Литература

1. Общая численность населения, численность населения по возрасту и полу, состоянию в браке, уровню образования, национальностям, языку, источникам средств к существованию по Гомельской области: стат. бюлл. / Нац. стат. к-т РБ, Глав. стат. упр. Гом. области. – Гомель, 2020. – 71 с.

2. Общая численность населения, численность населения по возрасту и полу, состоянию в браке, уровню образования, национальностям, языку, источникам средств к существованию по Гомельской области: стат. бюлл. / Нац. стат. к-т РБ, Глав. стат. упр. Гом. области. – Гомель, 2010. – 37 с.

3. Соколов, А.С. Современная языковая ситуация в Белоруссии и её динамика в постсоветский период / А.С. Соколов // Геополитика и экогеодинамика регионов. – 2020. – Том 6 (16). – Вып. 4. – С. 66–82.

ПРОБЛЕМЫ РАЗВИТИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ МАССОВОМ ПРИМЕНЕНИИ IT-ТЕХНОЛОГИЙ

Дузь С.В.
учащаяся 4 курса ГПОУ «Беловский политехнический техникум»,
г. Белово, Российская Федерация
Научный руководитель – Латышева А.Р., преподаватель

Проблемы развития и обеспечения информационной безопасности при массовом применении IT-технологий достаточно важная тема «Информационного века». Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем. Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

На сегодняшний день информационные системы играют значительную роль в обеспечении эффективной работы коммерческих и государственных предприятий, министерств, ведомств, а также некоммерческих организаций. Глобальное использование систем для хранения, обработки и передачи данных приводит к росту проблем, связанных с их защитой, а именно, учитывая глобальный характер роста числа кибератак, приводящих к значительным финансовым и материальным утратам.

В действительности, все крупные и средние предприятия имеют не только развитую информационную инфраструктуру, но и приняли меры к защите от наиболее значимых угроз. Угрозы, связанные с уязвимостью информационных систем предприятий, постоянно возрастают из-за постоянного повышения сложности внедряемых программных обеспечений. Также это обусловлено увеличением передачи данных через глобальную сеть Internet [1, с. 120].

В таких условиях системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным.

Киберпреступность – это незаконные действия, которые осуществляются людьми, использующие информационные технологии для преступных целей. Целями информационных атак являются:

- кража конфиденциальной информации;
- установка вредоносных программ;
- использование ЭВМ жертвы для рассылки спама;
- вымогательство.

Существует огромное множество видов хакерских атак, и с развитием информационных технологий они дополняются и совершенствуются. Важно выделить основные виды, которые чаще всего используются для несанкционированного доступа:

– переполнение буфера;
– вирусы;
– сниффер;
– DoS;
– DDoS.

Когда речь заходит об информационной безопасности (далее ИБ), то большинство начинает вспоминать про антивирусы, межсетевые экраны, IPS и т.д. Принято считать, что безопасность – это исключительно технический вопрос, который решается с помощью специализированного оборудования или программного обеспечения. Это большое заблуждение. Инструменты информационных технологий составляют менее 80% от общего концепта информационной безопасности компании [2, с. 201].

Информационные технологии, безусловно, занимают важное место в обеспечении информационной безопасности, но далеко не самую главную. Информационная безопасность – это целый комплекс мер из различных сфер деятельности компаний. Самый главный миф информационной безопасности – дорогое программное обеспечение. По его вине многие специалисты опускают руки и отказываются от мыслей об ИБ в своих компаниях. При этом они забывают даже про бесплатные технические и административные меры. Практически любое сетевое оборудование и все операционные системы имеют встроенные механизмы защиты.

Таким образом, можно сделать вывод, что защита конфиденциальной информации главной и неотъемлемой частью технологического процесса. Как это выглядит на практике?

Одними из самых распространенных в судебной практике являются споры с правообладателями. Количество исков возрастает с каждым годом. Данная категория дел является самой дорогостоящей. Так, ответчики по таким делам – люди, публично размещающие информацию, права на которую принадлежат другим гражданам. При этом если спорный информационный объект распространяют с подачи владельца сайта его пользователи, ответственность также несет владелец сайта.

Важной частью судебной практики являются споры, связанные с хищением денежных средств через каналы дистанционного банковского обслуживания. Данные дела носят резонансный характер, при этом суды теперь не только обвиняют во всем клиента банка, заключившего договор и взявшего на себя все риски по электронным платежам, но и проводят оценку безопасности непосредственно банковских платежей. Судами прямо указывается, что электронная форма составления, сохранения и представления документов не исключает наличия состава преступления в действиях субъекта. Так, в соответствии со ст. 327 УК РФ указанные документы отвечают признакам официального документа, форма же его предъявления в суд роли не играет. Следует отметить, что в рамках данной статьи невозможно проанализировать весь объем судебной практики по делам в сфере информационной безопасности.

Что в итоге? Можно заключить, современная судебная практика рассматривает сегодня различные дела, связанные с информационной безопасностью – с нарушением конфиденциальности информации, разглашением персональных данных, подделкой электронных документов и пр.

С каждым годом количество таких дел, находящихся на рассмотрении в судах, растет. Это подтверждает актуальность рассматриваемой проблемы и свидетельствует о необходимости вновь вернуться к ее рассмотрению в ближайшей перспективе [3, с. 10].

Литература

1. Информационное право: учебник для вузов / Н.Н. Ковалева [и др.]; под редакцией Н.Н. Ковалевой. – Москва: Издательство Юрайт, 2020. – 353 с. – (Высшее образование).

2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; ответственный редактор Т.А. Полякова, А.А. Стрельцов. – Москва: Издательство Юрайт, 2020. – 325 с. – (Профессиональное образование).

3. Информационная безопасность: Журнал "Information Security / Учредитель и издатель Компания "ГРОТЕК": сайт. – Москва, 2004 –2020. – URL: http://jurnali-online.ru/information-securityinformacionnaya-bezopasnost.

РАЗРАБОТКА КОМПЛЕКСА ТЕСТОВ «ИНФОРМАТИКА. 6–8-е КЛАССЫ»

Кондратьева И.Д.

учащаяся 11-го класса ГУО «Средняя школа № 45 г. Могилева»

Научный руководитель – Артёмова Е.В., учитель

Информационные технологии в образовании приобретают все более существенное значение. Современный учебный процесс сложно представить без использования компьютерных учебников, контролирующих систем и других компьютерных средств обучения. Компьютер становится помощником учителя и учащихся на уроках почти любого предмета. При изучении информатики компьютер может быть использован в роли средства обучения и как предмет изучения. О внедрении компьютерных технологий в учебный процесс большинства учебных предметов свидетельствуют и нормативные документы. Следовательно, важно готовить специалистов, способных применять информационные и компьютерные технологии в своей профессиональной деятельности.

Таким образом, одним из перспективных направлений реформы средней общеобразовательной школы является разработка электронных средств обучения и использование информационных технологий и прежде всего, электронных комплексов тестов.

При разработке электронных тестов необходимо придерживаться следующих этапов:

1) Определение тематики, целей и задач комплекса;
2) Проектирование структуры комплекса тестов и связей между вопросами;
3) Подготовка материалов (текста и графики);
4) Описание логической структуры комплекса тестов;
5) Описание внешнего вида комплекса тестов;
6) Тестирование и редактирование комплекса тестов.

Для определения тематики, целей и задач комплекса, а также при проектировании структуры комплекса и связей между вопросами, самое лучшее решение – это использование программы учебных занятий по информатике (табл. 1).

Далее необходимо выбрать необходимую программную среду для разработки комплекса тетстов.

Цель исследования – изучение основных возможностей программы iSpring QuizMaker на примере создания комплекса тестов «Информатики. 6 класс».

Объект исследования: программа iSpring Sute8.

Предмет исследования: комплекс тестов «Информатика. 6 класс», разработанный в программе iSpring QuizMaker.