законодательный* - это правила, нормы, стандарты и т. д.

Нормативно-правовая база определяет правила защиты информации:

• Ст. 16 закона от 27.07.2006 № 149-ФЗ "ОБ информации, информационных технологиях по защите информации".

В соответствии со статьей защита информации - принятие правовых, организационных и технических мер. Средства должны быть направлены на обеспечение защиты информации от несанкционированного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

• Ст. 9 Федерального закона № 149-ФЗ, пункт 5 изложить в следующей редакции "Сведения, полученные от граждан (физических лиц) при исполнении ими профессиональных обязанностей или организациями при осуществлении некоторых видов деятельности (профессиональная тайна), подлежит защите в случаях, если эти лица федеральными обязанности соблюдения такой информации. Такая обязанность возлагается трудового кодекса Российской Федерации (далее – таможенный кодекс), глава 14, который определяет защиту персональных данных работника. В соответствии со статьей ТК РФ: "Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданскую или уголовную ответственность в соответствии с федеральным законом.

• Для развития этих положений в Российской федерации принят закон № 152-ФЗ РФ "О защите персональных данных». Его основной

целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейные тайны. Статья 3 этого закона определяет: "Персональные данные - любая информация, касающаяся определенного или неопределенному на основании такой информации лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, положение, имущественного, другая информация"

• Закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию", в соответствии с которым содержание и графической информации, предназначенные для детей в дошкольных образовательных учреждениях, должны соответствовать содержанию и художественному проектирования информации для детей в этом возрасте. А также, в соответствии с Федеральным законом "Об основных гарантиях прав ребенка", образовательные учреждения обязаны ограничивать доступ учащихся к ресурсам сети Интернет, пропагандирующим насилие и жестокость, порнографию, наркоманию, токсикоманию, антиобщественное поведение.

2. *Моральный и этический*. Всевозможные стандарты, несоблюдение которых ведет к падению престижа конкретного человека или целой организации.

3. *Административный*. Действия общего характера, предпринимаемые руководством организации.

4. *Физический*. Механические, электрические и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей.

5. *Аппаратно - программный* (электронные устройства и специальные программы защиты информации).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Надежная система защиты должна соответствовать следующим принципам:

Стоимость средств защиты должна быть меньше, чем размеры возможного ущерба.

Каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы.

Защита тем более эффективна, чем проще пользователю с ней работать.

Возможность отключения в экстренных случаях.

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать.

Под защитой должна находиться вся система обработки информации.

Разработчики системы защиты, не должны быть в числе тех, кого эта система будет контролировать.

Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.

Объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других.

Надежная система защиты должна быть полностью протестирована и согласована.

Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.

Система защиты должна разрабатываться, исходя из предположения, что пользователи будут совершать серьезные ошибки и, вообще, имеют наихудшие намерения.

Существование механизмов защиты должно быть по возможности скрыто от пользователей, работа которых находится под контролем.

1.4. Средства защиты информации.

Средства защиты информации - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

- *Аппаратные (технические) средства.* Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, сторожа, защитная сигнализация и др. Вторую - генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов,

высокой устойчивостью к модификации. Слабые стороны - недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

- *Программные средства* включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств - универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки - ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств)

1.5. Программные средства защиты информации.

Программные средства - это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения

Программными называются средства защиты данных, функционирующие в составе программного обеспечения. Среди них можно выделить и подробнее рассмотреть следующие:

· средства архивации данных;

· антивирусные программы;

· криптографические средства;

· средства идентификации и аутентификации пользователей;

· средства управления доступом;

· протоколирование и аудит.

1.6. Анализ программных средств защиты информации

Средства архивации информации

Иногда резервные копии информации приходится выполнять при общей ограниченности ресурсов размещения данных, например владельцам персональных компьютеров. В этих случаях используют программную архивацию. Архивация это слияние нескольких файлов и даже каталогов в единый файл - архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т. е. с возможностью точного восстановления исходных файлов. Действие большинства средств архивации основано на использовании алгоритмов сжатия, предложенных в 80-х гг. Абрахамом Лемпелем и Якобом Зивом. Наиболее известны и популярны следующие архивные форматы:

· ZIP, ARJ для операционных систем DOS и Windows;

· TAR для операционной системы Unix;

· межплатформный формат JAR (Java ARchive);

· RAR (все время растет популярность этого формата, так как разработаны программы позволяющие использовать его в операционных системах DOS, Windows и Unix).

Пользователю следует лишь выбрать для себя подходящую программу, обеспечивающую работу с выбранным форматом, путем оценки ее характеристик - быстродействия, степени сжатия, совместимости с большим количеством форматов, удобности интерфейса, выбора операционной системы и т.д. Список таких программ очень велик - PKZIP, PKUNZIP, ARJ, RAR, WinZip, WinArj, ZipMagic, WinRar и много других. Большинство из этих программ не надо специально покупать, так как они предлагаются как программы условно-бесплатные (Shareware) или свободного распространения (Freeware).

Антивирусные программы

Это программы разработанные для защиты информации от вирусов. Неискушенные пользователи обычно считают, что компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять нежелательные различные действия на компьютере. Специалисты по компьютерной вирусологии определяют, что обязательным (необходимым) свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Следует отметить, что это условие не является достаточным, т.е. окончательным. Вот почему точного определения вируса нет до сих пор, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому “хорошие” файлы можно отличить от “вирусов”. Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Особую проблему представляют собой компьютерные вирусы. Это отдельный класс программ, направленных на нарушение работы системы и порчу данных. Среди вирусов выделяют ряд разновидностей. Некоторые из них постоянно находятся в памяти компьютера, некоторые производят деструктивные действия разовыми "ударами".

Существует так же целый класс программ, внешне вполне благопристойных, но на самом деле портящих систему. Такие программы называют "троянскими конями". Одним из основных свойств компьютерных вирусов является способность к "размножению" - т.е. самораспространению внутри компьютера и компьютерной сети.

С тех пор, как различные офисные прикладные программные средства получили возможность работать со специально для них

написанными программами (например, для Microsoft Office можно писать приложения на языке Visual Basic) появилась новая разновидность вредоносных программ – Макро Вирусы. Вирусы этого типа распространяются вместе с обычными файлами документов, и содержатся внутри них в качестве обычных подпрограмм.

С учетом мощного развития средств коммуникации и резко возросших объемов обмена данными проблема защиты от вирусов становится очень актуальной. Практически, с каждым полученным, например, по электронной почте документом может быть получен макровирус, а каждая запущенная программа может (теоретически) заразить компьютер и сделать систему неработоспособной.

Поэтому среди систем безопасности важнейшим направлением является борьба с вирусами. Существует целый ряд средств, специально предназначенных для решения этой задачи. Некоторые из них запускаются в режиме сканирования и просматривают содержимое жестких дисков и оперативной памяти компьютера на предмет наличия вирусов. Некоторые же должны быть постоянно запущены и находиться в памяти компьютера. При этом они стараются следить за всеми выполняющимися задачами.

На рынке программного обеспечения наибольшую популярность завоевал пакет AVP, разработанный лабораторией антивирусных систем Касперского. Это универсальный продукт, имеющий версии под самые различные операционные системы. Также существуют следующие виды: Acronis AntiVirus, AhnLab Internet Security, AOL Virus Protection, ArcaVir, Ashampoo AntiMalware, Avast!, Avira AntiVir, A-square anti-malware, BitDefender, CA Antivirus, Clam Antivirus, Command Anti-Malware, Comodo Antivirus, Dr.Web, eScan Antivirus, F-Secure Anti-Virus, G-DATA Antivirus, Graugon Antivirus, IKARUS virus.utilities, Антивирус Касперского, McAfee VirusScan, Microsoft Security Essentials, Moon Secure AV, Multicore

antivirus, NOD32, Norman Virus Control, Norton AntiVirus, Outpost Antivirus, Panda и т.д.

Способы обнаружения и удаления неизвестного вируса:

· Профилактика заражения компьютера;

· Восстановление пораженных объектов;

· Антивирусные программы.

Профилактика заражения компьютера.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которое позволяет значительно снизить вероятность заражения вирусом и потери каких-либо данных.

Для того чтобы определить основные правила компьютерной гигиены, необходимо выяснить основные пути проникновения вируса в компьютер и компьютерные сети.

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word. Пользователь зараженного макро - вирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д. Выводы - следует избегать контактов с подозрительными источниками информации и пользоваться только законными (лицензионными) программными продуктами.

Восстановление пораженных объектов

В большинстве случаев заражения вирусом процедура восстановления зараженных файлов и дисков сводится к запуску подходящего антивируса, способного обезвредить систему. Если же вирус неизвестен ни одному антивирусу, то достаточно отослать зараженный файл фирмам-производителям антивирусов и через некоторое время

(обычно - несколько дней или недель) получить лекарство - “update” против вируса. Если же время не ждет, то обезвреживание вируса придется произвести самостоятельно. Для большинства пользователей необходимо иметь резервные копии своей информации.

Анализ антивирусных программ

Самыми популярными и эффективными антивирусными программами считаются антивирусные фаги (иначе эти программы называются сканерами или полифагами) и ревизоры (CRC сканеры). Часто обе приведенные разновидности объединяются в одну универсальную антивирусную программу, что значительно повышает ее мощность. Реже используют различного типа мониторы (блокировщики) и вакцины (иммунизаторы). Следует, однако, иметь в виду, что, в принципе, нельзя создать универсальное и абсолютно надежное средство борьбы со всеми существующими и будущими вирусами.

Программы-фаги. Принцип работы антивирусных программ-фагов (сканеров) основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски или, как их еще называют, некоторая постоянная последовательность кода, специфичная для конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Например, перебор всех возможных вариантов кода вирусов. Этот способ эффективно используется для детектирования полиморфных вирусов.

Во многих полифагах используются алгоритмы эвристического сканирования, т. е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие мягкого решения («возможно, заражен» или «не заражен») для каждого проверяемого объекта.

К достоинствам сканеров относится их универсальность, к недостаткам — низкая скорость сканирования, а также необходимость постоянного обновления антивирусных баз.

Принцип работы типичного алгоритма сканирования сводится к следующему. После загрузки с дискеты, на которой операционная система гарантированно свободна от вируса, программа проверяет дерево каталогов диска, логическое имя которого указывается в виде параметра при запуске. При нахождении *.exe или *.com модуля проверяется его длина. Если длина модуля больше 4 Кбайт, в теле программы ищется сигнатура вируса по соответствующему смещению. Если вирус найден, восстанавливаются скрытые в теле вируса байты начала модуля, после чего длина файла уменьшается на длину вируса и вирус удаляется из зараженного модуля. После этого восстанавливаются исходные время и дата создания файла.

Программы-ревизоры. Они подсчитывают контрольные суммы для присутствующих на диске файлов и системных секторов. Эти суммы сохраняются в базе данных антивируса вместе с некоторой другой информацией: размерами файлов, датами их последней модификации и т.п. При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

Ревизоры, использующие антиСТЕЛС алгоритмы, являются довольно сильным оружием против вирусов: практически 100 % вирусов оказываются обнаруженными почти сразу после их появления в компьютере. Существенным недостатком таких средств борьбы с вирусами является то, что программы-ревизоры распознают наличие вируса в системе уже после его распространения. Кроме того, они не распознают вирусы в новых, только что полученных или записанных

файлах, поскольку в их базах данных отсутствует информация об этих файлах. Периодически появляются вирусы, которые используют эту слабость ревизоров, заражая только вновь создаваемые файлы. Такие вирусы остаются невидимыми.

Программы-мониторы. Антивирусные мониторы — это резидентные программы, перехватывающие вирусоопасные ситуации и сообщающие об их возникновении. К вирусоопасным относятся вызовы на открытие для записи в выполняемых файлах, запись в загрузочные секторы дисков, попытки программ остаться резидентно. Иначе говоря, вызовы генерируются вирусами в моменты их размножения.

К достоинствам программ-мониторов относится их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения, что бывает очень полезно в случаях, когда давно известный вирус постоянно «выползает неизвестно откуда». К недостаткам относятся существование путей обхода защиты монитора и большое количество ложных срабатываний. Существуют аппаратные реализации некоторых функций мониторов, в том числе встроенные в BIOS. Однако, как и в случае с программными мониторами, такую защиту легко обойти прямой записью в порты контроллера диска, а запуск DOS утилиты FDISK немедленно вызывает ложное срабатывание защиты.

Программы-вакцины. Антивирусные вакцины (иммунизаторы) подразделяются на два типа: сообщающие о заражении и блокирующие заражение каким-либо типом вируса. Первые обычно записываются в конец файлов (по принципу файлового вируса), и при запуске файла каждый раз проверяют его на предмет обнаружения изменений. Недостаток у таких вакцин один, но он летален: абсолютная неспособность вакцины сообщить о заражении СТЕЛСвирусом. Поэтому такие иммунизаторы, как и мониторы, в настоящее время практически не используются.

Второй тип вакцин защищает систему от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженными. Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса. При запуске зараженной программы, вирус распознает вакцину как свою резидентскую копию и не активизируется. Такой тип вакцинации не может быть универсальным, поскольку при его помощи нельзя иммунизировать файлы от всех известных вирусов. Однако несмотря на это подобные программные средства в качестве полумеры могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет детектироваться антивирусными сканерами.

Антивирусные программные комплексы. В современных условиях лишь они могут обеспечить надежную защиту от вирусных программ, отличающихся большим разнообразием принципов построения и функционирования. Обычно современные антивирусные программные комплексы включают в свой состав монитор, сканер, ревизор и планировщик.

Планировщик используется для координации работы разных компонентов антивирусного пакета и планирования антивирусных мероприятий в вычислительной системе.

Вакцина вследствие своей естественной ограниченности использования низкой универсальности в настоящее время практически не применяется.

Назвать среди большого количества программ, лучший антивирусник невозможно, ведь критериев, которыми могут руководствоваться пользователи при выборе, множество. Несомненно одно - все решения заслуживают внимания пользователей и относятся к числу достойных.

Криптографические средства

Механизмами шифрования данных для обеспечения информационной безопасности общества является криптографическая защита информации посредством криптографического шифрования.

Криптографические методы защиты информации применяются для обработки, хранения и передачи информации на носителях и по сетям связи. Криптографическая защита информации при передаче данных на большие расстояния является единственно надежным способом шифрования.

Криптография - это наука, которая изучает и описывает модель информационной безопасности данных. Криптография открывает решения многих проблем информационной безопасности сети: аутентификация, конфиденциальность, целостность и контроль взаимодействующих участников.

Термин *«Шифрование»* означает преобразование данных в форму, не читабельную для человека и программных комплексов без ключа шифрования-расшифровки. Криптографические методы защиты информации дают средства информационной безопасности, поэтому она является частью концепции информационной безопасности.

Криптографическая защита информации (конфиденциальность).

Цели защиты информации в итоге сводятся к обеспечению конфиденциальности информации и защите информации в компьютерных системах в процессе передачи информации по сети между пользователями системы.

Защита конфиденциальной информации, основанная на криптографической защите информации, шифрует данные при помощи семейства обратимых преобразований, каждое из которых описывается параметром, именуемым «ключом» и порядком, определяющим очередность применения каждого преобразования.

Важнейшим компонентом криптографического метода защиты информации является ключ, который отвечает за выбор преобразования и порядок его выполнения. Ключ - это некоторая последовательность символов, настраивающая шифрующий и дешифрующий алгоритм системы криптографической защиты информации. Каждое такое преобразование однозначно определяется ключом, который определяет криптографический алгоритм, обеспечивающий защиту информации и информационную безопасность информационной системы.

Один и тот же алгоритм криптографической защиты информации может работать в разных режимах, каждый из которых обладает определенными преимуществами и недостатками, влияющими на надежность информационной безопасности.

Основы информационной безопасности криптографии (Целостность данных)

Защита информации в локальных сетях и технологии защиты информации наряду с конфиденциальностью обязаны обеспечивать и целостность хранения информации. То есть, защита информации в локальных сетях должна передавать данные таким образом, чтобы данные сохраняли неизменность в процессе передачи и хранения.

Для того чтобы информационная безопасность информации обеспечивала целостность хранения и передачи данных необходима разработка инструментов, обнаруживающих любые искажения исходных данных, для чего к исходной информации придается избыточность.

Информационная безопасность с криптографией решает вопрос целостности путем добавления некой контрольной суммы или проверочной комбинации для вычисления целостности данных. Таким образом, снова модель информационной безопасности является криптографической - зависящей от ключа. По оценке информационной безопасности, основанной на криптографии, зависимость возможности

прочтения данных от секретного ключа является наиболее надежным инструментом и даже используется в системах информационной безопасности государства.

Как правило, аудит информационной безопасности предприятия, например, информационной безопасности банков, обращает особое внимание на вероятность успешно навязывать искаженную информацию, а криптографическая защита информации позволяет свести эту вероятность к ничтожно малому уровню. Подобная служба информационной безопасности данную вероятность называет мерой лимитостойкости шифра, или способностью зашифрованных данных противостоять атаке взломщика.

Идентификация и аутентификация пользователя

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс представления компьютерной системе, который включает две стадии:

* идентификацию - пользователь сообщает системе по ее запросу свое имя (идентификатор);

* аутентификацию - пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль).

Для проведения процедур идентификации и аутентификации пользователя необходимы:

* наличие соответствующего субъекта (модуля) аутентификации;

* наличие аутентифицирующего объекта, хранящего уникальную информацию для аутентификации пользователя.

Различают две формы представления объектов, аутентифицирующих пользователя:

* внешний аутентифицирующий объект, не принадлежащий системе;

* внутренний объект, принадлежащий системе, в который переносится

информация из внешнего объекта.

Внешние объекты могут быть технически реализованы на различных носителях информации - магнитных дисках, пластиковых картах и т. п. Естественно, что внешняя и внутренняя формы представления аутентифицирующего объекта должны быть семантически тождественны.

Управление доступом защиты информации

Управление доступом как один из способов защиты информации - это способ защиты информации с помощью регулирования использования всех ресурсов системы (технических, программных средств, элементов баз данных).

Управление доступом включает следующие функции защиты:

- проверку полномочий, заключающуюся в проверке соответствия времени, ресурсов и процедур установленному регламенту;

- разрешение и создание условий работы в пределах (и только в пределах) установленного регламента;

- регистрацию (протоколирование) обращений к защищаемым ресурсам;

- реагирование (задержка работ, отключение, сигнализация) при попытках несанкционированных действий.

- идентификацию пользователей, персонала и ресурсов системы, причем под идентификацией понимается присвоение каждому объекту персонального идентификатора (имени, кода, пароля и т.п.) и опознание (установление подлинности) субъекта или объекта по предъявленному идентификатору;

Протоколирование и аудит

Под *протоколированием* понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит – это анализ накопленной информации, проводимый оперативно, в

реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов;

- обеспечение возможности реконструкции последовательности событий;

- обнаружение попыток нарушений информационной безопасности;

- предоставление информации для выявления и анализа проблем.

Протоколирование требует для своей реализации здравого смысла. Какие события регистрировать? С какой степенью детализации? На подобные вопросы невозможно дать универсальные ответы. Необходимо следить за тем, чтобы, с одной стороны, достигались перечисленные выше цели, а, с другой, расход ресурсов оставался в пределах допустимого. Слишком обширное или подробное протоколирование не только снижает производительность сервисов (что отрицательно сказывается на доступности), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Характерная особенность протоколирования и аудита – зависимость от других средств безопасности. Идентификация и аутентификация служат отправной точкой подотчетности пользователей, логическое управление

доступом защищает конфиденциальность и целостность регистрационной информации. Возможно, для защиты привлекаются и криптографические методы.

Защита информации в КС от несанкционированного доступа

Для осуществления несанкционированного доступа злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав КС. Он осуществляет несанкционированный доступ, используя:

* знания о КС и умения работать с ней;

* сведения о системе защиты информации;

* сбои, отказы технических и программных средств;

* ошибки, небрежность обслуживающего персонала и пользователей.

Для защиты информации от несанкционированного доступа создается система

разграничения доступа к информации. Получить несанкционированный доступ к информации при наличии системы разграничения доступа возможно только при сбоях и отказах КС, а также используя слабые места в комплексной системе защиты информации. Чтобы использовать слабости в системе защиты, злоумышленник должен знать о них.

Одним из путей добывания информации о недостатках системы защиты является изучение механизмов защиты. Злоумышленник может тестировать систему защиты путем непосредственного контакта с ней. В этом случае велика вероятность обнаружения системой защиты попыток ее тестирования. В результате этого службой безопасности могут быть предприняты дополнительные меры защиты.

Гораздо более привлекательным для злоумышленника является другой подход. Сначала получается копия программного средства системы защиты или техническое средство защиты, а затем производится их

исследование в лабораторных условиях. Кроме того, создание неучтенных копий на съемных носителях информации является одним из распространенных и удобных способов хищения информации. Этим способом осуществляется несанкционированное тиражирование программ. Скрытно получить техническое средство защиты для исследования гораздо сложнее, чем программное, и такая угроза блокируется средствами и методами обеспечивающими целостность технической структуры КС. Для блокирования несанкционированного исследования и копирования информации КС используется комплекс средств и мер защиты, которые объединяются в систему защиты от исследования и копирования информации. Таким образом, система разграничения доступа к информации и система защиты информации могут рассматриваться как подсистемы системы защиты от несанкционированного доступа к информации.

Другие программные средства защиты информации

Межсетевые экраны (также называемые брандмауэрами или файрволами - от нем. Brandmauer, англ. firewall -- «противопожарная стена»). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода - это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

Proxy-servers (proxy - доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью -- маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные

серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях -- например, на уровне приложения (вирусы, код Java и JavaScript).

VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

Вывод по главе 1

Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

Многообразие условий, способствующих неправомерному овладению конфиденциальной информацией, вызывает необходимость использования не менее многообразных способов, сил и средств для обеспечения информационной безопасности. Проблема информационной безопасности образовательной организации превращается в последнее время из гипотетической во вполне реальную. Количество угроз растет с каждым днем, изменяется нормативно-правовая база, соответственно

реалиям времени должны изменяться и методы обеспечения информационной безопасности учебного процесса.

В современной ОО информация, информационная инфраструктура – один из главных компонентов учебного процесса. Учебные классы оснащаются компьютерной техникой и её качественное бесперебойное функционирование существенно определяет качество полученных знаний, способствует формированию профессиональных компетенций учащихся.

Вот поэтому-то обеспечение информационной безопасности учебного процесса, в том числе непрерывного функционирования компьютерных и информационных ресурсов, является весьма важной для его качества.

Для обеспечения информационной безопасности используются различные средства защиты информации.

Основные направления использования программной защиты информации:

- защита информации от НСД,
- защита программ от копирования,
- защита информации от разрушения,
- защита информации от вирусов,
- защита программ от вирусов,
- программная защита каналов связи.

По каждому из данных направлений имеется большое количество качественных программных продуктов, распространяемых на рынке.

ГЛАВА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ (ОО).

2.1. Информационная безопасность ОО

Учитывая изложенное, под информационной безопасностью ОО следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Построение системы информационной безопасности в школе происходит следующим образом. На первом этапе определяется, что подлежит защите. На втором этапе выявляются возможные каналы утечки информации и определяются возможные угрозы информационным системам. Далее вырабатываются меры по защите информации и технологических систем. На основе выработанных мер защиты разрабатываются нормативно-правовые документы, регламентирующие информационную безопасность. В последующем организуется контроль за соблюдением установленных правил. При таком подходе система информационной безопасности будет направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию. В целях обеспечения информационной безопасности и ее организации, на основании законодательных документов, в ОО следует разрабатывать соответствующие нормативно-правовые акты. Правовые нормы обеспечения информационной безопасности в конкретном ОО фиксируются в учредительных, организационных и функциональных документах. Требования обеспечения информационной безопасности отражаются в уставе (учредительном договоре) в виде следующих положений:

- ОО имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных учащихся, работников ОО, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз;

- ОО обязано обеспечить сохранность конфиденциальной информации. Такие требования дают право администрации ОО:

- назначить ответственного за обеспечение информационной безопасности;

- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

- включать требования по обеспечению информационной безопасности в коллективный договор;

- включать требования по защите информации в договоры по всем видам деятельности; разрабатывать перечень сведений конфиденциального характера;

- требовать защиты интересов ОО со стороны государственных и судебных инстанций.

К организационным и функциональным документам следует отнести:

- приказ руководителя ОО о назначении ответственного за обеспечение информационной безопасности;

- должностные обязанности ответственного за обеспечение информационной безопасности;

- перечень защищаемых информационных ресурсов и баз данных;

- инструкцию, определяющую порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников ОО.

Данный перечень документов не является исчерпывающим. В зависимости от особенностей, специфики и характера ОО он может быть расширен и дополнен. Кроме того, должен быть определен порядок допуска сотрудников ОО к информации.

Такой допуск предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства РФ и ОО об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

- инструктаж работника специалистом по информационной безопасности; - контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

Как показала практика, при проверке организации системы информационной безопасности, как правило, отмечаются следующие недостатки:

- отсутствует перечень сведений, составляющий конфиденциальную информацию;

- отсутствуют должностные обязанности ответственного за информационную безопасность;

- не соблюдается порядок учета носителей информации конфиденциального характера;

- нарушен порядок делопроизводства.

Самым серьезным недостатком в организации информационной безопасности является отсутствие взаимопонимания между теми, кто обеспечивает информационную безопасность, и теми, кто пользуется данной информацией. Нередко пользователи информации нарушают порядок обращения с ней и не соблюдают требования нормативно-правовых документов, регламентирующих информационную безопасность. Решение данной проблемы возможно только при соблюдении принципов информационной безопасности, постоянной требовательности по соблюдению конфиденциальности со стороны руководителя ОО.

С учетом этих недостатков для обеспечения информационной безопасности в ОО требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности ОО;

- защита компьютеров, локальных сетей и сети подключения к системе Интернета в классе информатики ОО;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и учащихся ОО;

- учет всех носителей конфиденциальной информации.

Реализация данного комплекса мер вносит кардинальные изменения в организацию работы с информацией в ОО, а также делопроизводства, в т. ч. и по вопросам безопасности.

При таком подходе, основными составными задачами делопроизводства станут: документирование информации, учет документов, организация документооборота, обеспечение надежного хранения документов, своевременное их уничтожение, проверка наличия хранящихся документов, контроль за своевременным и правильным их исполнением. Необходимо помнить, что не на всяком документе имеется гриф "Для служебного пользования" ("Ограниченного пользования"), однако это не означает, что такой документ не представляет никакой ценности. Не бывает важных или не очень важных документов. Самый малозначительный, на первый взгляд документ, при определенных обстоятельствах может оказаться чрезвычайно важным. Организация вышеперечисленных мероприятий позволит избежать непредвиденных ситуаций, путаницы и неразберихи. Следует отметить, что при организации делопроизводства необходимо выявить и учесть все возможные каналы утечки информации. Наиболее характерными каналами утечки информации для ОО могут стать разглашение, хищение и

несанкционированный доступ. Учитывая эти аспекты, систему организации делопроизводства можно представить в следующем виде:

- учет всей документации ОО, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

- регистрация и учет всех входящих (исходящих) документов ОО в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);

- особый режим уничтожения документов. Уничтожать документы можно с помощью уничтожителя бумаг, или сжиганием. В обязательном порядке нужно составлять об этом акт, подписываемый комиссией, назначенной приказом руководителя ОО.

Для облегчения контроля все документы следует разделить на две группы: для общего пользования и для служебного пользования (ограниченного пользования). Документам каждой категории необходимо присвоить свой гриф. Это можно сделать при помощи штампов, специальных отметок или цветового выделения (для общего пользования – зеленый цвет, для служебного – красный). При присвоении соответствующего грифа соблюдаются определенные правила, которые необходимо учитывать в своей работе: ответственность за присвоение соответствующего грифа несет исполнитель документа, а субъектом оценки его присвоения является руководитель ОУ; ценность информации определяется с помощью таких критериев, как полезность, своевременность, актуальность, достоверность, конфиденциальность; информация подлежит защите при условии, что доступ к ней закрыт на законном основании. В ходе использования, передачи, копирования и

исполнения документов также необходимо соблюдать определенные правила: Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах.

Для создания безопасной информационной системы в ОО можно принять меры:

- Обеспечить защиту компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.)

- Установить строгий контроль за электронной почтой, обеспечить постоянный контроль за входящей и исходящей корреспонденции.

- Использовать контент-фильтры для фильтрации сайтов по их содержимому.

Одна сумма всех этих мероприятий, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Специалисты, которые имеют отношение к системе защиты, должны быть в полной мере представить себе принципы ее функционирования и в случае возникновения сложной ситуации адекватно реагировать. Под защитой должна находиться вся система обработки информации.

Лица, занимающиеся обеспечением информационной безопасности, должны нести ответственность.

Надежная система защиты должна быть полностью протестирована и совместима. Защита становится более эффективной и гибкой, если она допускает изменение их параметров со стороны администратора.

2.2. Информационная безопасность персональных данных

Начиная с 2006 года согласно 152 ФЗ «О защите персональных данных любая государственная ОО является оператором персональных данных. С этим сложно спорить, поскольку любое учебное заведение хранит у себя персональные данные обучающихся и сотрудников и не только хранит, но и ведет автоматизированную обработку этих данных. В Санкт-Петербурге во всех ОО имеется АИС «Параграф» с помощью, которого и ведется данная обработка. Но на самом деле, автоматизированная обработка персональных данных ведется и в тех регионах, в которых системы управления ОО еще не внедрены повсеместно. Поскольку с точки зрения проверяющего органа, которым в данном случае является Роскомнадзор, ввод списка персональных данных с помощью текстового редактора, тоже является автоматизированной обработкой персональных данных. Если же разбирать ситуацию более пристально, то мы увидим, что существует еще и информация о родителях учащихся, с паспортными данными, местом проживания, местом работы, контактными телефонами, испокон веков, заполнявшаяся на последних страницах классных журналов, а сейчас без раздумий переносящаяся в автоматизированные системы. Подводя итог вышесказанного можно посчитать, что в ОО на 800 учащихся хранятся данные на 800 учащихся, примерно 1200 родителей и около 100 сотрудников учреждения. Итого в ОО хранятся текущие персональные данные на более чем две тысячи человек. Много это или мало? С одной стороны, видно, что такое количество данных требует работы по их защите, с другой с точки зрения 152 ФЗ и иных нормативных документов (Приказы ФСТЭК России, ФСБ России, Мининформсвязи России N 55/86/20), значения обрабатываемых персональных данных относятся к категории 3 и объем обрабатываемых персональных данных относятся к категории 2 (от 1000 до 100 000 записей). А значит информационную систему персональных данных

(ИСПДн) ОО можно отнести к 3 классу и ограничить работу по защите персональных данных организационными мерами. Сразу оговоримся, что существуют случаи, когда нельзя говорить о 3 классе персональных данных. Например, если ОО имеет функции районного или муниципального центра, собирающего персональные данные с разных учреждений. В этом случае, даже если число записей не велико, сам функционал сбора, повышает класс ИСПДн до 2-го. Еще один случай повышения класса, когда информационные системы могут содержать данные о заболеваниях, судимостях, политических предпочтениях и т.п. данные. В этом случае надо говорить о 1 классе ИСПДн. Во всех вышеперечисленных случаях учреждение не может ограничиться организационными мерами, а должно заказать технические работы по защите персональных данных. Причем, именно заказать, поскольку такие работы осуществляются только при наличии соответствующих лицензий ФСБ или ФСТЭК и требуют серьезного финансирования. В нашей работе мы рассмотрим только необходимые организационные меры и перечень необходимых документов. Ниже приведен примерный перечень из 15 документов, которые необходимо разработать ОО. Он не является единственно возможным.

− Приказ о назначении ответственных за безопасность ПДн (персональные данные).

− Приказ о назначении ответственных лиц за ПДн и список ответственных лиц.

− Приказ о введении режима обработки ПДн.

− Приказ о создании комиссии для классификации ИСПДн.

− Перечень подразделений и сотрудников, допущенных к работе с ПДн.

− Перечень ИСПДн.

− Перечень ПДн.

− Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах.

− Частная модель угроз.

− Инструкция пользователя ИСПДн.

− Акт Классификации ИСПДн.

− СОГЛАСИЕ на обработку ПДн.

− Обязательство о неразглашении ПДн.

− Журнал учета носителей ПДн.

− Журнал учёта обращений субъектов ПДн о выполнении их законных прав. Видно, что перечисленные документы делятся на несколько групп. 1-я группа приказы по учреждению. Самый важный из приказов – о назначении ответственных за безопасность ПДн. Одна из типичных ошибок администрации ОО – назначить на эту должность учителя информатики или инженера. Но работа по организации безопасности ПДн это работа не столько с техникой, сколько с документами и людьми, а значит разумнее, чтобы отвечал за нее заместитель руководителя. Оптимальным вариантом, нам представляется ситуация, когда над задачей в связке работают заместитель директора и технический специалист. К тому же, именно заместитель директора, а то и только сам директор, владеют информацией, о том, кто из сотрудников с какими персональными данными и с какими ИСПДн работает. После выпуска первых приказов, ответственный или, созданная рабочая группа, готовят вышеперечисленный набор документов. 2-я часть документации это набор перечней, положений и частная модель угроз. Эти документы разрабатываются один раз и надолго. Существенные изменения в них вносятся только в случае добавления ИСПДн или серьезных изменений в организационной структуре ОО. Эти документы разрабатываются в соответствии с образцами, спускаемыми из органов управления образованием или региональных министерств, занимающихся

информационными технологиями. 3-я группа документов состоит всего из двух документов, но зато требует большого объема организационной работы. Это согласие на обработку персональных данных и обязательство о неразглашении персональных данных. После того как эти документы разработаны, согласие необходимо взять у всех субъектов персональных данных – детей, педагогов и родителей. Обязательство о неразглашении подписывается всеми сотрудниками учреждения работающими с персональными данными. Все согласия и обязательства собираются и хранятся в бумажном виде в соответствующих папках и предъявляются проверяющим органам при необходимости. 4-я группа документов – Журналы, которые должны вестись круглогодично. Грамотно проведенная работа позволит, не только подготовить необходимый комплект документов для возможной проверки, но и серьезно настроить сотрудников, работающих с персональными данными и ввести персонифицированную ответственность за эти данные. С каждым годом все больше родителей знает требования к защите персональных данных (и ребенка и своих), а значит, ОО должна быть готова работать в ситуации жесткого прессинга по поводу автоматизированной обработки персональных данных со стороны родительской общественности.

2.3. Защита детей от доступа к негативной информации.

Закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью развитию», подписанный 29.12.2010 г. с поправками принятыми летом 2012 года. Вступление в силу закона активизирует разговоры о необходимости контроля учебным заведением предоставляемого учащимся контента. Безусловно, ОО уже давно работают в данном направлении, а первые системы контентной фильтрации были поставлены в ОО вместе с пакетом лицензионного программного обеспечения «Первая помощь 1.0» еще в 2007 году. Однако,

необходимо отметить, что зачастую ОО относятся к защите учащихся от нежелательного контента формально, ограничиваясь минимально требуемыми процедурами. С нашей точки зрения решение данной задачи должно идти по трем направлениям, взаимно дополняющим друг друга.

1. Разработка нормативных документов

2. Установка на компьютеры, к которым имеют доступ учащиеся, системы контентной фильтрации

3. Обучение учащихся правилам безопасной работы в сети Интернет

Если говорить о нормативной документации, то в данном направлении она немногочисленна и значительно менее регламентирована.
1. Необходимо выпустить приказ об ответственном за установку и поддержку системы контентной фильтрации.

2. В регламенте работы с сетью Интернет, обязательно должен быть раздел о правах и обязанностях учащихся.

3. Желательно создать памятку для учащихся о правилах работы в сети Интернет в ОО и ознакомить их с ней под роспись в специальном журнале.

4. Желательно завести журнал, в котором учителя бы фиксировали использование сети Интернет на своих уроках. Данный перечень документации не исчерпывающий, но достаточный для большинства ОО. Стоит еще сказать, что можно издать один общий приказ об ответственных за информационную безопасность ОО, в котором прописать ответственных по направлениям деятельности.

Системы контентной фильтрации, используемые в ОО России, делятся на два типа в соответствии с подходом к фильтрации ресурсов.

1. Системы с белым списком – доступ разрешен только в сайты из белого списка Это например, Интернет-цензор – разработан в Москве одним из лидеров на рынке интеллектуальных домов — системным интегратором «Интернет- дом» при содействии Фонда поддержки развития

общества «Наши дети». Белые списки составляются экспертами разработчика, с возможностью добавить или удалить сайт из этого списка. Проект предназначен, прежде всего, для родителей, однако сильно пропагандировался в ОО. Из недостатков можно отметить необходимость устанавливать программу на каждый конкретный компьютер Еще один пример, ТЫРНЕТ Прокси – разработан в Санкт-Петербурге, порталом Тырнет. Белый список составляется компанией Тырнет с помощью приглашенных экспертов. Устанавливается на сервер, через который в ОО настроен вход в сеть Интернет.

2. Системы с черным списком – доступ разрешен только во все сайты кроме сайтов из черного списка Основными системами являются программы разработанные московской компанией ЦАИР (Центр анализа Интернет-ресурсов) − СКФ – система поставленная в ОО с пакетом «Первая помощь 1.0», − NetPolice – более свежий продукт компании ЦАИР. Вообще ЦАИР наверное единственная компания, чьей основной специализацией является как раз создание систем Интернет-фильтрации различных уровней от домашнего до регионального.

Сами продукты позволяют организовать 2-х уровневый контроль

1. На уровне региона (по черному списку ЦАИР) 2. На уровне учреждения (дополнения в список по желанию учреждения, например социальные сети) Самый важный момент, что составляются черные списки с помощью экспертного педагогического сообщества с хорошей отлаженной системой с обратной связью. Нет однозначного ответа, какой из подходов лучше. Черные списки не дают 100% гарантии закрытия всех вредоносных сайтов, поскольку Интернет динамическая система в котором новые сайты появляются ежесекундно, в том числе и с вредоносным содержанием. Белые списки могут гарантировать, ребенок не увидит «плохие» сайты, однако затрудняет учебную работу и существенно ограничивает ресурсы сети Интернет. Необходимо отметить, что системы

контентной фильтрации в том или ином виде используются практически в 100% ОО России, что стимулируется регулярными проверками Прокуратуры РФ. Хуже всего дело обстоит с Обучением учащихся правилам безопасной работы в сети Интернет. По данному направлению нет рекомендованной учебной программы и нет предметов, в рамках которого эту программу можно было бы преподавать. Стоит надеяться, что подобный модуль может быть введен в данные предметы в ближайшее время.

Исходя из вышесказанного, были выделены основные угрозы в ОО:

· нарушение целостности информации;

· нарушение конфиденциальности информации;

· неавторизованный доступ;

· несанкционированный доступ.

На основании этого, наиболее эффективным путем для защиты информации в ОО будет применение программного комплекса.

Вывод по главе 2

Нельзя сказать, что проблема информационной безопасности может быть полностью решена в образовательных учреждениях. Связано это с несколькими ключевыми моментами:

− не выделено финансирование на работы по защите информации;

− нет единой политики информационной безопасности образовательных учреждений.

− администрации образовательных учреждений не всегда знает, что и как необходимо защищать.

Следует отметить, что только комплексная работа по всем вышеуказанным вопросам может привести к решению проблемы защиты информации и созданию безопасной информационной образовательной среды в ОО.

ГЛАВА 3. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЮЖНО-УРАЛЬСКОМ ГОСУДАРСТВЕННОМ ТЕХНИЧЕСКОМ КОЛЛЕДЖЕ (ЮУрГТК).

3.1. Анализ системы защиты информации в ЮУрГТК.

В ЮУрГТК почти все сотрудники имеют автоматизированное рабочее место. Используются компьютеры разных марок и комплектации. Компьютеры объединены в единую локальную сеть, существует разграничение прав доступа пользователей. Кроме того, все компьютеры подключены к сети Интернет, имеются в наличии межсетевые экраны.

Сотрудники поддерживают связь с другими организациями через Интернет, а именно: переписываются по электронной почте, ведут переговоры по телефонам.

Основным объектом защиты ЮУрГТК являются предоставленные сведения, составляющие коммерческую тайну и персональные данные сотрудников,учащихся

К таким объектам относятся:

1. Архив, в котором хранятся персональные данные обучающихся .

2. Архив, в котором хранятся персональные данные сотрудников и работников.

3. Бухгалтерия.

4. Архив данных с информацией, носящей обучающий характер, а также различные научные диссертации.

Большое количество занятий проходит с использованием компьютеров с выходом в Интернет и мультимедийного оборудования. Доступ учащихся к информационным ресурсам сети Интернет дает возможность учащимся пользоваться основным и дополнительным учебным материалом, необходимым для обучения, выполнять домашние

задания, самостоятельного обучаться. Благодаря таким ресурсам у учащихся появляется возможность узнавать о проводимых олимпиадах, конкурсах, и принимать в них активное участие.

Проанализировав информационную безопасность ЮУрГТК можно сделать вывод, что информационной безопасности уделяется недостаточное внимание:

- Отсутствует дополнительная защита файлов и информации (отсутствует элементарный запрос пароля при открытии или изменении информации в файлах, не говоря уже о средствах шифрования данных);

- В организации стоит не надежная программа по ограничению доступа к ресурсам информационно - телекоммуникационной сети «Интернет», не совместимых с образовательным процессом и способным причинить вред здоровью и развитию учащихся

- А также не достаточно сильная антивирусная программа, которая не обеспечивает полную защиту компьютеров от вредоносной информации и не регулярное ее обновление;

Все вышеперечисленное является очень важными недостатками обеспечения информационной безопасности данной организации.

Для решения этих проблем был рекомендован программный комплекс по защите информации.

3.2. Программный комплекс защиты информации.

Отправной точкой при разработке комплексной системы защиты информации ЮУрГТК , является ясное понимание роли и места системы защиты информации в деятельности ОО и в сфере обеспечения безопасности в целом. В ЮУрГТК используются большой объем информации. Безопасность ОО представляет собой своеобразную многоуровневую систему барьеров, включающих в себя такие меры, как установка различных типов сигнализации, организация наблюдения и

другие охранные процедуры. Кроме того, нельзя забывать, что при построении систем безопасности не должно оставаться «тонких» мест, и все компоненты системы должны быть сбалансированы, взаимосвязаны и согласованы. Ни одна современная система сигнализации, ни сверхчувствительные датчики не являются эффективными, если будет место человеческому фактору - не дисциплинированность, неумение, безответственность сотрудников. Можно утверждать, что ни одна система безопасности не застрахована от влияния человеческого фактора полностью. Но современная интеллектуальная система безопасности должна сводить это влияние к минимуму. Чем меньше возможность человека влиять на систему, тем ниже роль ошибок в безопасности информации. С каждым годом технические возможности злоумышленников расширяются. Соответственно, системы безопасности должны всегда быть в развитии на шаг вперед. Следовательно, необходимо стремиться сразу, строить такую систему безопасности, которая со временем не устареет, и с возможностью при необходимости её модернизировать, «нарастить» до более совершенного уровня. Система так-же должна сохранять целостность данных даже при форс мажорных обстоятельствах, включая природные катаклизмы, пожары, саботаж, прочие действия потенциальных злоумышленников и другие факторы, так или иначе нарушающие работу системы. Защита будет прочной, если будет комплексной.

Поэтому в ЮУрГТК было предложено использовать разные программные средства защиты информации, а некоторые старые заменить на более сильные.

-*Средства шифрования* - аппаратные, программные ипрограммно-аппаратные шифровальные (криптографические) средства, реализующие а лгоритмыкриптографического преобразования информации для ограничен ия доступа к ней, в том числе при ее хранении, обработке и передаче.

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств - универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

- *Фильтр SkyDNS для учебных заведений (Рис.2)*.

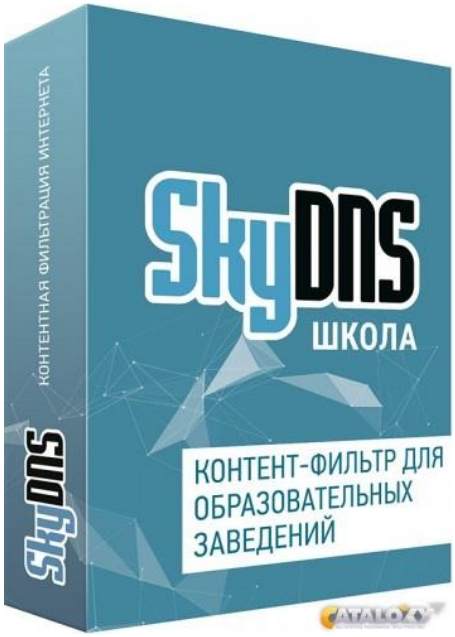

Рис.2

Аппаратная версия контент-фильтра на базе роутеров ZyXEL Keenetic. Совместно с компанией ZyXEL создан инновационный продукт для администраторов сетей учебных заведений и библиотек — аппаратный контент-фильтр SkyDNS Z. В него входят специальный тариф контент-фильтра SkyDNS Школа Z с расширенными возможностями и интернет-шлюз ZyXEL Keenetic со встроенным модулем контент-фильтрации. Преимущества SkyDNS Z очевидны — с приобретением этого комплекта значительно упрощается внедрение интернет-фильтрации и управление ее настройками.

- *Антивирусная программа Kaspersky CRYSTAL 3.0(Рис.3)*

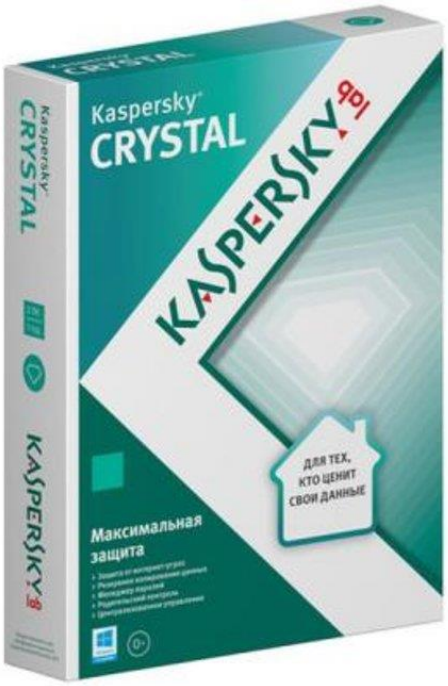

Рис.3

Пакет **Kaspersky Crystal** включает в себя как самый полный набор антивирусных функций, так и возможность осуществлять контентную фильтрацию.

- *VPN (виртуальная частная сеть)* (Рис.4) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

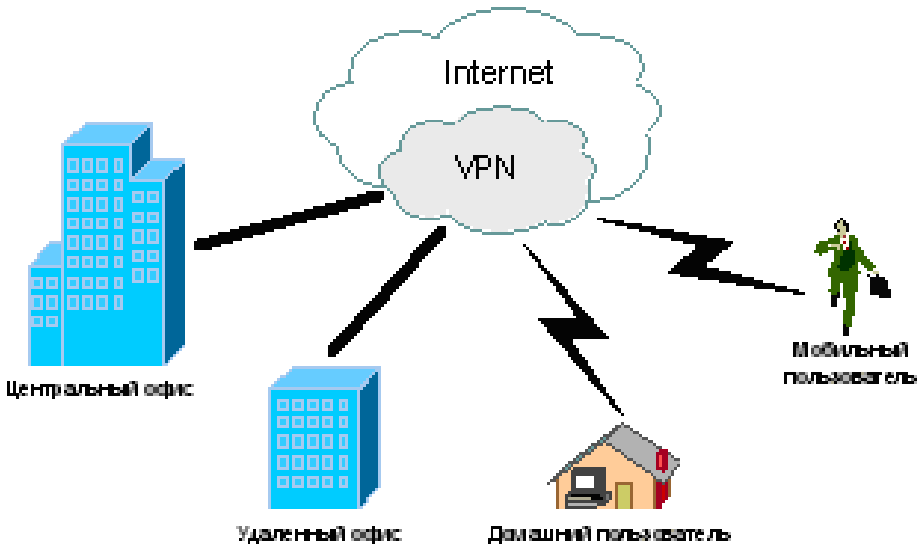

Рис.4

- *Лицензионные версии операционных систем Microsoft Windows XP (Рис.5) и Microsoft Windows Vista.(Рис.6)*

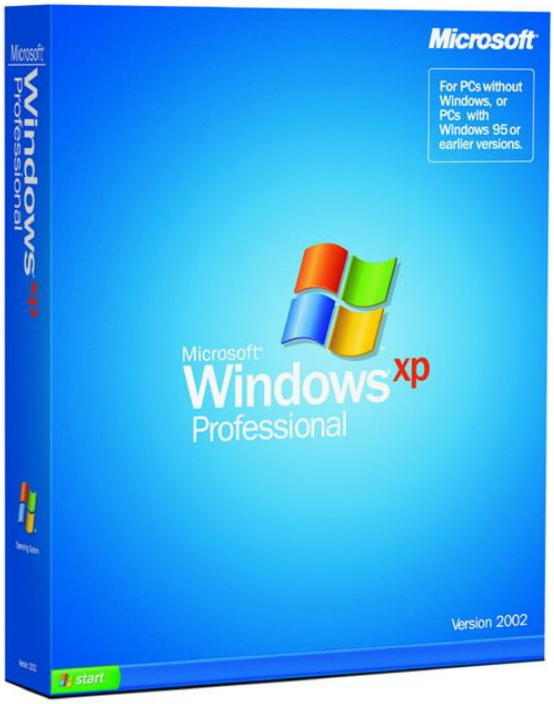

Рис.5

Microsoft Windows XP (Рис.5) - операционная система семейства Windows NT корпорации Microsoft. Была выпущена 25 октября 2001 года и является развитием Windows 2000 Professional. Название XP происходит от англ. experience (опыт). Название вошло в практику использования, как профессиональная версия.

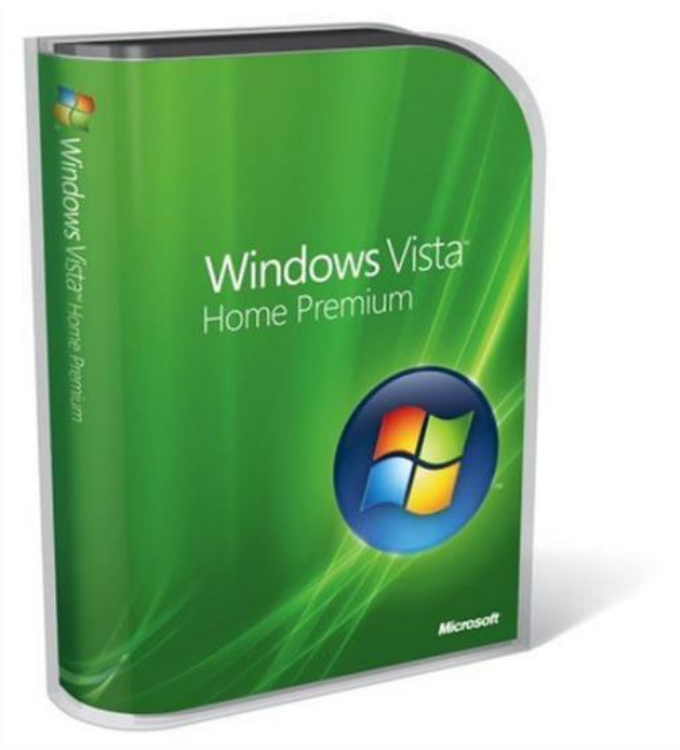

Рис.6

Microsoft Windows Vista (Рис.6).- операционная система семейства Microsoft Windows NT, линейки операционных систем, используемых на пользовательских персональных компьютерах. В линейке продуктов Windows NT Windows Vista носит номер версии 6.0. Для обозначения «Windows Vista» иногда используют аббревиатуру «WinVI», которая объединяет название «Vista» и номер версии, записанный римскими цифрами.

- *Интернет-браузеры «Opera 10.62» и «Internet Explorer 6.0».*

Веб-браузер и программный пакет для работы в Интернете, выпускаемый компанией Opera Software. Разработан в 1994 году группой исследователей из норвежской компании Telenor. С 1995 года продукт компании Opera Software, образованной авторами первой версии браузера.

Браузер написан на языке программирования C++, обладает высокой скоростью работы и совместим с основными веб-технологиями.

Отличительными особенностями Opera долгое время являлись многостраничный интерфейс (система вкладок в окне программы) и

возможность масштабирования отображаемых документов целиком, вместе с графикой; впоследствии эти функции появились и в других браузерах. В Opera расширены функциональные возможности использования мыши: кроме стандартных способов навигации предусмотрены так называемые «жесты мышью».

Internet Explorer 6.0 - наиболее распространенный веб-браузер в мире, созданный для удобной и комфортной работы пользователей Интернета. Считается самым простым, безопасным и быстрым в работе. Браузер способен оптимизировать возможности пользователей и разработчиков во время работы с веб-службами. Обозреватель Internet Explorer обладает новыми функциональными возможностями, благодаря которым навигация по веб-страницам стала более быстрой, простой и безопасной. Internet Explorer имеет простой и лаконичный интерфейс, позволяющий пользователям освоить программу за максимально короткое время.

- *Программное обеспечение защиты информации «Secret net 6»(Рис.7)*

Рис.7

Система защиты информации Secret Net 6.5-C (сетевой вариант) интегрируется с доменом Microsoft Active Directory и дополняет своими защитными механизмами стандартные средства обеспечения информационной безопасности операционных систем семейства Microsoft Windows.

Реализация предложенных мероприятий и средств позволит:

- Разграничить права доступа в систему.
- Повысить уровень защищенности информации каждого пользователя в отдельности и системы в целом.
- Уменьшить количество спама.
- ограничить доступ к ресурсам информационно - телекоммуникационной сети «Интернет», не совместимых с образовательным процессом и способным причинить вред здоровью и развитию учащихся
- Отражать вредоносные атаки через сеть.
- Повысить уровень защиты ПД.

Вывод по главе 3

Основные выводы о способах использования рассмотренных выше средств, методов и мероприятий защиты, сводится к следующему:

1. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации.
2. Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.
3. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.

4. Необходимо осуществлять постоянный контроль функционирования механизма защиты.

Заключение

Использование современных технологий управления информацией на основе связанных между собой систем управления базами данных, позволяет осуществлять подобные операции в автоматическом режиме. Вмешательство человека требуется только на этапах ввода исходной информации и формирования запроса на предоставление информации. В то же время, невозможно построить универсальную систему, которая вмещала бы в себя все существующие на сегодняшний день возможности и функции управления информацией. Одним из вариантов решения данной проблемы является организация единого операционного пространства с помощью специализированной электронной оболочки, способной интегрировать различные программные компоненты и виды данных. К рассматриваемым видам данных следует отнести: бумажные документы, файлы данных различных форматов, электронные документы, аудио и видео материалы, базы данных, приложения для работы с электронными документами, информационные ресурсы Интернет и другие. В частности, всякая информационная система, для которой определены механизмы автоматического входа-выхода, также может рассматриваться как информационный ресурс. Каждое учебное заведение имеет свои особенности и механизмы управления, которые необходимо учитывать при создании системы.

В ходе данной работы рассмотрены основные нормативные документы, регулирующие правовые отношения в области защиты информации, приведены сведения о возможных угрозах безопасности информационной системе, в том числе подробно приведена и рассмотрена характеристика угроз несанкционированного доступа. При рассмотрении угроз, особое внимание уделялось классификации нарушителей

безопасности, поскольку они выполняют доминирующую роль в нарушении безопасности информационной системе.

Особое внимание уделено основным компонентам для построения защищённой информационной системы. Подробно рассмотрены организация хранения информации в базе данных, классификация программного обеспечения и основные средства защиты локальной сети, приведены организационные меры защиты.

Единого рецепта, обеспечивающего 100% гарантии сохранности данных и надёжной работы сети, не существует. Однако создание комплексной, продуманной концепции безопасности, учитывающей специфику задач конкретной организации, поможет свести риск потери ценнейшей информации к минимуму.

Практически любую информацию можно защитить, если пользователь пожелает это сделать, сохранив ее таким образом. В скором будущем компьютеры заменят многие привычные сейчас вещи, следовательно, нам придется доверить компьютеру самое сокровенное, которое человек никогда в жизни не доверит другому человеку, поэтому потребуется более надежная защита информации, такая, что тайны человека смогут лишь узнать, в крайнем случае, после его смерти. Человечество надеется, что компьютер станет другом, которому можно будет сказать все, зная, что он никогда сам не раскроет их тайны.

Обеспечение информационной безопасности достигается только при комплексном использовании всех средств защиты информации - организационные, физические, социально-психологические мероприятия и программном - технические средства защиты. Исходя из проделанной работы можно сделать вывод, что программные средства защиты информации играют большую роль в обеспечении информационной безопасности образовательной организации.

Список использованной литературы

1. Абдеев Р.Ф. Философия информационной цивилизации. М.: ВЛАДОС, 1994 .-336с.

2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах:Учеб.пособие для студ. высш. учеб. заведений/Павел Борисович Хорев.–М.:Издательский центр «Академия», 2005.–256с.

3. Скиба В.Ю. Курбато В.А. Руководство по защите от внутренних угроз информационной безопасности/Скиба В.Ю. :Питер.–2008..-320с.

4. Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. Защита информации в компьютерных системах и сетях. М: "Радио и связь", 1999. – 328

5. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 25.07.2011) "О персональных данных"

6. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.04.2011, с изм. от 21.07.2011) "Об информации, информационных технологиях и о защите информации"

7. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 19.07.2011)

8. Алексеева И.Ю. Человеческое знание и его компьютерный образ. -М.,1993.- 218 с.

9. Баева И. А. Психологическая безопасность образовательной среды: теоретические основы и технологии создания. Дисс. д. пед. наук СПб., 2002.-с.244

10. Бекасова С. Н. Информационные потребности студентов как фактор профессионального и личностного развития. (На материале цикла педагогических дисциплин.) /Автореф. дис. к. п. н. СПб. -1999, с. 24

11. Белов Г. В. Некоторые проблемы системологии информационного права. Материалы всероссийской научно-практической конференции «Информационное право: информационная культура и информационная безопасность» , СПб., 2002. С. 10 – 13

12. Беспалько В. П. Основы теории педагогических систем. Воронеж: Издательство Воронежского университета, 1977.- 240 с.

13. Василенко Л.А. Интернет в информатизации государственного управления (социолого-методологический анализ).- /Автореф. дис. д. социол. наук. М.,2000.- 54 с.

14. Василенко Л.А. Интернет и проблема обеспечения информационной безопасности. Тезисы международной научно-практической конференции «Анализ систем на рубеже тысячелетий».М.,1998. С.23

15. Василенко Н. В. Интеграция знаний на основе использования новых информационных технологий в общеобразовательной школе: Дисс. к. пед.н. СПб., 2001.-202 с. /с прилож./

16. Белов С.А. Понятие «информационная компетентность», её компонентный состав, свойства и функции /С.А. Белов// Непрерывное образование как ресурс развития региона: сборник статей Всеросийской науно-практиекой конференци с международным участием (май-октябрь 2011.г. Барнаул, Россия).- Т.1.:профессиональное образование.- Барнаул: АЗБУКА, 2011.- С.110-114

17. Вендровская Р. Б. О компьютерах и компьютеризации образования // Педагогика, 1998, № 4. С. 120 -121.

18. Вершловский С. Г. и др. Эффективная школа. СПб.: ЦПИ, 1995,- 123 с.

19. Веряев А.А. Семиотический подход к образованию в информационном обществе. Монография. Барнаул: Изд-во БГПУ, 2000.- 298 с.

20. Водопьян Г.М. «Прозрачная» школа и Интернет. Расширение образовательного пространства. // Тез. Докладов Международной конф. «Российская школа и Интернет» 18-19 сентября 2001 г., СПб., 2001,- С. 61-62

21. Войскунский А.Е., Бабаева Ю.Д., Смыслова О.В. Интернет и личность . Санкт-Петербург. // Тезисы докладов Международной конференции «Интернет.Общество.Личность»,1999. 376 с.

22. Гнатышина, ЕА. Управление инновационными процессами в учреждениях профессионально-педагогического образования : учеб.-методическое пособие / ЕА. Гнатышина; Челяб. гос. пед. ун-т. - Челябинск: Изд-во ЧГПУ, 2006. - 68 с.

23. Вуе М. А. Информационная безопасность: цивилизованный аспект и человеческое измерение.//Материалы научно-практической конференции «Информационная безопасность школьников: состояние, проблемы, перспективы» 28 30 апреля 2003 г., СПб., 2003.- С. 6- 17.

24. Гейн А. Г. Изучение информационного моделирования как средства реализации межпредметных связей информатики с дисциплинами естестественнонаучного цикла /Автореф. дис. д. пед.наук М.: 2000.- 47 с.

25. Гессен С. И. Основы педагогики. Введение в прикладную в философию. -М.: Школа- Пресс, 1995. -448 с.

26. Говорунов А.В. Человек в ситуации виртуальной реальности/ Технологии информационного общества Интернет и современное общество: Материалы Всероссийской объединенной конференции. Санкт-Петербург, 20-24 ноября 2000 г. - СПб.; 2000. - 292с.

27. 51. Джуди Хейм . Советы по Internet. Научите своих детей безопасным прогулкам по Internet. Мир ПК • № 1, 1998,- С. 112-113

28. Доктрина информационной безопасности РФ.// «Безопасность», № 1-12, С. 191-22

29. Домозетов Х. Компьютеризация и проблемы здоровья, свободы и безопасности личности // Философская и социологическая мысль, 1991, № 4, С.93-99

30. Еремин А. Информация и здоровье. Краснодар, 2001,- 163 с.

31. Ершов А.П. Информатизация: от компьютерной грамотности учащихся к информационной культуре общества // Коммунист, 1988, №2 2, С.82-92.

32. Гнатышина, ЕА. Инновационный подход к формированию профессиональной компетентности педагогов профессионального обучения / ЕА. Гнатышина // Наука / Кост. инжекерно-экон. ун-т им. М. Дулатова. - Костанай, 2007. - № 1. — С. 42-48.

33. Заболотский В.П., Иванов В.П., Лазарев В.М. Информационные потоки и их влияние на социокультурное развитие. //Материалы конференции

34. Закон об информации, информатизации и защите информации // Российская газета, 22 февраля 1995 г.65.Запесоцкий А. С. Образование: философия, культурологи, политика. — М.: Наука, 2002.-456 с.

35. Игнатьев М.Б, Пятина Е.О, Шейнин Ю.Е. Информационное общество - парадигмы и базовые технологии. Санкт-Петербург. Тезисы докладов Международной конференции «Интернет. Общество. Личность», 1999.- 376 с

36. Иезуитов А.Н. Философские основы информационной безопасности: теория и практика. //Материалы конференции «Информационная безопасность регионов России. ИБРР-2001, Спб, 26-29 ноября 2001 г. Том 2.-С.64-68

37. Извозчиков В.Н. Слово об информации (о концепции нового спецкурса «Введение в информологию»)// Наука и школа, 2000.№ 1. С.34-44

38. Ионов А. С. , Н. В. Баскакова Н. В. Оценка достоверности информации в Интернет с помощью комплексной логики. Тезисы докладов Международной конференции «Интернет. Общество. Личность»,1999.- С. 325-326

39. Калугина Т.А., Мельникова Н.И., Хамидуллин Ф.З. Образ Интернет в средствах массовой информации// Интернет и современное общество: Тез. докл. II Всероссийск. науч.-метод. конф., 29ноября-3 декабря 1999 г., Санкт-Петербург, С. 45

40. Каптелинин В. Н. Психологические проблемы формирования компьютерной грамотности школьников. Вопросы психологии, № 5, 1986 .-С.54-65

41. Колин К.К. Социальная информатика научная база постиндустриального общества // Социальная информатика-94. М., 1994. - 336 с.

42. Компьютер в школе: диктатор или помощник?/ Литературная газета. 1986.- 17 мая.

43. Конаржевский Ю.А. Менеджмент и внутришкольное управление/ М.: центр «Педагогический поиск», 2000.-224 с.

44. Конституция Российской Федерации. Принята 12 декабря 1993 г. -«Проспект», 1999.-48 с.

45. Концепция информационной безопасности РФ (проект) М. 1994, С.40.

46. Концепция национальной безопасности РФ. 17 декабря 1997 г. //Информационный сборник «Безопасность». № 1-12, 2000.- С. 155- 190

47. Корсунцев И.Г. Субъект деятельности и информационные технологии: философско-методологический анализ. /Автореф. дис. д. филос. наук. М.,2000. 53 с.

48. Кузнецов В.Н. Культура безопасности. Тезисы к докладу «Культура безопасности в трансформирующемся обществе». М.: октябрь 2002// Безопасность Евразии, № 1-2002, январь-март.- С.126-141

49. Лопатин В. Н. Проблемы правовой охраны и защиты интеллектуальной собственности в России. //Материалы конференции «Информационная безопасность регионов России. ИБРР-2001, Спб, 26-29 ноября 2001 г. Т.2. -С.77

50. Ляпуров В., Узуев А. Опыты раскрытия информации в США // Компьютерра, 1998, №6. С.46-49

51. Майкл Бэнкс. Психи и маньяки в Интернете. Руководство по выживанию в киберпространстве. Пер. с англ. - Издательство «Символ-Плюс» Санкт-Петербург, 1998 . - 320 с.

52. Машарова Т.В. Теория и практика социального самоопределения подростка в учебной деятельности. /Автореф. дис. д. пед. наук. Ярославль, 1999.-38 с.

53. Медведева Е.А. Основы информационной культуры (программа курса для вузов) // Социс.-1994.- №11.- С.59.

54. Мельников Е.А. Негативно влияющая информация в интернет. Санкт-Петербург. Тезисы докладов Международной конференции «Интернет. Общество. Личность».-1999. 376 с.

55. Моисеев Н.Н. Человек. Среда. Общество.-М.: Наука, 1982.-312 с.

56. Наумов В.Б. Особенности правового регулирования сети Интернет // Интернет и современное общество: Тез. докл. Всеросс. научно-метод. конф. СПб, 7-11 декабря 1998 г.- СПб, 1998. С.51-53.

57. Новиков А. М. Методология образования. М.: «Эгвес», 2002.-320 с.

58. Орехов А.М. Информатизация общества информационное общество // Социальная информатика-93.- М., 1993. - С.32-35.

59. Парфенов В.Г. Подготовка компьютерщиков-профессионалов./ Компьютерные инструменты в образовании.№ 3,СПб, 1998.- С. 84

60. Петров С. Т. На пути к информационному государству. //Информационное общество. -1999!-№4.-С. 64-65

61. Пиявский С.А., Д.К.Жиганов. Формирование потребности в интернет у одаренной молодежи. Информационное общество парадигмы и базовые технологии. СПб., Тезисы докладов Международной конференции «Интернет. Общество. Личность»., 1999. - С. 376

62. Поздняков А.И. Информационная безопасность личности, общества, государства // Военная мысль, 1993, № 10.- С.89

63. Пола Статмэн. Безопасность вашего ребенка. СПб.: Дельта. 1996. -382 с.

64. Проблемы информатизации , № 3/4,1993.- С.81-88

65. Программы для общеобразовательных учреждений. Информатика. -Министерство общего и профессионального образования Российской Федерации. М.: "Просвещение", 1998.- 143 с.

66. Роберт И.В. Современные информационные технологии в образовании. М.: Школа-Пресс, 1994.-41 с.

67. Робертсон Д.С. Информационная революция // Информационная революция: наука, экономика, технология: Реферативный сб./ ИНИОН РАН. М., 1993, С.17-26.

68. Сальников В.П. Информационная безопасность в системе составляющих безопасность РФ //Материалы конференции «Информационная безопасность регионов России.ИБРР-2001 26-29 ноября 2001 г. Т. 2, Спб.- С.29

69. Саттарова Н. И. Учитель информатики рекомендует//Компьютерные инструменты в образовании. СПб., 2000. - № 2-3. - С. 129-133.

70. Саттарова Н. И. Обеспечение информационной безопасности детей, использующих Интернет // Сборник трудов Первой Всероссийской научно-практической конференции «Российская школа и Интернет» 18-19 сентября 2001 СПб.-С. 151-152

71. Саттарова Н.И. Обеспечение правовой и психологической безопасности детей, использующих Интернет. Тезисы докладов IIIмежрегиональной научно практической конференции «Информатизация образования на современном этапе» 21 июня 2001 г., СПб., 2001.- С. 2

72. Саттарова Н.И. К вопросу об информационной безопасности школьников // Информационные и коммуникационные технологии в образовании: Межвузовский сборник научных трудов. СПб.: Изд-во БАН, 2002.- С.90-92

73. Саттарова Н.И. Модели обеспечения информационной безопасности школьников.//Материалы научно-практической конференции «Информационная безопасность школьников: состояние, проблемы, перспективы», 28 30 апреля 2003 года, СПб, 2003.- С. 102-103.

74. Семенов А.JT. Образование, информатика, компьютеры// Информатика и образование. 1995.№ 5.- С. 6-11

75. Смольникова И.А. Информационные технологии и образование // Социальная информатика 95.- С.51-64

76. Сыренский В.И. Психофизиология информационной безопасности школьника. //Материалы научно-практической конференции «Информационная безопасность школьников: состояние, проблемы, перспективы», 28 30 апреля 2003 года, СПб, 2003.- С. 30-32

77. Уваров А. Ю. ИНТЕРНЕТ В ШКОЛЕ: СМЕНА ПАРАДИГМЫ http://center.fio.ru/vio/VIO01 /Articlel 6.htm

78. Урсул А. Д. Обеспечение безопасности через устойчивое развитие.//Безопасность Евразии, №1-2001, январь март, 2003.- С.457-461

79. Федеральная целевая программа "Развитие единой образовательной информационной среды (2001-2005 гг.)"

80. Чупаха И.В., Пужаева Е.З., Соколова И. Ю. Здоровьесберегающие технологии в образовательно-воспитательном процессе. Научно-практический сборник инновационного опыта. М.: Илекса, Ставрополь: Ставропольсервисшкола, 2001,- 400 с.

81. Элиасберг Н.И. Гуманистические основы правового образования в школе: Дис. д.пед.наук.-СПб., 1998.- 462 с.

82. Эстер Дайсон . ЖИЗНЬ В ЭРОХУ ИНТЕРНЕТА: Release 2.0. Пер. с англ. Под редакцией А.В. Евтюшкина и Ю.А.Кузьмина // М.: «Бизнес и компьютер», 1998.- 400 с.

83. Якушина Е.В. Необходимость моделирования обучения подростков работе в Интернете. Материалы Первой Всероссийской научно-практической конференции «Российская школа и Интернет». 18-19 сентября 2001 года. -СПб. С.86

84. Яновский Р. Г. Глобальные изменения и социальная безопасность. М., 1999.- С.39

85. Ярочкин В. И. Информационная безопасность. Учебное пособие для студентов вузов. — М.: Междунар. отношения, 2000.- 400 с.