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
Анохина Елена Дмитриевна
Научный руководитель:
зав.кафедрой АТИТиМОТД ППИ
к.т.н, доцент
Руднев Валерий Валентинович

Проверка на объем заимствований:
____76,5_____% авторского текста

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

Челябинск 2017

ОГЛАВЛЕНИЕ

Введение

Обеспечение, создание и управление информации организация службы безопасности образования является одним из основных направлений информатизации и, в целом, функционированием образовательной организации. Информационная безопасность является обязательным условием и одним из критериев эффективности образовательной организации.

В федеральных нормативных документах словосочетание "Информационная безопасность" не используется, используются такие понятия, как "безопасность информации", "доступ к информации", "конфиденциальность", и другие. В руководстве в разделе "Информационная безопасность образовательной организации" мы имеем в виду состояния защиты персональных данных субъектов образовательного процесса, учащихся от информации, причиняющей вред их здоровью и развитию информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Системы информационной безопасности в образовательной организации включает следующие компоненты:

1. Нормативно - специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

2. Организационные - это регламентация производственной деятельности и взаимоотношений исполнителей на правовой основе, исключающей какой-либо ущерб;

3. Программного обеспечения и аппаратных средств является использование различных алгоритмов, программного обеспечения и оборудования, предотвращение ущерба. Следует отметить, что необходимым условием для функционирования системы безопасности образовательной организации является проведение мероприятий для учителей, учащихся и родителей, с

целью развития компетенций, связанных с работой на компьютере устройств, поиск и обработка информации в Интернете, защищены от "вредной" информации.

В систему информационной безопасности образовательной организации можно выделить следующие направления:

— организация фильтрации Контента из Интернета на компьютерные устройства, используемых студентами;

— обеспечение антивирусной защиты и других угроз из Интернета, компьютеров и мобильных устройств локальной сети организации;

— обеспечение защиты персональных данных субъектов образовательного процесса; организация добросовестное использование авторских прав.

Современное развитие мировой экономики характеризуется ростом рынка зависимость от значительного объема информационных потоков. Несмотря на возрастающие усилия по созданию технологий защиты данных, их уязвимость не только не уменьшается, но и растет. Поэтому актуальность вопросов, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач.

Например, конфиденциальность данных, которая обеспечивается применением различных криптографических методов и средств (шифрование закрывает данные от посторонних лиц, а также решает задачу их целостности); идентификация пользователя на основе анализа кодов, используемых их для подтверждения своих прав на доступ в систему (сеть) для работы с данными и изменять их (обеспечивается введением соответствующих паролей, анализ электронной подписи).

Перечень аналогичных задач по защите информации и информационной безопасности в современных системах обработки и передачи данных может быть продолжен. Это также должно быть обусловлено быстрым развитием в техническом и программном обеспечении информационных технологий в связи с прогрессом в области микроэлектронных технологий и появлением новых многопроцессорных систем обработки данных. Как следствие, расширена функциональность и повышенный "интеллект" средств обработки и передачи данных, а также технические средства, используемые для защиты информации.

Актуальностью информационной безопасности свидетельствует тот факт, что персональный компьютер или рабочая станция является частью систем обработки информации, систем коллективного пользования, вычислительных сетей. В таких случаях предъявляются жесткие требования по надежности и достоверности передаваемой информации. Любой канал связи характеризуется наличием шума, что приводит к искажению информации, поступающей на обработку. Для уменьшения вероятности ошибок принимается ряд мер, направленных на улучшение технических характеристик каналов с использованием различных видов модуляции, расширение мощностей и т. д. также должны быть приняты для защиты информации от ошибок или несанкционированного доступа.

Доступ может использовать информацию, хранящуюся в ЭВМ (системе).

Вся информация в машине или системе требует особой защиты, то есть совокупность методов, позволяющих управлять доступом к системе программ к хранящейся информации.

Защита-это любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу.

Общие вопросы информационной безопасности посвящены в работах таких ученых, как В.В.Домарев, В.А. Галатенко, С. М. Доценко, В.Ф. Шпак, В.И.

Ярочкин, А. Володин, Б. Байбурин, А. В. Петраков, А. Ю. Щербаков, Е. Б. Белов, А. А. Малюк и др.

Информационно-образовательной организации безопасности посвящены работы Р. И. Конеев, А.В. Беляева, В. Ю. Скибы, В. А. Курбатов, А. Игнатьев, И. М. Петров, С. А. Кузьмин, Одинцов А. А. и других авторов.

Технические стороны информационной безопасности отражены в работах А. П. Тимофеев, А. В. Соколов, Г. Н. Устинова, В.Г. Проскурин, С. А. Маркова,

О. Ю. Макаров и другие

Информационная безопасность государства представлено в работах А. А. Стрельцова, Ю.С. Уфимцева, Н. В. Лопатин, И. Н. Панарин, Е. А. Ерофеева, В. Г. Шевченко, И. Ю. Алексеевой, И.В. Овчарова, Д. С. Сатрина и другие.

Изучив на начальном этапе исследований различной педагогической и учебно-методической литературы, а также анализа состояния изучаемой проблемы, мы сформулировали объект исследования.

Объектом исследования- является информационная безопасность.

Предметом исследования - является влияние антивирусных программ в области информационной безопасности в образовательной организации.

Цель исследования: анализ и систематизация материалов по информационной безопасности в образовательных организациях.

Задачи исследования:

1. Выбрать и проанализировать литературу по теме исследования
2. Охарактеризовать понятие «информация», изучить ее основные свойства.
3. Описать виды "опасная" информация.
4. Для систематизации методов защиты, анализировать преимущества и недостатки антивирусных программ.

5. Разработать методическое приложение для использования материала в практике образовательных организаций.

Гипотеза: Если в процессе учебно-воспитательной организации включает в себя создание и управление информационной безопасностью.

Информационная безопасность в образовательных организациях является эффективной.

Методы научного исследования:

Теоретические: анализ научной и научно-методической литературы.

Диссертационное исследование построено на основе фундаментальных теоретических положений социологии управления, теории информационной безопасности.

В исследовании использовались такие социологические методы исследования, как наблюдение, а также общенаучные методы: анализ, синтез, анализ информации, системный подход, сравнение, обобщение.

Глава 1. Теоретические основы создания и управления информационной безопасности в образовательной организации

1.1. История развития информационной безопасности

Согласно информации, в рамках его создания и управления, а также защита ссылается на сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. В зависимости от формы представления информация может быть речевой, телекоммуникационной, документальной.

Информационные процессы - процессы сбора, накопления, обработки, хранения, распространения и поиска информации.

Информационная система - совокупность документов и массивов документов и информационных технологий.

Наименование информационных ресурсов, документ или массив имеющихся документов либо отдельно, либо как часть информационной системы.

Процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства называется информатизация.

Информатизация делится на открытую и с ограниченным доступом.

Информация является одним из объектов гражданских прав, включая права собственности, владения, пользования. Собственник информационных ресурсов, технологий и систем - субъект с правом владения, пользования и распределения этих объектов. Владелец ресурсов, технологий и систем-субъект с полномочиями владения, и пользования таких объектов. Пользователь относится к компании, которая получает доступ к информационной системе за получением нужной информации и ее использования.

К защищаемой информации относится информация, которая является предметом собственности и подлежит защите в соответствии с требованиями правовых документов или требованиями владельца информации.

Под утечкой понимают неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа и получения данных.

Несанкционированный доступ-получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

Несанкционированное воздействие на охраняемую информацию, последствий нарушения правил (например, заменой электронных документов). Под непреднамеренным воздействием на защищаемую информацию понимается воздействие на нее из-за ошибки пользователя, сбоя оборудования или программного обеспечения, природных явлений и других непреднамеренных последствий (например, уничтожение документов на жестком диске).

Целью защиты информации является предотвращение причинения вреда пользователю, владельцу или собственнику. Под эффективностью защиты информации- понимается степень соответствия результатов защиты цели. Объектом защиты может быть носитель информации, информационный процесс, в отношении которых он должен быть защищен в соответствии с поставленными целями.

Конфиденциальность информации является знание его содержания только имеющим соответствующие полномочия.

Шифрование информации - это преобразование информации в результате, которого содержание информации является непонятным для субъекта, не имеющих соответствующий доступ. Результат шифрования называют шифротекстом.

Под угрозой информационной безопасности в компьютерной системе понимают события или действия, которые могут вызвать изменения функционирования КС, связанные с нарушением безопасности информации, обрабатываемой в нем.

Уязвимость информации - это возможность на любом этапе жизненного цикла КС такого ее состояния при котором создастся условия для реальной угрозы безопасности в ней

Нападение - это действия преступника в поиске информации и использовании той или иной уязвимости.

Угрозы могут быть разделены на угрозы, независимым от человеческой деятельности и искусственным угрозам, связанные с человеческой деятельностью. Искусственные угрозы, в свою очередь, делятся на непреднамеренные (ошибки в проектировании, ошибки в программном обеспечении) и преднамеренные (несанкционированный доступ, несанкционированное мероприятие). Результатом реализации угроз могут быть утечка, искажение или потеря информации.

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, которые должны быть включены в состав и выполняющие (как самостоятельно, так и с помощью программного обеспечения) некоторые функции обеспечения информационной безопасности.

К основным аппаратными средствами защиты информации относятся: устройства ввода идентифицирующий пользователя информации; устройства шифрования информации; устройства для предотвращения несанкционированного включения рабочих станций, серверов.

В рамках обеспечения информационной безопасности понимают специальное программное обеспечение, которое входит в состав программного обеспечения КС исключительно для выполнения защитных функций. Основные программные средства защиты информации включают: определение программы, аутентификации пользователей КС; программы доступа пользователей к ресурсам КС; программы от несанкционированного доступа, копирования, изменения и использования.

Идентификация пользователей в отношении безопасности КС, включает однозначное четкое распознавание уникального имени субъекта КС. Проверка подлинности означает подтверждение того, что представленное название соответствует заданному вопросу.

В онлайновом словаре Мерриама-Вебстера (Merriam-Webster) дается следующее определение информации:

сведения, полученные при исследовании, изучении и обучении;

известия, новости, факты, данные;

команд или символов для представления данных (в системах связи или в компьютере);

знаний (экспериментальных данных, изображения), изменение концепции в результате физического или психического опыта.

Безопасность определяется следующим образом как: свобода от опасности, сохранность; свобода от страха или беспокойства.

Если мы объединим эти два понятия вместе, то мы получим определение информационной безопасности - меры, принятые для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним.

Как следует из определения, Информационная безопасность не обеспечивают абсолютную защиту. Вы будете строить сильную крепость в мире - и тогда будет кто-то с еще более мощной оперативной памяти.

Информационная безопасность - это меры предосторожности, чтобы защитить информацию и оборудование от угроз и уязвимостей.

Способы защиты информации и других ресурсов постоянно меняются, как меняется наше общество и технологии. Это очень важно понимать, что для того, чтобы выработать правильный подход к безопасности. Итак, давайте посмотрим на свою историю, чтобы не повторять прошлых ошибок.

На заре цивилизации ценные знания были сохранены в материальной форме: высеченные на каменных скрижалях, позднее записанные на бумаге. Для защиты они использовали те же материальные объекты: стены, рвы и охранников.

К сожалению, физическая защита имеет один недостаток. Сообщение захвата, враги знали, что в ней написано. Юлий Цезарь решил защитить ценные данные в процессе передачи. Он изобрел шифр Цезаря этот шифр позволял посылать сообщения, которые никто не мог прочитать в случае перехвата.

Эта концепция была разработана во время Второй мировой войны. Германия использовала машину под названием Enigma для шифрования Сообщений, отправляемых воинскими частями.

Немцы считали, что машина "Энигма" было практически невозможно взломать. Это действительно будет очень трудно взломать - если бы не ошибки, что позволило союзникам читать некоторые сообщения. В военкомате обычно используются кодовые слова для обозначения географических мест и воинских частей. Япония заменила имена кодовых слов, так что понять их послание было очень сложно, даже после взлома кода шифрования.

Если не считать ошибок в использовании системы шифрования, программный комплекс шифрования очень трудно взломать. Таким образом, был постоянный поиск других способов перехватывать информацию, передаваемую в зашифрованном виде.

В 1950 году было установлено, что доступ к отчетам осуществляется через анализ электронных сигналов, возникающих при передаче по телефонным линиям. Работу любых электронных систем сопровождается излучением, в том числе телетайпов и блоки шифрования, используемые для передачи зашифрованных Сообщений. Блок шифрования посылает зашифрованное сообщение по телефонной линии, и вместе с ней передается и электрического сигнала из исходного сообщения. Поэтому, если у вас есть хорошее оборудование, исходное сообщение может быть восстановлено.

При передаче сообщений по телеграфу было достаточно, обеспечить защиту коммуникаций и радиации. Потом пришли компьютеры, которые были переведены в электронный формат информационных ресурсов организации. Через какое-то время для работы на компьютерах стало легче, и многие пользователи научились общаться с ними в режиме интерактивного диалога. Информация теперь может применяться для любого пользователя, вошедшего в систему. Необходимо защищать компьютеры.

В начале 70-х годов XX века Дэвид Белл и Леонард Ла Падула разработали модель безопасности для операций, проводимых на компьютер. Эта модель была основана на правительственной концепцией уровни классификации информации (несекретные, конфиденциальные, секретные, секретные) и уровни толерантности. Если человек (субъект) имел уровень допуска выше, чем уровень файла (объекта) классификации, он получил доступ к файлу, в противном случае доступ будет отклонен. Эта концепция нашла свою реализацию в стандартном 5200.28 "Доверенной вычислительной системы критериев оценки" (TCSEC) ("критерий оценки безопасности компьютерных систем"), разработанный в 1983 году Министерством обороны США. Из-за

цвета обложки он назывался "оранжевая книга". "Оранжевая книга" попал в компьютерную систему в соответствии со следующей шкалой. Минимальная защита (не нормируется) защита по усмотрению регулируемых безопасности для защиты доступа к защите ярлыками структурированные защиты. Домен защита проверяем развития

1.2. Нормативно-методические средства обеспечения службой информационной безопасности в образовательной организации

Одним из следствий технического прогресса стало активное внедрение информации, это привело к образованию определенного рынка, а затем началось формирование информационного общества. В наше время невозможно представить образовательную организацию без развитой системы информационных сетей, их активного использования потребителями. Информация (и как следствие информатизации) доказали свою перспективность в стимулировании роста благосостояния общества в решении других социальных проблем.

Нормативная основа правовых отношений, связанных с информацией:

Основанием для принятия мер, регулирующих доступ к сети Интернет в образовательной организации (к которым относятся ограничение доступа учащихся к интернет-ресурсам, содержащих информацию, не совместимую с целями образования и воспитания детей; информация на интернет-ресурсах ОО), являются приказами и письмами регионального и (или) муниципальном уровнях, а также Федеральные законы:

— Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации";

— Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"; — Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию";

— Федеральный закон от 25.07.2002 № 114-ФЗ "О противодействии экстремистской деятельности";

— Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Для обеспечения функционирования системы информационной безопасности в образовательной организации будет нужен набор внутренних правил.

Рассмотреть документы в области информационной безопасности в образовательной организации.

Защита персональных данных субъектов образовательного процесса в образовательной организации являются операторами персональных данных, обработка персональных данных студентов и преподавателей. Следовательно, ответственными сотрудниками этих учреждений должны быть обеспечены законом № 152-ФЗ "О персональных данных". Статья 19 Федерального закона № 152 "О персональных данных". Меры по обеспечению безопасности персональных данных при их обработке Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Использование и хранение биометрических персональных данных (далее-Персональные данные) вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии хранения, которые защищают этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения. В рамках образовательных организаций должен быть выполнен комплекс работ по сбору пакета документов (25 форм) для регуляторов (регулирующих органов). Трудность заключается в том, что в настоящее время отсутствуют нормативные акты, утверждающий форму этих типовых ведомственных документов по защите персональных данных в образовательных организациях.

Пакет документов для проверки;

— Положение о защите персональных данных;

— Положение о подразделение по защите информации;

— приказ о назначении лиц, ответственных за обработку персональных данных;

— концепция информационной безопасности;

— политики информационной безопасности;

— перечень персональных данных, подлежащих защите;

— приказ о проведении внутреннего аудита;

— отчет о результатах внутренних аудитов;

— акт классификации информационной системы персональных данных;

— ограничение прав доступа к обрабатываемым персональным данным;

— модель угроз безопасности персональных данных;

— план мероприятий по защите персональных данных;

— порядок резервирования технических средств и программного обеспечения, баз данных и средств защиты информации;

— план внутренних аудитов;

журнал учета мероприятий по контролю безопасности персональных данных;

— реестр обращений субъектов ПДН о выполнении их законных прав; — инструкция администратора информационной системы персональных данных;

— инструкция пользователя информационных систем персональных данных;

— инструкция администратора безопасности информационной системы персональных данных;

— инструкцию пользователя по обеспечению безопасности обработки персональных данных в чрезвычайных ситуациях;

— список учета средств защиты информации, эксплуатационной и технической документации;

типовой круг ведения для разработки системы безопасности информации объекта вычислительной техники;

проект по созданию системы информационной безопасности объекта оборудованием;

— Положение об электронном журнале обращений пользователей информационных систем персональных данных (проект приказа).

- Гражданским кодексом Российской Федерации (его значение в этом направлении увеличивается с вступлением в силу с 1 января 2008 года четвертой части, посвященной объектам интеллектуальной собственности);

Гражданский кодекс Российской Федерации (его значение в этом направлении возрастает в связи с вступлением в силу с 1 января 2008 года четвертой части, посвященной объектам интеллектуальной собственности); Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

Указом Президента РФ от 12 мая 2004 г. № 611 "О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена" (с изм. и доп. от 22 марта 2005 г. 3 марта 2006 г.)

Указом Президента РФ от 31 декабря 1993 г. N 2334 "О дополнительных гарантиях прав граждан на информацию" (с изм. и доп. от 17 января 1997 года 1 сентября 2000 года)

Указом Президента РФ от 22 декабря 1993 г. N 2255 "О совершенствовании государственного управления в сфере массовой информации" (с изм. и доп. от 6 апреля 1999 г., 9 августа 2000 года)

Указом Президента Российской Федерации от 12 мая 1993 г. N 663 "О мерах по созданию единого эталонного банка данных правовой информации"

Постановлением Правительства РФ от 31 августа 2006 г. N 532 "О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации"

Постановление Правительства Российской Федерации от 15 августа 2006 г. N 504 "О лицензировании деятельности по технической защите конфиденциальной информации"

Основные понятия, связанные с информацией и Информатизацией, Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" в статье 2:

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 баз, данных и обеспечивающих обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, осуществляется с использованием компьютерной техники;

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;

доступ к информации - возможность получения информации и ее использования;

конфиденциальность информации является обязательным для человека, чтобы получить доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

электронное сообщение - информация, переданная или полученная в информационно-телекоммуникационной сети пользователя;

документированная информация фиксируется на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации, если ее материальный носитель;

оператор информационной системы - гражданин или юридическое лицо, участвующее в функционировании информационной системы, в том числе обработку информации, содержащейся в ее базах данных.

Согласно статье 3 Закона, правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

ограничить доступ к информации только федеральными законами;

открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, за исключением случаев, установленных федеральными законами;

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, установленных федеральными законами.

Конфиденциальную информацию можно отличить от секретной информации, которая предназначена для собственника и общественной безопасности. Аналогичным образом, необходимо различать конфиденциальную информацию, как широкое понятие, подразумевающее отсутствие доступа к различной офисной и коммерческой информации, которая распределяется на дополнительные функции**.**

Вывод по 1 главе:

Понятие информационной безопасности в образовательной организации в научной литературе рассмотрено достаточно подробно в контексте таких понятий как: информация, информационные системы, информационные процессы, несанкционированный доступ, уязвимость, атака. Что позволяет нам говорить об создании и управлении службой информационной безопасности в образовательной организации не только на уровне руководителя образовательной организации, но и на уровне службы информационной безопасности.

Процесс создания и управления службы информационной безопасности образовательной организации является частью управления образовательной организацией в целом. Процесс планирования призван дать ответ на вопросы: кто, что, когда должен будет делать, каким образом, с какими ресурсами и с какими результатами. Организация с точки зрения управления, в свою очередь создает и управляет службой информационной безопасности в образовательной организации, обеспечивает взаимодействие подразделений. Знание основ создания и управления позволяет грамотно и эффективно выстроить процесс управления информационной безопасностью в образовательной организации.

Специфика планирования и организации информационной безопасности в образовательной организации основывается на законах, приказах, которые предъявляют требования к структуре, условиям реализации и результатам информационной безопасности в образовательной организации.

Глава 2. Анализ обеспечения информационной безопасности в образовательной организации

2.1 Проблемы обеспечения информационной безопасности в образовательной организации

Информационные и компьютерные технологии заняли прочное место в процессе обучения. Практика показывает, что использование ИКТ в развивающих занятиях по психологии также способствует повышению познавательной активности и мотивации студентов. Программа Lokalova Н. П. "уроки психологического развития", К. Н. Поливановой "Введение в школьную жизнь", Коноваленко И. Н. "развитие познавательной активности учащихся" являются ключом к организации занятий. Работы по любой из вышеперечисленных программ требует огромного количества раздаточного дидактического материала. В качестве иллюстративного учебного материала мы используем компакт-диск "супер-интеллект" вызывает большой интерес у ребят вызывают задания, которые определяют этот диск так же, компьютерных игр.

Радикальные изменения государственной политики в сфере национальной безопасности и, в частности, информационной безопасности (ИБ), в области образования и информации; опыт создания и функционирования системы подготовки специалистов в области защиты информации (коммуникации); результаты анализа его состояния, определяют актуальность проблемы формирования у студентов педагогических специальностей вуза компетентности в области информационной безопасности как составляющей информационной культуры специалиста. Сегодня отмечаются достаточно серьезные противоречия: возрастающий спрос на преподавателей с высоким уровнем компетентности в области информационной безопасности и отсутствием целостной концепции подготовки специалистов; необходимость более глубокой теоретической и методологической подготовки будущих учителей в области защиты информационных ресурсов сферы образования и

необходимость усиления прикладной направленности обучения; между потребностями педагогической практики в эффективных инструментов для обеспечения безопасности и диагностики открытого образовательного пространства и отсутствием научной разработки этого инструментария. Социальную значимость проблемы, необходимость подготовки специалистов, способных творчески решать профессиональные задачи, связанные с защитой информационной инфраструктуры в сфере открытого образования, определили выбор темы настоящего исследования.

К совершению противоправных действий в области ИКТ: использование нелицензионного программного обеспечения; написание вирусов и других вредоносных программ, взлома компьютеров и сетей, защиты банковской системы, подделки кредитных карт, бесплатный доступ к ресурсам Интернет и междугородная телефонная сеть и т. д. была степень правовой грамотности в сфере защиты интеллектуальной собственности в сфере высоких технологий; мы определили уровень сформированности нравственных качеств в деятельности, опосредованной ИКТ, определены по отношению к нарушителям информационной безопасности, в материалах, связанных с хакерской атакой (Интернет, литература); определить степень знакомство с видами информационно-психологического воздействия ИКТ на людей, меры профилактики и намерение негативного влияния ИКТ на психическое и физическое здоровье и т. д. Во время диагностики его использовали как традиционные методы, так и уникальные методы, с помощью которых был определен уровень (эталонный и реальный/диагноз) компетентности респондентов в области информационной безопасности. Как показали результаты исследования, 64,60 % респондентов имеют низкий, средний 28,05 % и 7.35 % высокий уровень компетентности в вопросах, связанных с обеспечением информационной безопасности в системе открытого образования. Недостаточный уровень компетентности также у студентов по специальностям и направлениям, связанным с ИКТ, а также молодых

специалистов, выпускников педагогических специальностей вузов (включая учителей информатики). Эта категория респондентов показал недостаточный уровень компетентности в области подготовки подрастающего поколения к жизни в информационном обществе, были не очень хорошо знакомы с особенностями обеспечения защиты информационной инфраструктуры образовательных организаций. "Узкими» оказались компетенции, связанные с подготовкой учителя: формирование у студентов культуры работы с информационными ресурсами; активизация воспитательной работы по формированию нулевой терпимости к незаконным действиям в сфере информационно-коммуникационных технологий, предотвращению компьютерных преступлений среди молодежи; в целях предотвращения и нейтрализации негативного воздействия информационных угроз на людей и технических систем; создание безопасных условий труда для учащихся и. Таким образом, подтверждена необходимость решения проблем совершенствования высшего педагогического образования в области информационной безопасности, которая определяется противоречием между возросшей потребностью в специалистах, владеющие современными методами и средствами защиты информационных структур образования, и недостаточной теоретико-методологические основы развития профессиональной подготовки, повышения квалификации и переподготовки учителей в этой области.

Следующий этап работы включал определение и разработка концепции формирования компетентности будущих учителей в области информационной безопасности. Концепция развития основана на изучении структуры Отечественной ИКТ-отрасли, анализ персонала и структуры спроса на персонал в сфере информационной безопасности, изучение методических основ в области информационной безопасности, глобальной концепции и тенденции его развития. Исследование проводилось с учетом рекомендаций Болонского процесса, международных профессиональных организаций ACM и IEEE, которые "вычислительной учебных планов 2005", Европейский Карьерное

пространство консорциум, международный консорциум по сертификации в области безопасности информационных систем (isc), на основе изучения опыта внедрения специализации "Информационная безопасность и защита информации" по специальности "Информатика" (квалификация "учитель информатики"). Разработанная нами концепция представляет собой систему (системное описание исследуемого процесса), определяющим основные задачи, принципы, направления совершенствования, приоритетные действия и ожидаемые результаты развития системы подготовки педагогических кадров в области информационной безопасности. Наша концепция содержит положения, касающиеся определения понятия, его цель, правовое и методическое обеспечение, границы применимости в педагогической теории. Основной целью концепции является переориентация образовательной политики по развитию педагогических специальностей университетов принципиально нового компонента информационной компетентности культуры в области обеспечения информационной безопасности в системе открытого образования.

В ходе проведения исследования, мы разработали модель компетенций будущих учителей в области информационной безопасности. Модель включает компетенции, относящиеся к приоритетным направлениям будущей профессиональной деятельности учителя: образовательные, социально-образовательные, культурно-просветительные, научно-методические и организационно-управленческая. Для каждого ключевого сектора (ключевые роли) отдельным темам компетенций, которые в свою очередь были разложены на два или более элементов. Для всех элементов компетенций, определены критерии оценки эффективности и перечислены необходимые знания и понимание, необходимые для успешного выполнения конкретных ролей и задач, связанных с безопасностью информационной инфраструктуры в системе открытого образования. Нами разработана концепция служит методологической основой для согласования деятельности всех субъектов образовательных организаций, научно-исследовательских организаций,

государственно-общественных и общественных объединений, работодателей, работающих в этой области.

Благодаря разработанной концепции, мы провели корректировку действующих учебных программ по предмету "Информатика", введены новые дисциплины в учебные программы регионального компонента и элективных дисциплин для педагогических специальностей университета. В настоящее время проводится проверка в реальном учебном процессе специальных курсов для студентов, учителей, преподавателей, соискателей и аспирантов; элективные курсы и факультативы для учащихся старших классов общеобразовательных школ по проблемам ИБ ("ИБ", "ИБ в открытом образовании", "Правовое обеспечение информационной безопасности", "проблемы информационно-психологической безопасности", "Компьютерная этика и этикет" и др.). Среди студентов педагогических специальностей университета и старшеклассников конкурсы, эссе, веб-проектов проблем безопасности.

Дальнейшее направление исследований будет посвящена разработке, тестированию (в системе профессиональной подготовки будущих учителей, повышения квалификации работников образовательных учреждений), подготовку и издание комплексного научно-методического обеспечения процесса формирования у будущих учителей компетентности в области обеспечения информационной безопасности, в том числе:

методические рекомендации для преподавателей по разделу обучения "основы ИБ" в рамках курса "информатика" в педагогическом факультетах;

Сборник научных и методических материалов, специальность "Информатика" с дополнительной специальностью "З и ПБ";

критерии оценки инструментарий педагогического мониторинга формирования компетентности студентов педагогических специальностей университетов в области обеспечения информационной безопасности;

методическое сопровождение разделов по проблеме исследования в программы спецкурсов и спец-семинаров для учителей средней школы, педагогов дополнительного образования, учителей, студентов педагогических специальностей вузов: "Гуманитарные аспекты информационной безопасности", "безопасность в открытом образовании", "основы информационной безопасности";

рекомендации по использованию технических и технологических средств защиты от нежелательной информации в образовательных учреждениях.

Таким образом, исходя из программы, мы предложили рекомендации по совершенствованию информационной безопасности в образовательных организациях.

2.2. Организация антивирусной защиты компьютеров и мобильных устройств сети образовательной организации.

Для любого активного пользователя сети Интернет вопрос о защите и безопасности электронной информации, в первую очередь, и любой образовательной организации не является исключением. Все содержащиеся на компьютерах, планшетах или мобильных устройствах может быть украдено и устранено различными вредоносными программами в считанные секунды.

Рассмотрим основные типы вредоносных программ.

Компьютерные вирусы-это вредоносный код или компьютерных программ, которые предназначены для нанесения вреда компьютеру пользователя, чтобы украсть или уничтожить данные, или удаленно управлять компьютером для личной выгоды. Таким образом, любой из все этих вирусов — нанести значительный ущерб компьютеру и парализовать ее работу.

Компьютерный червь-это вредоносные программы, которая может копировать себя на компьютерах или через компьютерные сети.

Пользователь не знает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна размножаться, заражение распространяется очень быстро. Есть так много различных типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению. Известная форма вредоносных программ-вирусов являются "троянскими конями". Трояны обычно маскируются под безобидные программы, чтобы спровоцировать пользователя запустить их. Конечной целью Троянской программы является нанесение вреда компьютеру пользователя, а в корыстных и бескорыстных целях. Есть "трояны", целью которого является стереть информацию на жестком диске вашего компьютера, поэтому все ваши данные: музыку, документы, фильмы, фотографии - Все удалены и восстановить их будет практически невозможно. Еще один вид "троянов" является кража

сохраненных на вашем компьютере паролей в различных программах, чаще всего кража паролей происходит из браузеров, так что если это случится, вы потеряете доступ к своей электронной почте, социальным сетям и другим счетам. Ну и последний распространенный вид троянских программ - которые блокируют работу компьютера с целью получения средств для разблокировки. Другими словами, Вы включаете компьютер и у вас есть окно блокировки, с требованием перечислить определенную сумму денег для разблокировки компьютера. Поэтому необходимо предусмотреть способы защиты. Этот способ является антивирусной программой.

Антивирусная программа (антивирус) - это специальная программа для обнаружения компьютерных вирусов и вредоносных программ имеют возможность для восстановления (лечения) зараженных программ и файлов. Новые системы обнаружения современных антивирусов быстро предотвращают заражение файлов или операционной системы вредоносным кодом. Помимо защиты вашего компьютера от вирусов и троянов, антивирус также может отслеживать сайты вы посещаете, прежде всего, чтобы блокировать ресурсы, которые могут причинить вред вашему компьютеру, а только те сайты, которые имеют вирусы. Кроме того, антивирусное программное обеспечение может блокировать рекламу на сайтах и всплывающие баннеры, которые действительно очень полезны. Не говоря уже об этой дополнительной функции, некоторые антивирусы, такие как "Родительский контроль". Эта функция предназначена для защиты детей от посещения нежелательных веб-ресурсов, и, по сути, выполняет функции фильтрации содержимого, с достаточно гибкой настройкой. Заражения вирус можно только извне, то есть сам по себе вирус не может появиться. Существует два способа заражения вашего компьютера вирусами через Интернет или через съемные носители. Через Интернет ваш компьютер может быть заражен вирусом при скачивании каких-либо файлов или посещении вредоносных сайтов. В качестве съемного носителя, примерами таких носителей являются флешки или CD/DVD-дисков, когда они были

записаны на зараженный компьютер, и путем копирования или запуска вирус перешел на свой компьютер. Антивирусное программное обеспечение в обоих этих случаях защищает компьютер от попадания вирусов извне. Сегодня на рынке антивирусных программ сосредоточен большой спектр антивирусов простой бесплатный мощный - комплекс, который использует лучшие технологии безопасности для защиты разного вида устройств. Как выбрать антивирус для образовательных организаций? Прежде всего, тот, который будет предоставлять полный спектр защиты с учетом особенностей и потребностей Вашей школе. Так какой выбрать антивирус - решать Вам. Мы, в свою очередь, даст вам критерии выбора антивирусных программ и перечислим самые популярные из них, которые достойны вашего внимания.

Давайте посмотрим на функции антивируса, которые необходимы для надежной защиты вашего компьютера, в порядке важности:

Антивирусный монитор отслеживает файлы и папки, с которыми вы работаете, чтобы проверить их на наличие вирусов.

Сканер-это функция, которая сканирует жесткий диск и оперативную память на наличие вирусов. Очень полезная функция для проверки подозрительных и потенциально вредоносных файлов на вашем компьютере, особенно полезно для сканирования съемных носителей. Самозащита антивируса. Функция самозащиты антивируса предназначена для антивируса может защитить себя от воздействия вирусов. Есть вирусы, которые пытаются отключить как некоторые функции антивируса, так и предотвратить его работу в целом, чтобы они не распространяли вирусы по всему компьютеру, именно для этого и нужна функция самозащиты. Программ мониторинг активности. Этот антивирус предназначен для управления работой программы. В случае, если программа заражена вирусом, то он начнет вносить изменения в ее работе, который должен определить контроль антивируса. Сетевой контроль и веб-антивирус. Эти компоненты антивируса, обеспечить безопасность Интернете.

Сеть контролирует сетевую активность и веб-антивирус сканирует http-трафик, блокируя угрожающие безопасности компьютерных скриптов, размещенных на веб-сайтах. Постоянное обновление антивирусных баз. Очень важно для защиты антивирус является возможность постоянного обновления антивирусных баз. Антивирусные базы - это своего рода знания о вирусах и их особенности, что антивирус использует для обнаружения и предотвращения вирусов. Потому что новые вирусы появляются почти каждый день, антивирус, обнаружения нового вируса, должны учить своих продуктов, установленных пользователи, знаний об их обнаружении и ликвидации. Таким образом, если вы хотите защитить ваш антивирус компьютер не только от известных, старых вирусов, но новые обновления должны быть регулярными. Низкая ресурсо-потребления. Одна из проблем со многими антивирусов - большой ресурс-потребление. При выборе антивирусного программного обеспечения, попробуйте выбрать продукт, который не будет сильно нагружать систему, так как в противном случае работать за таким компьютером или ноутбуком будет очень неудобно. Репутация и популярность антивируса - очень важный фактор, который следует учитывать при выборе антивирусной программы. Более популярный антивирус, тем больше и больше пользователей его используют, и поэтому вряд ли большое количество людей будут использовать слабый антивирус. Каждый из нас понимает, что продукты не всегда лучшего качества, чем бесплатный. Думаю, что антивирус защитит необходимый персонал, который будет постоянно собирать информацию о новых вирусах и вредоносных кодов из Интернета и работы по их нейтрализации. Затем, данные из базы знаний, необходимых для создания обновления и загружать их на сервер программы был обновлен и поэтому должна быть постоянной. Кроме того, необходимо разработать новые версии и вирусов. Какой вывод мы можем сделать из этого? Создание и поддержка антивируса нужен персоналу и полной занятости, и поэтому в общей теории относительности, чтобы все организовать, конечный продукт должен покрыть все затраты на эту деятельность. Ну, кто согласится работать бесплатно? И если это так, то качество антивирус будет

уместен. Рассмотрим основные критерии, которым должны соответствовать качественные антивирусные программы. Надежность работы и простота использования являются наиболее важным критерием, поскольку даже "абсолютный антивирус" может оказаться абсолютно бесполезной, если она конфликтует с системой резко снижает его производительность или периодически "зависает". Если антивирус требует специальных знаний, которыми не обладает большинство обычных пользователей, то это будет слишком сложно работать. Если корпоративные версии антивируса не содержит необходимый функционал для администрирования сети, большинство системных администраторов предпочитают менее надежные, но более удобный продукт.

2.3. Защита информационных ресурсов образовательной организации, обучающихся от нежелательной информации, антивирусная защита

Для организации безопасною доступа н Интернет, в образовательной организации необходимо разработать следующий пакет документов:

— правила использования сети Интернет в образовательной организации для всех субъектов образовательного процесса;

— документ ознакомления и согласия с Правилами использования сети Интернет в образовательной организации, удостоверенное подписью в документе ознакомления и согласия с правилами.

Регулярное (периодичное) заполнение документа ознакомления; — инструкция для сотрудников образовательной организации о порядке действий при осуществлении контроля за обучающимися, работниками организации, родителями при использовании ресурсов Интернета — приказ, назначающий администратора точки доступа к сети Интернет;

— должностная инструкция администратора точки доступа к сети Интернет в образовательной организации;

— положение о Совете образовательной организации по вопросам регламентации доступа к ресурсам сети Интернет.

В положении указать персональный состав Совета, поддерживать в актуальном состоянии персональный состав Совета;

— регламент работы обучающихся, родителей, учителей (преподавателей) и других сотрудников образовательной организации; — документ регистрации посетителей точки доступа к сети Интернет в образовательной организации;

— документ регистрации ресурсов, посещаемых с точки доступа к сети Интернет в образовательном учреждении. Регулярное (периодичное) заполнение документов регистрации;

— ответственный за антивирусную безопасность образовательной организации;

— локальные акты, регламентирующие обязанности ответственных за антивирусную безопасность образовательной организации;

— положение «О защите детей от информации, причиняющей вред их здоровью и развитию» в образовательной организации, содержащее классификаторы информации, доступ к которой обучающимся запрещен и разрешен;

— лицензионное соглашение или договор на использование программных контент-фильтров, используемых в образовательной организации;

Напомним, что на всех компьютерных устройствах, входящих в сеть образовательной организации, необходимо установить лицензионное антивирусное программное обеспечение и регулярно обновлять антивирусные базы (сигнатуры), в том числе и на личных устройствах, обучающихся и сотрудников.

2.4. Законодательное обеспечение защиты персональных данных

Закон № 152-ФЗ определяет требования к сбору и обработке (хранению, актуализации, использованию, раскрытию и предоставлению) персональных данных физических лиц во всех сферах, где используются персональные данные, в т. ч. в сфере трудовых правоотношений. Требования закона распространяются на все организации (независимо от формы собственности), в т. ч. на образовательные, которые выступают операторами, обрабатывающими в своих информационных системах персональные данные физических лиц (работников, обучающихся и др.).

Вопрос правовой регламентации обеспечения защиты персональных данных работников в настоящее время особенно актуален, поскольку информационные системы персональных данных работников образовательной организации должны представлять собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием или без использования средств автоматизации. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации, применяемые в информационных системах.

В соответствии с частью 3 статьи 4 Закона № 152-ФЗ постановлением Правительства РФ от 15.09.2008 № 687 утверждено Положение об особенностях обработки персональных данных, осуществляемой без

использования средств автоматизации. Данное Положение предусматривает, что обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований этого Положения. Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 05.02.2010 № 58 утверждено Положение о методах и способах защиты информации в информационных системах персональных данных, которое подробно регламентирует вопросы, связанные с порядком применения методов и способов защиты информации в информационных системах персональных данных оператором или уполномоченным им лицом. В соответствии с частью 1 статьи 22 Закона № 152-ФЗ оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять 20 обработку персональных данных, за исключением случаев, предусмотренных частью 2 указанной статьи.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Россвязькомнадзор) выступает таким уполномоченным органом, который приказом от 17.07.2008 № 08 утвердил образец Уведомления об обработке (о намерении осуществлять обработку) персональных данных и Рекомендации по заполнению образца формы

уведомления об обработке (о намерении осуществлять обработку) персональных данных. Частью 2 статьи 22 Закона № 152-ФЗ установлено, что оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных, относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения. Следовательно, образовательные организации не должны уведомлять этот уполномоченный орган об обработке ими персональных данных работников, состоящих в трудовых отношениях с учреждениями. Планирование мероприятий по защите персональных данных при планировании в образовательной организации мероприятий, связанных с защитой персональных данных, рекомендуется привлекать юристов, специалистов отдела кадров по информационной работе (компьютерным технологиям).

Правовая составляющая должна стать обязательным элементом всей деятельности организации в этом направлении, поскольку необходимо: - разработать локальные акты (нормативные и правовые), связанные не только с организационной и правовой, но и с технической защитой персональных данных; - сформировать механизмы взаимоотношений с органами, осуществляющими управление в сфере образования, профсоюзными организациями, органами контроля и надзора и т. д.

Главным условием защиты персональных данных является четкая регламентация функций работников, а также принадлежности работникам документов, дел, картотек, журналов персонального учета и баз данных. Далее ключевым вопросом становится оценка наличия предусмотренных законодательством оснований для обработки персональных данных, а в случаях, когда они отсутствуют, - получение согласия субъекта персональных данных на их обработку.

При этом согласно Закону № 152-ФЗ обязанность доказательства согласия субъекта персональных данных на их обработку возлагается на оператора, т. е.

на работодателя. Несмотря на то, что в данном комментарии речь идет исключительно о защите персональных данных работников, необходимо обратить внимание на то, что в образовательной организации обрабатываются персональные данные обучающихся и их родителей, поэтому организация предварительно должно получить согласие родителей на обработку персональных данных их самих и их детей. Следует уделить особое внимание процедуре передачи персональных данных третьим лицам. Для этого необходимо наличие: - основания для такой передачи, предусмотренные федеральными законами, или согласия субъекта персональных данных, закрепленного, например, в договоре на оказание услуг; - договора с этим третьим лицом, существенным условием которого должна быть обязанность обеспечения указанным лицом конфиденциальности и безопасности персональных данных при их обработке. Необходимо очень внимательно подойти к вопросу размещения информации, содержащей персональные данные на сайте образовательной организации.

С учетом выше изложенного можно выделить следующие обязательные этапы работы по защите персональных данных работников:

1) определение всех ситуаций, когда требуется проводить обработку персональных данных;

2) выделение процессов, в которых обрабатываются персональные данные;

3) выбор ограниченного числа процессов для проведения аналитики (на этом этапе формируется перечень подразделений и работников, участвующих в обработке персональных данных в рамках своей служебной деятельности);

4) определение круга информационных систем и совокупности обрабатываемых персональных данных;

5) проведение категорирования персональных данных и предварительной классификации информационных систем;

6) разработка пакета организационно-распорядительных документов для обеспечения защиты персональных данных (положения, приказы, акты, инструкции и т. п.);

7) внедрение системы обеспечения безопасности информации. Следовательно, защита персональных данных работников в образовательной организации, по сути; сводится к созданию режима обработки персональных данных, включающего: - создание внутренней документации по работе с персональными данными; - организацию системы защиты персональных данных; - внедрение технических мер защиты персональных данных

2.4. Система защиты персональных данных участников образовательного процесса

Определение термина «персональные данные» можно найти в двух основных нормативных документах

- Федеральном законе от 27 июля 2006 г, № 152-ФЗ «О персональных данных» и Трудовом кодексе РФ.

К персональным данным относится информация, которая позволяет идентифицировать лицо. Единственное отличие определений заключается в том, что трудовое законодательство говорит именно о работниках, закон - о любых субъектах персональных данных. В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ к персональным данным относится любая информация о физическом лице: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация. Обработкой персональных данных признаются действия (операции) с ними, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т. ч. передачу), обезличивание, блокирование, уничтожение данных. Защита персональных данных представляет собой комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных). Образовательная организация собирает и использует большой массив информации обо всех участниках образовательного процесса. В настоящее время в образовательных организациях активно внедряются информационные системы, осуществляющие обработку персональных данных, делопроизводство, бухгалтерские программы и др. Эти системы предназначены для ведения базы данных обучающихся, родителей и работников, оперативного управления организацией. Вместе с тем, любой гражданин обладает правами на

неприкосновенность частной жизни, личную и семейную тайну. Эти права не должны нарушаться ради эффективности образовательного процесса либо удобства работы с персоналом. Одной из задач законодательства, и, следовательно, образовательной организации является охрана и защита персональных данных обучающихся, их законных представителей и работников. Защита персональных данных участников образовательного процесса в образовательной организации осуществляется на основе следующих нормативно-правовых документов: Федеральный закон от 28 декабря 2010 г. Ха 390-ФЗ «О безопасности», Федеральный закон от 27 июля 2006 г. Хв 149-ФЗ «Об информации, информационных технологиях и о защите информации», II Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об у т в е р ж д е н и и перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», документы, регламентирующие вопросы обеспечения безопасности персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 №21: - «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», - «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», - «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». В комплекс мероприятий по защите персональных данных в образовательной организации входят: - разработка необходимых документов в интересах организации по обеспечению защиты персональных

данных; - обоснование требований по защите информации в информационных системах персональных данных; - применение методики оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных; - определение состава и структуры программно-аппаратных средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

2.5. Предложения по усовершенствованию обеспечения информационной безопасности в образовательных учреждениях

Одним из приоритетных направлений развития образовательной организации на протяжении нескольких лет является внедрение новых информационных технологий в образовательном процессе.

Сформированное информационное пространство школы-сложная система, и в идеале она должна обеспечить условия эффективного взаимодействия всех структур образовательной организации с целью повышения качества образовательного процесса. Управление создаваемые системой призвано обеспечить использование кадровых, материальных, финансовых, временных и других ресурсов с максимальной эффективностью и продуктивностью для развития детей.

Основными задачами заместителя директора по информатизации является:

Компьютеризация управленческой деятельности.

Информатизации образовательного процесса.

Формирование и развитие информационной культуры учащихся и учителей на основе НДТ.

используются сегодня в школе в нескольких направлениях:

Компьютеризация управления школой:

Для автоматизации документооборота и делопроизводства;

Для создания базы данных для студентов и сотрудников;

Для хранения различных вопросов управления информацией;

Создание программ и баз данных "здоровье";

В учебно-воспитательном процессе:

Научить студентов основам компьютерной грамотности, информатике и программированию;

Для диагностики качества образования (тесты);

Для подготовки презентаций и докладов, выступлений;

Как средство наглядности на уроках при введении нового материала (мультимедиа, видео, компакт-диски);

Для проведения практических занятий (компьютеры, компакт-диски);

Для самообразования учащихся и учителей (компьютерные классы, компакт-диски, Интернет, дистанционное образование);

Для видеосъемки школьных мероприятий и создания видеотеки по истории школы;

Для получения информации через подключение к Интернет;

Для электронной переписки.

Сегодня всей структуры информационного учебного центра (далее-ШИЦ). Все подразделения объединены в локальную общешкольную сеть. Деятельность классов информатики можно подразделить на учебный процесс, организацию внеурочной деятельности учащихся, место для индивидуальной работы по подготовке документов, отчетов, презентаций студентов и преподавателей. В вечернее время кабинет используется для педагогов образование для взрослых города компании "Мастер-сервис".

В штатное расписание школы введена ставка заместителя директора по информатизации, который является координатором всей работы по внедрению новых информационных технологий в образовательном процессе. Для поддержки компьютерной техники в рабочем состоянии нанять квалифицированный инженер, программист и техник по обслуживанию. Персонал обеспечивает функционирование локальной сети, поддержка Веб-

страница повышения квалификации для педагогов пользовательские навыки. Программа разработана двухуровневая профессиональную квалификацию на компьютере в разных средах и использования периферийных устройств.

С введением ставки программиста началось целенаправленное создание базы данных (Microsoft Access), которая обеспечивает новые возможности обработки данных и представления их в виде отчетов. Работа программиста направлена на выполнение конкретных задач, с учетом особенностей и потребностей школы.

В организации формируется определенный круг преподавателей, являющихся носителями компьютерных образовательных технологий. Некоторые из них объединяются в проблемные группы для изучения эффективных методов использования ИКТ в образовании.

ИКТ в организации, изучаются в значительно большей степени, чем в общеобразовательной школе, объеме и на более высоком уровне сложности, может показаться профессионального прихоти руководства. Однако опыт эффективного использования ИКТ в образовательном процессе гимназии демонстрирует значительный потенциал информационных и коммуникационных технологий в реализации идей компетентностного подхода и, в частности, культурно-исторической педагогики.

Цель образования, Е.А.Ямбург, стоит передавать будущим поколениям ценности культуры и научить их жить в быстро меняющемся мире. Учебно-воспитательный процесс образовательной организации, по определению, ориентирован в первую очередь на культурные ценности обучающегося; очевидно также, что способность жить в быстро меняющемся мире лучший способ для формирования эффективного обучения ИКТ. Внедрение ИКТ помогает обучающемуся и преподавателю в преодолении восприятия культуры как "лавку древностей, где хранится красивый, но давно отработанный материал" создает условия для реального включения молодого человека в контекст культуры, в первую очередь через применение метода проектов.

Проектная деятельность позволяет студентам приобрести дополнительные знания в их предметной области, научиться планированию собственной учебной деятельности, освоить основные программы, необходимые для современного пользователя ПК.

С его значительными ресурсами, чтобы удовлетворить потребности учащихся в самовыражении и самореализации, ИКТ развитие молодого человека, умение жить в гармонии с собой и с окружающими. Это, естественно, улучшает процесс развития таких ключевых компетенций, как ответственность и умение принимать решение в ситуации выбора.

Один из способов для расширения системы информационной безопасности общеобразовательного учреждения является создание (далее "услуги"). Показательным является опыт использования информационной службы в г.Челябинск. Сервис предназначен для осуществления поэтапного решения задач информатизации образования, внедрения новых информационных технологий в образовательный и управленческий процессы, информационно-методическое обеспечение процессов выявления, изучения и пропаганды передового педагогического опыта, инноваций в области образования, внедрения и поддержки документооборота, использования возможностей телекоммуникационных технологий.

Методическое сопровождение внедрения НИТ в учебный процесс и сопровождение образовательных технологий, ориентированных на формирование у учащихся навыков самообучения (сетевые Олимпиады, телекоммуникационные проекты, дистанционное обучение, развивающее обучение).

Создание единого информационного пространства городской системы образования:

сбор, накопление, обработка, систематизация, обобщение и распространение педагогической информации в соответствии с принятыми стандартами в системе образования;

выявление информационных потребностей и удовлетворение педагогического персонала образовательных учреждений в области новых технологий и педагогических инноваций;

взаимодействие с информационными службами всех уровней для расширения информационного Банка образования;

брокерские услуги для удовлетворения потребностей пользователей (работников образовательных учреждений) по доставке информации о достижениях психологии и педагогики, новых педагогических и информационных технологий;

организация обучения персонала образовательного учреждения навыки на компьютере на уровне пользователя.

Технологическая поддержка мониторинга в образовательных учреждениях.

Деятельности службы:

Организационная поддержка:

разработка программы информатизации образовательного учреждения;

разработка и реализация плана совместных действий всех подразделений образовательного учреждения по вопросам информации, по согласованию с окружной и городской уровень;

организация в школах, компьютерных клубах и других объединениях учащихся, использует в своей работе элементы медиаобразования;

обеспечение доступа к правовым и инструктивно-методическим материалам;

организация и поддержка сервиса по структуре в образовательных учреждениях;

тестирование и внедрение информационно-аналитической системы управления образованием.

организация и поддержка учителей, интересующихся проблемами информатизации образования.

Методическое обеспечение:

анализ текущей ситуации процесса информатизации образовательных учреждений, коррекции и мониторинга по данному вопросу;

подготовка методических пособий и рекомендаций по вопросам информатизации образовательных учреждений;

анализ и апробация методических, программных и технических разработок в районе, городе, области, России и за рубежом по вопросам информатизации образования и других направлений, касающихся работы информационных служб образовательных учреждений;

изучение существующего опыта и разработка плана работы в соответствии с программой развития образовательного учреждения, обеспечение эффективного освоения НИТ и включение новых медиа в учебный процесс образовательных учреждений;

организация научно-методической деятельности учителей по проблемам информатизации образования (в рамках проблемных объединений) с последующим выходом с конкретными результатами на научно-практических конференциях и форумах различного уровня, включая телекоммуникации.

Программно-методическое обеспечение образовательного процесса:

рекомендации по приобретению программного и методического обеспечения для образовательных учреждений;

создание и поддержка образовательного учреждения Банка учебной информации, обеспечение санкционированного доступа к ним учреждениях районного и городского уровня;

обоснование и подготовка к введению новых интегрированных учебных программ, направленных на профессиональное обучение студентов работе с современными информационными ресурсами;

организация и содействие подготовке и переподготовке учителей различных дисциплин и сотрудников образовательных учреждений по вопросам освоения НИТ, образование СМИ, лучшая практика в глобальных информационных сетях.

Информационная поддержка:

подключение образовательных учреждений к телекоммуникационным системам различного уровня с выходом в глобальные сети;

организация доступа к банку образовательной информации на любом носителе;

организация публикаций опыта и разработок учителей и сотрудников школы по вопросам образования;

Вывод по второй главе

Информационно-коммуникационные технологии помогают усилить воспитывающую функцию обучения, достигается новый качественный уровень гимназического образования, который выражается в способности учащихся находить и обрабатывать информацию, овладевать знаниями и умениями, эффективно применимыми в любой сфере жизнедеятельности, самостоятельно принимать решения в ситуации выбора.

Таким образом, в ходе работы по созданию и управлению службой информационной безопасности в образовательной организации были выявлены технологии, которые помогают усилить информационную безопасность, который выражается в способности педагогов находить и обрабатывать информацию, овладевать знаниями и умениями, эффективно применимыми в любой сфере жизнедеятельности, самостоятельно принимать решения в ситуации выбора.

Глава 3. Экспериментальная работа по информационной безопасности на базе Южноуральского государственного технического колледжа

Проблема информационной безопасности образовательного учреждения превращается в последнее время из гипотетической в реальную. Количество угроз растет с каждым днем, меняется нормативная база, в соответствии с реалиями времени должны меняться и методы обеспечения информационной безопасности учебного процесса.

"Кто владеет информацией, правит миром" - эти слова Н. Ротшильд становится все более важным в наше время. Действительно, тот, кто обладает знаниями и использует его умело, способен решать поставленные задачи, организовать работу подчиненных, чтобы обеспечить успешное развитие предприятия.

В современном колледже информации, информационная инфраструктура является одним из основных компонентов учебно-воспитательного процесса. Кабинеты оборудованы компьютерной техникой и ее высокое качественное бесперебойное функционирование существенно определяет качество полученных знаний, способствует формированию профессиональной компетентности студентов. Поэтому обеспечение информационной безопасности учебного процесса, в том числе непрерывного функционирования компьютерных и информационных ресурсов является весьма важной для его качества. В этой статье я хочу описать свое видение проблемы и ее решений, реализуемых в нашем колледже.

Проблемы обеспечения информационной безопасности четко различают технические, организационные и документационные аспекты.

Технический аспект связан с выбором программного обеспечения, и организационный – с деятельностью по реализации Закона № 152-ФЗ "О персональных данных" и документация с созданием локальных актов колледжа. Однако, в современном информационном обществе организационные и документированные аспектов во многом пересекаются.

В первую очередь рассмотрим технические вопросы.

Для студентов и преподавателей главным способом поиска информации является использование глобальной сетью Интернет. Какие угрозы в интернете? Это компьютерное мошенничество, компьютерные вирусы, хакерские атаки, вандализм, хищение, разглашение конфиденциальной информации и так далее. Для борьбы с ними с помощью программ для фильтрации входящего трафика (прокси-сервер). В нашем колледже эта программа стала программой usergate. Это хорошее комплексное решение для организации общего доступа в Интернет из локальной сети учета трафика и защиты от внешних угроз, и брандмауэр защищает сеть от внешних атак. При необходимости, для подключения к Интернет-классов компьютер или отключить их, установить периоды времени для работы в Интернете, блокировать нежелательные ресурсы отдельно, или категориям сайтов. Это экономит огромное количество времени. Наоборот, в библиотеке, доступ полностью открыт, за исключением общепризнанных "опасных" ресурсов (реклама, сайты, игры для взрослых, казино и т. д.). Прокси-серверы также позволяло контролировать объем загруженных данных из сети, что значительно снижает нагрузку на локальную сеть. Кроме того, хорошо настроенная антивирусная программа с автоматическим обновлением и образуется дополнительный список угроз (в случае нашего колледжа Касперского 6.0) дает, в свою очередь, качественную антивирусную защиту.

Время пляжа сегодня – вирусы "авторай", портативный флэш-накопители блокируются от нас с помощью отключить автозапуск на любых носителях, а также специальная организованная структура для хранения данных на флэш-накопитель. Для этого проводят краткие тренинги по информационной безопасности для сотрудников, преподавателей и студентов.

Другой канал распространения угроз электронной почты, который используют почти все. Самый надежный способ контроля - организация собственного почтового сервера, который легче отслеживать протоколы электронной почты,

чтобы фильтровать нежелательные или сомнительные "сообщения". В этом случае все сотрудники имеют свои адреса электронной почты на собственном почтовом сервере колледжа и запрещен официальный (служебный) документооборот через стороннего сервера. Тем не менее, это идеальный вариант, и он будет реализован в ближайшем будущем, а пока просто усиление контроля над ресурсами, посещаемых сотрудниками. В тех случаях, когда требуется криптографической защиты программное и аппаратное обеспечение банков, Пенсионного фонда, налоговой инспекции и других структур, с которыми необходимо обмениваться информацией конфиденциальной информации.

Еще один технический аспект проблемы бесперебойной работы — компьютеров-это разделение доступа к информации и ресурсам. Есть как минимум две учетные записи (одна с ограниченными правами – основной и второй с администратором – только настройки, и обе обязательно защищенные паролем) позволяет намного дольше сохранять работоспособность компьютеров в целом, контролировать установку программного обеспечения. Таким образом, установка контрафактных и "вредоносных", в большинстве случаев, просто невозможно (не хватает мощности).

Второй аспект проблемы информационной безопасности – организационные. Он регулирует производственной деятельности и взаимоотношений исполнителей на законном основании для исключения или ослабления причинив никакого ущерба. Для успешной работы всех участников образовательного процесса должны быть четко осведомлены о проблеме информационной безопасности. Между тем, пользователи часто нарушают процедуру обработки информации, не соответствуют требованиям нормативно-правовых документов, регламентирующих информационную безопасность. Информационная безопасность может быть обеспечена только при комплексном использовании всех средств защиты. Процесс построения системы информационной безопасности не может быть одноразовым

мероприятием, а также исполнения и контроля не могут быть возложены на одного, ответственный за информационную безопасность. Этот процесс должен быть управляемым, постоянно совершенствуется. Этот подход является стратегическим звеном всей системы информационной безопасности, так как информация является основным охраняемого элемента.

Между понятиями "Информационная безопасность" и "компьютерная безопасность" невозможно поставить знак равенства, первая более обширная и требует много работы. Соответственно, в этой области в нашем колледже в качестве коллективных усилий преподавателей колледжа создан список интернет-ресурсов, необходимых для студентов, преподавателей и сотрудников; создана и утверждена "белый" список образовательных ресурсов (при активном содействии методическим Советом колледжа). Лаборатория "информационная и вычислительная техника" разработаны правила доступа к Интернет и инструкция о порядке контроля использования студентами сети Интернет.

Одним из самых сложных угроз любой информационной системы — наличие "инсайдер", официальным экспертом организации, которые имеют доступ к конфиденциальной информации, и, по некоторым причинам (психологического характера или для получения прибыли) занимается кражей информации. Соответственно, для предотвращения этой угрозы, систематическое обучение сотрудников и преподавателей колледжа информационной культуры на заседаниях педагогического совета колледжа и тематические заседания методических комиссий по всем дисциплинам. Привитое понятие "корпоративной" этики, мониторинг психологической устойчивости сотрудников колледжа, коллектив имеет "теплый" психологический климат.

Теперь пришло время перейти к наиболее актуальным и сложным проблемам защиты информационной безопасности учебного процесса.

В нашем колледже активно внедряются информационные системы, которые обрабатывают персональные данные (в простейшем случае, написанный программистом базе колледжа), системного администрирования, бухгалтерские программы (Парус и 1С: Предприятие 8). Все они предназначены для учета студентов, их родителей и учителей (человек), оперативное управление колледжа. Колледж должен отвечать требованиям законодательства о защите персональных данных участников образовательного процесса, в первую очередь, потому что речь идет о защите информации, неправомерное использование которой может отрицательно сказаться на правах граждан.

Защита персональных данных-комплекс мер технического, организационного, организационно-технических и правовых мер по защите информации, относящейся к определенному или определяемому на основании такой информации физическому лицу – субъекту персональных данных (работнику).

Положения о защите персональных данных работников регламентируются:

· Конституции Российской Федерации;

· Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации";

· Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных"

· Трудовой кодекс Российской Федерации

В соответствии с ФЗ № 152-первых, внутреннее обследование информационной системы колледжа, а также определен его класс К3 в соответствии с этим разработаны: уведомление в Роскомнадзор, приказ ответственных лиц на сотрудников и Положения о защите персональных данных. Это положение является основным локальным актом и было учтено мнение первичной профсоюзной организации учреждения в порядке, установленном статьей 372 Трудового кодекса.

Этот документ определяет: обработки персональных данных работников; обеспечение защиты прав и свобод работников при обработке их персональных данных; ответственность лиц, имеющих доступ к персональным данным работников, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных работников.

Этот локальный нормативный акт является обязательным, поэтому его отсутствие может быть квалифицировано государственным органом контроля и надзора в качестве нарушения работодателем трудового законодательства.

В заключение следует сказать, что, по моему мнению, неоценимую помощь может оказать независимый аудит. В планах колледжа проведение такого мероприятия с помощью одного из интеграторов нашего региона, что позволит выявить уязвимые места, возможные каналы утечки информации и объективно оценить существующий режим информационной безопасности. Также ожидается, что такой аудит позволит добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание системы безопасности колледжа.

Итак, обеспечение информационной безопасности учебного процесса в современных условиях становится одним из видов деятельности колледжа. Без использования новых подходов, поиска современных форм и способов обеспечения информационной безопасности учебного процесса решить эти задачи невозможно!

Заключение

Проведенное нами исследование носило теоретический характер и было посвящено актуальной проблеме созданию и управлению службой информационной безопасности в образовательной организации

В ходе работы над темой нами были последовательно реализованы все поставленные задачи.

В данных задачах были рассмотрены механизмы для реализации следующих направлений информационной безопасности в образовательных организациях общего и среднего профессионального образования:

— организация контентной фильтрации данных из Интернета на компьютерных устройствах, используемых учениками;

— обеспечение антивирусной защиты и других интернет-угроз компьютеров и мобильных устройств локальной сети организации;

— обеспечение защиты персональных данных субъектов образовательного процесса; — организация правомерного использования объектов авторского права. Рассмотрены вопросы разработки системы информационной безопасности ОО, подготовки пакета внутренних нормативных документов и инструкций для функционирования системы информационной безопасности, выбора и организации работы контентной фильтрации, антивирусных программ на компьютерных устройствах сети ОО, разработки системы защиты персональных данных субъектов образовательного процесса, разработки системы защиты информационных ресурсов ОО, проведение мероприятий с участием субъектов образовательного процесса для повышения уровня информационной культуры в области информационной безопасности.

Данные рекомендации позволят оптимизировать процесс обучения на программах повышения квалификации, где рассматриваются вопросы информационной безопасности образовательной организации, а также окажут

методическую помощь педагогам-практикам в создании, усовершенствовании системы информационной безопасности образовательной организации в соответствии с существующими нормативно-правовыми документами.

Таким образом, можно отметить, что создание и управление службой информационной безопасности в образовательной организации охарактеризованы, цель исследования достигнута, поставленные задачи реализованы в полной мере, гипотеза исследования подтверждена.

Библиографический список

1. Административное право /под ред. Л.Л. Попова. М.: Юристъ - 703 с.
2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник/Под ред. Б.Н. Топорнина. СПб.: Издательство "Юридический центр Пресс", 2001. С. 436-438.
4. Белов Е.Б. Основы информационной безопасности. Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. -М.: Горячая линия - Телеком, 2006. - 544с
5. Бекетов Н. Информационная безопасность развития государства // Информационные ресурсы России, № 6, 2004. -С.: 32-35;
6. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
7. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации СПб, Питер 2002- 464 с.

8.Галатенко В.А. Стандарты информационной безопасности: курс лекций. Учебное пособие. - 2-ое издание. М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2009. - 264 с.

9. Гаврилов Э.П. Коммерческая тайна и результаты интеллектуальной деятельности // Патенты и лицензии. 2002. N 4. С.19-23

10.Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с

11. Городов О.А. Информация как объект гражданского права //Правоведение. 2001. N 5. С.80 - 82

12. Гражданское право /под ред. Е.А.Суханова. М.: Волтерс Клувер, 2004 - 734 с.

13. Дозорцев В.А. Интеллектуальные права. Понятие. Система. Задачи кодификации. М.: НОРМА, 2003. - 400 с.

14. Дозорцев В.А. Понятие исключительного права // Юридический мир. 2000. N 3. С.4-11; N 6. С.25-35.

15. Доктрина информационной безопасности Российской Федерации утверждена Президентом РФ 9 сентября 2000 г. N Пр-1895 (РГ, 2000, N 187)

16. Даль В. Толковый словарь живого великорусского языка. Т. 1. М., 1989. С. 67.

17. Домарев В.В. Энциклопедия безопасности информационных технологий. Методология создания систем защиты информации. Киев.: ООО "ТИД "ДС", 2001

18.Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.

19. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ, 2013. - 239 с.

20. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография. / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ, 2015. - 239 с.

21. Закон РФ от 10 июля 1992 г. N 3266-1 «Об образовании» (с изменениями от 24 декабря 1993 г., 13 января 1996 г., 16 ноября 1997 г., 20 июля, 7 августа, 27 декабря 2000 г., 30 декабря 2001 г., 13 февраля, 21 марта, 25 июня, 25 июля, 24 декабря 2002 г., 10 января, 7 июля, 8, 23 декабря 2003 г., 5 марта, 30 июня, 20 июля 2004 г.)

22. Запечинков, С.В. Информационная безопасность открытых систем в 2-х томах т.1 / С.В. Запечинков. - М.: ГЛТ, 2006. - 536 с.

23. Запечинков, С.В. Информационная безопасность открытых систем в 2-х

томах т.2 / С.В. Запечинков. - М.: ГЛТ, 2008. - 558 с.

24. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 - Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. - М.: ГЛТ, 2006. - 536 с.

25. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 - Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ, 2008. - 558 с.

26. Запечников, С.В. Информационная безопасность открытых систем. Том 1. Угрозы, уязвимости, атаки и подходы к защите: Учебник для вузов. / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ , 2006. - 536 с.

27. Запечников, С.В. Информационная безопасность открытых систем. Том 2. Средства защиты в сетях: Учебник для вузов. / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ , 2008. - 558 с.

28. Зверева Е.А. Информация как объект неимущественных гражданских прав //Право и экономика. 2003. N 9. С.28-33

29. Информатика /под ред. С.В.Симоновича. СПб, Питер 2001- 400 с.

30. Каймин В.А. Информатика и дистанционное образование - М.: НОРМА-ИНФРА-М, 2002 - 432 с.

31. Каймин В.А. Информатика. М.: ИНФРА-М, 2002 - 328 с.

32. Кирмайер М. Информационные технологии. СПб.: Питер, 2003 - 443 с.

33. Конституция Российской Федерации.

34. Копылов В.А. Информационное право Российской Федерации. М.: Инфра-М, 2006 - 400 с.

35. Конотопов, М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М.: КноРус, 2013. - 136 с.

36. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. - М .: Академия, 2006. - 256 с.

37. Лапчик М.П. Методика преподавания информатики: учеб. Пособие для студ. Пед. Вузов. /М.П. Лапчик, И.Р. Семакин, Е.К. Хеннер; под общей редакцией М.П. Лапчика. - М.: Издательский центр Академия, 2001. - 624 с.

38.Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. - М.: ГЛТ, 2004. - 280 с.

39. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. / А.А. Малюк. - М.: Горячая линия -Телеком , 2004. - 280 с.

40. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М.: Флинта, 2013. - 448 с.

41. Моисеев А.М. Проблемы и пути совершенствования внутришкольного управления. Пособие для руководителей образовательных учреждений. Тамбов: ТОИПКРО. 2002. 331 с.

42.Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

43. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

44. Педагогика /под ред. А.А. Радугина. М.: Центр, 2001 - 272 с.

45. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации. М.Финансы и статистика, 2002 - 512 с.

46. Роберт И. Современные информационные технологии в образовании: дидактические проблемы; перспективы использования.- М: Школа-Пресс, 2001 -292 с.

47. Рогаткин Д.В. Службы примирения в системе школьного самоуправления // Вестник восстановительной юстиции». 2002. № 4. С. 12-30.

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

49. Селевко Г.К. Современные образовательные технологии.- М: Народное образование, 2002 -255 с.

50. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И., Основы организационного обеспечения информационной безопасности объектов информатизации // Гелиос АРВ, 2008 г., 192 с

51. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2010. - 277 с.

52. Семененко, В.А. Информационная безопасность / В.А. Семененко. - М.: МГИУ, 2011. - 277 с.

53.Тихонов В.А., Райх В.В., Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты // Гелиос АРВ, 2009г., 528 с

54. 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.

55. Чашников Л.А. Современные модели информационно-аналитического обеспечения школьного управления // Вопросы психологии. 1993. № 9. С.36-57. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» //СПС Гарант

56.Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2010. - 336 с.

57. Чупрасова В.И. Современные технологии в образовании. Владивосток: Издательский дом «ДВР», 2004 - 154 с.

58. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

59. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с

60.Шубинский М.И. Информационная безопасность для работников бюджетной сферы: учеб. пособие / НИУ ИТМО. - СПб., 2012.

61. Шафеева Е.Ю. Шубинский М.И. Основы безопасности жизне деятельности в сети Интернет (ОБЖИ): метод, пособие / МПСС. СПб., 2010.

62. Ярочкин В.И., Информационная безопасность: учебник для студентов вузов// -М.: Академический проект; Гаудеамус, 2-е изд., 2009 г., 544 с

63. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008. - 544 с.

64. Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин. - М.: Академический проект, 2008. - 544 с.