Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Information security as a basic science in teaching informatics

Irina BAYMURATOVA[1], Erkin BOZOROV[2]

Tashkent State Technical University of Islam Karimov
National University of Uzbekistan

ARTICLE INFO

Article history:
Received May 2021
Received in revised form
28 May 2022
Accepted 20 June 2022
Available online
25 July 2022

Keywords:
information,
information security,
information society,
protection measures,
teaching information
technology

ABSTRACT

The article describes the concept of information, properties of information presentation and measures to protect information, and the specifics of the use of information, teaching information technology in educational institutions and new features in teaching.

2181-1415/© 2022 in Science LLC.
DOI: https://doi.org/10.47689/2181-1415-vol3-iss6/S-pp52-57

Axborot xavfsizligi informatika fanini o'qitishda asosiy fan sifatida

Kalit so‘zlar:
axborot,
axborot xavfsizligi,
axborot jamiyati,
himoya qilish choralari,
axborot texnologiyalarini
tayyorlash.

ANNOTATSIYA

Maqolada axborot tushunchasi, axborotni taqdim etish xususiyatlari va axborotni himoya qilish chora-tadbirlari hamda axborotdan foydalanishning o‘ziga xos xususiyatlari, ta’lim muassasalarida axborot texnologiyalarini o‘rgatish va o‘qitishdagi yangi xususiyatlar yoritilgan.

[1]Master's student, information technology educator Tashkent State Technical University of Islam Karimov, Teacher of the Institute of Nuclear Physics, Academy of Sciences of the Republic of Uzbekistan, Tashkent, Uzbekistan
[2] Doctor of technical sciences, professor of the National University of Uzbekistan, Tashkent, Uzbekistan, Doctor of technical sciences, professor of the Institute of Nuclear Physics, Academy of Sciences of the Republic of Uzbekistan, Tashkent, Uzbekistan

Информационная безопасность как базовая наука в преподавании информатики

Ключевые слова:
информация,
информационная безопасность,
информационное общество,
меры защиты,
преподавание информационных технологий

АННОТАЦИЯ

В статье описывается понятие информации, свойства представления информации и меры по защите информации, и специфика применения информации, преподавание информационных технологий в учебных заведениях и новые особенности в его обучении.

Специфика преподавания предмета информатики основана на самом предмете информатике – информации. Отсюда и вытекает основные направления и проблемы данного предмета. Преподавание информационных технологий в общеобразовательных школах в нашем государстве начинается с 5-го класса, когда учащиеся переходят в среднее звено, это обусловлено взаимосвязью информатики с математикой. Так как решение информационных задач основано на знании в области арифметических действий и понятий среднего звена.

Хотя многие страны, такие как Эстония, Франция, Израиль, Испания, Словакия, Великобритания, Финляндия, Польша, Португалия, частично США, Индия, Китай, Австралия, подошли к обучению данного предмета намного раньше, т.е., с 3-го класса и продолжают до окончания школы.

Информатика, как наука, дает понятие информационного общества. Из известного выражения Найтана Майера Ротшильда «кто владеет информацией, тот владеет миром» вытекает, что, владея большим количеством информации по какому-либо вопросу, можно деформировать механизмы коммуникации, дестабилизировать механизмы функционирования основных систем общества, лишить возможности реализации информационной составляющей личности.

Понятие «информационные технологии» у большинства ассоциируется с работой на компьютере, но это далеко не так, – это, прежде всего, учение о правильном мышлении. Учитель должен уметь учить учащихся правильно видеть поставленную задачу, а значить, правильно составить алгоритм, а также методы решения этого алгоритма и только после этого приступать к описанию данного алгоритма при помощи языков программирования.

Поэтому предмет «информационные технологии» нужно вводить вместе с понятием математики уже в начальных классах, развивая логическое восприятие информационной действительности.

Вследствие этого будет воспитываться новое информационное общество.

Человечество на протяжении своего развития всегда стремилось к статусу «информационного общества», который меняет само понятие информации, расширяя ее потенциал, как позитивного ресурса, так и выявляя ее резко негативные возможности.

Как только человек осознал своё существование, он начал понимать окружающую его информацию, поэтому любое общество можно считать информационным.

Правильное понятие информационного общества меняет полностью сознание индивидуума, который мыслит по иному и имеет разное восприятие действительности.

Также использование компьютера, а в частности развивающие игры с большим количеством используемых кнопок клавиатуры, позволяет развивать мелкую моторику учащихся с физиологическими отклонениями в школах специализированного обучения.

В раннем возрасте при помощи игровых элементов можно описать свойства, которыми обладает информация.

Если рассматривать информацию как стратегической ресурс развития человечества, то она обладает следующими свойствами: достоверной и актуальной, новой и устаревшей, но не может быть передана, принята или хранима в чистом виде, любой источник информации имеет своего носителя и передается по каналам коммуникации. Отсюда следует, что информация –это любая форма представления сведений, воспринимаемая человеком или специальными устройствами. Информация не только может управлять человеком, обществом, но и целым государством. Поэтому на первом плане в современном обществе стоит проблема информационной безопасности и безопасности информации, обеспечения ее целостности, достоверности и доступности.

Данные же проблемы в игровой форме должны прорабатываться с учащимися на уроках, что будет развивать у учеников информационную этику пользования информацией.

Во всем мире для создания информационной безопасности имеют формулировку базовых принципов и основных мер информационной безопасности, которые должны обеспечить:

целостность данных – защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;

конфиденциальность информации и одновременно ее доступность для всех авторизованных пользователей.

Во время реализации указанных принципов государства определяет уязвимые сферы возможных нарушений: банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры. Эти структуры государства требуют специальных мер безопасности, поскольку они обеспечивают суверенитет страны.

Основными мерами по информационной безопасности считаются средства шифрования информации.

Современные системы обнаружения нарушения информационной безопасности включают в себя системы виртуализации, песочницы со встроенными системами антивирусной защиты и системы управления знаниями о киберугрозах и уязвимостях (Threat Intelligence).

В современном обществе любой вид деятельности в Интернете несет информационную безопасность. С одной стороны Интернет дает необъятные возможности для получения полезной информации, а с другой возможность

потери вашей ценной информации, её целостности и скрытности, так как информация в интернете проходит через сотню устройств и в каждом из них могут возникать угрозы её целостности.

Чаще всего источники угрозы запускаются с целью получения незаконной выгоды вследствие нанесения ущерба информации. Но возможно и случайное действие угроз из-за недостаточной степени защиты и массового действия угрожающего фактора.

Существует разделение уязвимостей по классам, они могут быть:

– объективными;

– случайными;

– субъективными.

Если устранить или как минимум ослабить влияние уязвимостей, можно избежать полноценной угрозы, направленной на систему хранения информации.

Объективные уязвимости напрямую зависит от технического построения оборудования на объекте, требующего защиты, и его характеристик. Полноценное избавление от этих факторов невозможно, но их частичное устранение достигается с помощью инженерно-технических приемов следующими способами:

1. Связанные с техническими средствами излучения: электромагнитные методики (побочные варианты излучения и сигналов от кабельных линий, элементов техсредств);

– звуковые варианты (акустические или с добавлением вибросигналов);

– электрические (проскальзывание сигналов в цепочки электрической сети, по наводкам на линии и проводники, по неравномерному распределению тока).

2. Активизируемые: вредоносные ПО, нелегальные программы, технологические выходы из программ, что объединяется термином «программные закладки»;

– закладки аппаратуры – факторы, которые внедряются напрямую в телефонные линии, в электрические сети или просто в помещения.

С одной стороны, Интернет создан для обеспечения доступной информации, с другой, информационная безопасность создает ряд ограничений доступа информации.

Существуют методы криптографии, которые могут защитит информацию, не ограничивая права пользователя.

Криптография – наука о шифровании информации. В основе метода заложен алгоритм шифрования. Для возврата к исходной информации нужен алгоритм дешифрования.

Государство обеспечивает защиту информации на законодательном уровне, но оно не может оградить нас от человеческого фактора.

Защита информации – гарантия безопасности, задача государства.

Особое место в обеспечении защиты информации и утечки, занимает медицинская информация.

Так как данная информация носит не только частный характер, но и морально- этические аспекты.

Для этого в мировой практики созданы большие централизованные информационные системы.

В развитии этого направления стала разработка таких экспертных систем, как MYCIN и INTERNIST-I. В 1965 году Национальная медицинская библиотека начала использовать MEDLINE и MEDLARS. В Соединенных Штатах Америки в 1996 году положения Закона о переносимости и подотчетности медицинского страхования (HIPAA), касающиеся конфиденциальности и передачи медицинских записей, побудили большое количество врачей перейти на программное обеспечение для электронных медицинских карт (EMR), в первую очередь для обеспечения безопасности медицинских услуг, данных.

Но и пользователи простых предприятия способны проводить мероприятия по повышению информационной безопасности и защите информации. Для этого применяются достаточно простые, но эффективные меры: выстраивание системы разграничения критичных полномочий в бизнес-системах, ограничение доступа к информационным ресурсам, превышающим минимально достаточный уровень. Но успех в области информационной безопасности может принести только комплексный подход, сочетающий надлежащее руководство, усилия компании по убеждению работников в необходимости повышения безопасности информации, создания законодательства и контроля со стороны государства за уровнем информационной безопасности и использованием отечественного программного обеспечения и информационных технологий.

Адаптация традиционных мер – сетевых решений, повышение качества сбора оперативной информации, моделирование угроз, повышение ответственности также расширяют границы «безопасного периметра» и создают условия для эффективного и безопасного использования информации в режиме реального времени.

Если рассматривать опыт нашего государства в данной сфере, то создание единого портала, электронного правительства, электронных ключей, все эти действия направлены на защиту информационных ресурсов нашего государства.

Исходя из выше сказанного, методика преподавания предмета информатики прежде всего должна быть основана на грамотном обучении его информационными ресурсами, их защите, умением собирать, хранить, перерабатывать информацию. Все эти навыки должны развиваться со становлением учащихся, как индивидуума, а значить и с начальной школы, а в среднем звене на заложенном фундаменте начальной школы будет развиваться в разных направлениях, таких как, IT-сфера, программирование, пользование офисными пакетами и веб-фрилансером.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Что такое информация? Значение слова Информации в философском словаре [Электронный ресурс]. URL: http://diclist.ru/slovar/filosofskiy/l/informatsija.html (дата обращения: 18.03.2016).

2. Белов Е.Б., Лось В.П. Основы информационной безопасности. М.: Горячая линия: Телеком, 2006.

3. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 3-е изд. М.: Академия, 2008.

4. Абашев А., Жедрин И., Акулов В. Глобальные тенденции рынка информационной безопасности // Information Security/ Информационная безопасность. 2015. – № 5. – С. 16–17.

5. Разумовская Е.А. Некоторые проблемы безопасности в сфере информационных технологий // МИФИ: Безопасность информационных технологий. 2015. – № 4. – С. 91–96.

6. https://mitc.uz/ru/pages/info_security.

7. https://open-education.net/academic/school/kak-prohodyat-uroki-informatiki-v-raznyh-stranah-mira/.