Тип работы: Курсовая работа

Предмет: Программирование

Содержание

Введение
Тема данной работы основана на том факте, что информационные ресурсы в современном обществе играют не менее важную роль, чем материальные ресурсы, а зачастую даже большую. С точки зрения рынка, информация уже давно является товаром, и эта ситуация требует интенсивного развития практики, промышленности и теории компьютеризации общества. Компьютеры как информационная среда не только сделали возможным качественный скачок в организации промышленности, науки и рынков, но и определили новые и ценные области производства: компьютерные технологии, телекоммуникации и программные продукты.
Использование услуг, предоставляемых Интернетом, глобальной информационно-коммуникационной сетью, в образовательном процессе, несомненно, является инновационной технологией. Но для того, чтобы в полной мере воспользоваться возможностями, открывшимися с появлением сетевого доступа во многих школах, необходимо правильно представлять себе образовательные характеристики, преимущества и ограничения новых технологий. На данном этапе в России практическое применение компьютерных технологий и сетей в целом, а также возможности Интернета являются незрелыми. Причины могут быть разными.
Во-первых, существует общая необразованность учителей, особенно пожилых. Это довольно сложная ситуация, потому что необходимо приобрести "компьютерную грамотность" в долгосрочной перспективе, которая играет важную роль на ранних этапах изучения основ компьютерной грамотности. Поскольку компьютеры стоят дорого, обычные учителя лишены таких возможностей. Неполная и односторонняя компьютерная грамотность подрастающего поколения учащихся часто приводит лишь к умению включать компьютер, запускать на нем любимые игры или, в лучшем случае, набирать и печатать текст, что не помогает решить ту или иную проблему. [6]
Во-вторых, сами учащиеся не применяют работу - это репутация Интернета среди учителей и родителей как источника сочинений, рефератов, самостоятельных проектов. Усилия по ограничению доступа учителей и родителей к такой информации в их жизни также были отклонены, поскольку материалы о порнографии, антигуманизме и насилии находятся в свободном доступе. Интернет-преступность тоже не является

призраком. Любые действия, которые могут привести к длительному тюремному заключению, могут быть предприняты учащимся со своего домашнего компьютера.
Цель данной работы - показать, как преодолеть вышеуказанные трудности и предложить эволюцию проблем информационной безопасности в общеобразовательных учреждениях.
В соответствии с определенными целями, задачи работы заключаются в характеристике теоретических основ информационной безопасности в образовательных учреждениях и анализе инициатив в области информационной безопасности в образовательных учреждениях.

1. Теоретические основы информационной безопасности в образовательных учреждениях

1.1 История развития информационной безопасности

Информация означает сведения о людях, объектах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления, применительно к задаче ее защиты. В зависимости от формы представления информация записывается в виде речи, телекоммуникаций и документируется.
Информационный процесс относится к процессу сбора, накопления, обработки, хранения, распространения, поиска и т.д. информации.
Информационная система - это совокупность документов, массивов и информационных технологий.
Информационный ресурс - это массив документов или подзаконных актов, которые существуют по отдельности или как часть информационной системы.
Процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства называется "информационная технология".
Информационные технологии делятся на открытый доступ и ограниченный доступ.
Информация является одним из объектов гражданского права, таких как собственность, владеть и право на использование. Владельцем информационных ресурсов, технологий и систем является субъект, который имеет право владеть, использовать и распространять эти объекты. Владельцы ресурсов, технологий и систем - это те, кто обладает властью владеть этими объектами и использовать их. Под пользователем понимается субъект, который обращается к информационной системе для получения необходимой информации и использует ее. [2]
Защищенная информация относится к уникальной информации, которая защищена в соответствии с требованиями юридических документов или предоставлена владельцем информации.
Под утечкой информации понимается беспорядочное распространение путем разглашения защищенной информации, несанкционированного доступа, получения информационным агентом и т.д.
Несанкционированный доступ - это получение защищенной информации от заинтересованных лиц в нарушение Правил доступа к защищенной информации.
Несанкционированное воздействие на защищенную информацию - это следствие нарушения правил изменения защищенной информации (например, замены электронных документов). Непреднамеренное воздействие на защищенную информацию означает воздействие на защищенную информацию из-за ошибок пользователя, сбоев оборудования или программного обеспечения, природных явлений или других непреднамеренных последствий (например, уничтожение документов на жестком диске).
Целью защиты информации является предотвращение причинения вреда пользователям, владельцам или

бенефициарам. Под эффективностью защиты информации понимается степень, в которой защищаемый результат соответствует заявленной цели. Защищаемым объектом может быть информация, ее носитель и информационные процессы, требующие защиты в соответствии с поставленной целью.
Конфиденциальность информации заключается в том, что только субъект, обладающий соответствующими полномочиями, знает ее содержание. [6]
Шифрование информации - это преобразование информации таким образом, чтобы содержание информации не было известно тем, у кого нет соответствующих прав доступа. Результат шифрования называется шифром.
Под угрозой информационной безопасности в компьютерной системе понимается событие или действие, которые могут вызвать изменение в работе КС, связанное с нарушением безопасности обрабатываемой в ней информации.
Информационная уязвимость относится к вероятности возникновения ситуации на любом этапе жизненного цикла КС, при которой существуют условия для реальной угрозы безопасности КС.
Атака - это действие, которое злоумышленник предпринимает, чтобы найти и использовать определенную уязвимость. Угрозы делятся на угрозы, не зависящие от человеческой деятельности, и техногенные угрозы, связанные с человеческой деятельностью. Искусственные угрозы можно разделить на непреднамеренные (недостатки дизайна, ошибки программного обеспечения) и преднамеренные (несанкционированный доступ, несанкционированное поведение). В результате применения угрозы информация может быть утечена, повреждена или утеряна.
Аппаратные средства защиты информации включают электронные и электронно-механические устройства, которые выполняют определенные функции (самостоятельно или с помощью программного обеспечения) для обеспечения безопасности информации, содержащейся в CS.
К основным средствам защиты информационного оборудования относятся устройства ввода для идентификации пользователей информации, устройства шифрования информации и * устройства для предотвращения несанкционированного запуска серверных рабочих станций.
Программное обеспечение информационной безопасности относится к конкретным программным средствам, включенным в программное обеспечение CS, которые предназначены только для целей защиты. Основные программные средства защиты информации включают программы, которые идентифицируют и аутентифицируют пользователей CS, программы, которые различают доступ пользователей к ресурсам CS, и программы против несанкционированного доступа, копирования, модификации и использования.

Список используемых источников

1. Бережной В. И., Астафьев В. А., Суспицына Г. Г. Управление персоналом в образовательных учреждениях. Учебное пособие. – М.: Проспект, 2021. – 320 с.
2. Бершадский М. Е., Нестеренко А. А., Гузеев В. В. Российская эффективная школа. Образовательная среда, организация и управление. / под ред. Гузеева В. В. – М.: НИИ Школьные технологии, 2019. – 154 с.
3. Бабаш А. В., Ларин Д. А., Баранова Е. К. Информационная безопасность. История специальных методов криптографической деятельности. – М.: Риор, 2019. – 236 с.
4. Гленн К. Системное администрирование в школе, ВУЗе, офисе. – М.: Солон-пресс, 2018. – 440 с.
5. Ищейнов В. Я., Мецатунян М. В. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. – М.: ИНФРА-М, 2021. – 256 с.
6. Лободина Н. В. Организация исследовательской и проектной деятельности обучающихся как основное требован. ФГОС. / под ред. Гринина Л. Е., Волковой-Алексеевы Н. Е. – М.: Учитель, 2020. – 275 с.
7. Мытник К. Я., Панасенко С. П. Смарт-карты и информационная безопасность. / под ред. Шаньгина В. Ф. – М.: ДМК-пресс, 2019. – 516 с.
8. Нестеров С. А. Основы информационной безопасности. Учебник. – М.: Лань, 2022. – 324 с.
9. Полищук Ю. В., Боровский А. С. Базы данных и их безопасность. – М.: ИНФРА-М, 2021. – 210 с.
10. Рунов А. Социальная информатика. – М.: Кнорус, 2019. – 428 с.
11. Сычев Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов. – М.: ИНФРА-М, 2020. – 223 с.
12. Тумбинская М. В., Петровский М. В. Комплексное обеспечение информационной безопасности на предприятии. Учебник. – М.: Лань, 2020. – 334 с.
13. Ткачева Г. В., Самарин Ю. Н., Логачев М. С. Образовательная программа как инструмент системы управления качеством профессионального образования. – М.: ИНФРА-М, 2019. – 166 с.

14. Уймин А. Г. Сетевое и системное администрирование. Учебно-методическое пособие. – М.: Лань, 2021. – 480 с.
15. Хоффман Э. Безопасность веб-приложений. Разведка, защита, нападение. с
16. Хирьянова И. С., Федяинова Н. В. Проектная деятельность младших школьников с использованием ИКТ. ФГОС. / под ред. Поповой Г. П., Концовой В. В. – М.: Учитель, 2020. – 175 с.
17. Шаньгин В. Д. Информационная безопасность и защита информации. / под ред. Мовчан В. А. – М.: ДМК-пресс, 2017. – 772 с.