Предисловие

Переход на новые образовательные стандарты общего образования и введение в старших классах средней школы профильного обучения в очередной раз поставили перед учителями непростую задачу, связанную с возможностью обучения предмету на разных уровнях, а также с подготовкой и проведением соответствующих элективных курсов.

Данное учебное пособие содержит необходимый материал для планирования и проведения элективного курса «Основы информационной безопасности при работе в телекоммуникационных сетях», который призван раскрыть наиболее важные вопросы методов и средств защиты информации в сети, сформировать у старшеклассников целостную, пригодную к практическому использованию систему понятий из данной области деятельности, заложить правовые основы в области защиты информации, персональных данных и использования электронной цифровой подписи, а также позволит освоить необходимые программные средства и сформировать практические навыки работы с ними.

При желании учитель может использовать данный элективный курс в качестве специального модуля в составе профильного курса информатики и ИКТ.

Представленное учебное пособие содержит программу элективного курса с пояснительной запиской и описанием необходимых программных средств, теоретическое содержание самого курса (в соответствии с приведенной программой), практические работы, тест для контроля знаний, дополнительный материал по теме, список использованной литературы и тексты федеральных законов (см. приложения).

Содержание элективного курса представлено в 11 главах и 9 практических работах и рассчитано на 18 учебных часов, если курс «Информатика и ИКТ» изучается на профильном уровне. Если же курс «Информатика и ИКТ» изучается на базовом уровне, то возможно изучение предлагаемого элективного курса в большем объеме часов и включение в него необходимых вопросов из разделов «Средства ИКТ» и «Телекоммуникационные технологии». Поскольку данный элективный курс может изучаться в разных вариантах, авторы не предлагают его поурочного планирования; его каждый учитель готовит самостоятельно. При этом темы, отмеченные значком ❖, являются дополнительными.

При преподавании данного электива необходимо учесть, что некоторые действия, описанные в составе практических работ, не следует выполнять в условиях реально работающей сети, чтобы не нарушить ее работу. Для выполнения этих работ желательно использовать среду виртуальных машин (см. соответствующее приложение).

В приложениях также содержатся тексты федеральных законов, о которых говорится в тех или иных разделах учебного пособия. Их можно использовать для выполнения заданий и проведения семинарских занятий.

Проверочный тест, включенный в учебное пособие, предназначен для проверки усвоения теоретического содержания курса.

Введение

«Информационная безопасность», равно как и «защита информации», — это одно из словосочетаний, которое сейчас очень часто попадается на глаза любому человеку, работающему в информационных сетях или просто следящему за новостями.

Формально простое и понятное, оно создает обманчивое впечатление простоты, а нередко — и не менее обманчивое впечатление крайней сложности и опасности. Однако подобные представления, составленные по всевозможной популярной прессе, к сожалению, годятся для увлекательных детективов, но не для реальной работы.

Немаловажным отрицательным их результатом является и то, что в итоге гораздо более привлекательной выглядит роль «нападающего» на чужую информацию, чем защищающего свою. В частности, потому, что защита часто рассматривается с точки зрения ее преодоления, с этаким «романтическим» образом современного Робина Гуда, так что у читателя (зрителя) складывается неверное представление о «всемогуществе» разнообразных информационных жуликов*.

Компьютерные телекоммуникации и связанные с ними технологии все больше и все чаще применяются в повседневной работе и в быту большинством людей. Каждый пользователь среды Интернет так или иначе, работая с сетью, сталкивается с задачами обеспечения безопасности информации.

---

* По личному мнению авторов, самомнение самих этих жуликов вовсе не оправдывает деструктивного характера их деятельности и ее чисто эгоистической направленности, — равно как и не является основанием для восхищения ими.

Этот элективный курс не претендует на исчерпывающую полноту, безупречность или научно-технологическую новизну. Его цель — ознакомить учащихся и преподавателей с основными понятиями, способами и методами обеспечения личной информационной безопасности, основными источниками угроз, а также с законодательной базой обеспечения информационной безопасности.

Следует отметить, что бóльшая часть современной литературы по обеспечению информационной безопасности так или иначе предназначена для профессионалов либо для пользователей, сталкивающихся с профессиональными задачами обеспечения безопасности информации в крупных компьютерных сетях. Обеспечение же личной безопасности имеет свою специфику, которая вполне очевидна и известна специалистам, но трудна для выделения из общего потока сведений обычными пользователями.

Авторы надеются, что после изучения данного электива у заинтересованного читателя возникнет некоторое, пусть не безупречное, но пригодное для работы и дальнейшего совершенствования представление об этой области информационных технологий.