Можно отметить ещё некоторые недостатки, выявленные в ходе эксплуатации ЭИОС в РГППУ. Выставление студентам оценок по результатам учебы подразумевает привязку к критериям балльно-рейтинговой системы (БРС) оценки знаний студентов. Однако, применение многочисленных форм учебной работы (включая СРС) с различными критериями оценки, неизбежная корректировка этих форм по ходу учебы, делают невозможным строгое выполнение требований БРС. Очевидно, нужны дополнительные механизмы в ЭИОС, позволяющие ранжировать и корректировать систему оценивания. Кроме того, необходимы некоторые меры, связанные с упрощением работы с ЭИОС (внедрение полноценных функций копирования, поиска и сортировки при оформлении графика учебного процесса, ведении журнала, внедрении и использовании тестов и т.д.) и повышения степени интегральности использования всех её подсистем (модулей). Не помешала бы в перспективе и возможность задания в системе индивидуальной траектории обучения для каждого студента. Следовало бы, очевидно, подумать и о возможности предоставления доступа к системе родителям обучающихся, о выводе показателей системы в удобных для представления форматах, о повышении технической вооруженности учебных аудиторий (организации сетевого взаимодействия и доступа к ЭИОС с каждого учебного компьютера). Следует отметить, что подобные и ряд других предложений рассматриваются в системе сопровождения ЭИОС и, зачастую, находят своё воплощение, расширяя тем самым её возможности и повышая эффективность её работы.

Подводя итоги вышеприведенным рассуждениям, следует признать безусловную необходимость внедрения и совершенствования ЭИОС в современных образовательных условиях. Вместе с тем, предстоит ещё многое сделать в техническом и методическом плане, а также продумать меры популяризации и стимулирования, для того, чтобы применение ЭОС стало повсеместно востребованным, необходимым и доступным инструментом образовательной среды, способствующим повышению эффективности и качества обучения студентов.

Список литературы

1. Карасик А.А., Барсуков Д.Н. Электронная информационно-образовательная среда РГППУ// Новые информационные технологии в образовании: материалы междунар. науч.-практ. конф., Екатеринбург, 10-13 марта 2015 г.: ФГАОУ ВПО «Рос. гос. проф.-пед.ун-т», Екатеринбург, 2015. – с.332-337.

2. Анахов С.В., Аношина О.В. Компьютерные технологии в физическом лабораторном практикуме// Новые информационные технологии в образовании: материалы междунар. науч.-практ. конф., Екатеринбург, 12-15 марта 2013 г.: ФГАОУ ВПО «Рос. гос. проф.-пед.ун-т», Екатеринбург, 2013. – с.16-18.

УДК 004.056.5

А. А. Большакова, Н. В. Потапова

МОДЕЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Большакова Анастасия Андреевна
anastaicha94@mail.ru
Потапова Наталья Викторовна
Potapova50@gmail.com
ФГБОУ ВО «Кубанский государственный университет», Россия, г. Краснодар

MODEL OF "INFORMATION SECURITY"

Bolshakova Anastasia Andreevna
Potapova Natalia Viktorovna
Kuban State University, Russia, Krasnodar

Аннотация. *Рассматривается структура и сфера влияния обеспечения информационной безопасности, как ориентационная модель для начинающих специалистов данной области.*

Abstract. *Deals with the structure and sphere of influence information security as an orientation model for beginners to experts the field.*

Ключевые слова: *Информационная безопасность, защита информации, криптографические преобразования информации.*

Keywords: *Information security, information protection, cryptographic transformation of information.*

Современный мир невозможно представить без электронно-вычислительных устройств. Образ современного человека невозможно представить без смартфона, гаджета, планшета, электронных часов, ноутбука или стационарного компьютера. И каждое это устройство передает, обрабатывает и хранит некоторую информацию. Круговорот электронной информации принято называть электронным документооборотом [4].

Но раз уж у человечества есть возможность передавать информационные ресурсы даже далеко за пределы планеты Земля, не заставляет себя ждать и острый вопрос обеспечения безопасности этих ресурсов.

Мы должны понимать, что под информационной безопасностью (далее - ИБ) понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

- доступность (возможность за разумное время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного доступа).

Область защиты информации зачастую понимается как защита информационных ресурсов от вредоносных ПО. Такое понимание ошибочно, так как концепция ИБ намного шире и включает в себя, в том числе, защиту информационных ресурсов. Не стоит забывать и про человеческий фактор. В организацию может проникнуть злоумышленник и, например, физически выкрасть информацию, незаметно изменить ее и прочее.

Таким образом, при изучении данной области должны быть сформулированы четкие ответы на конкретные вопросы:

- что защищать?
- от чего (кого) защищать?
- как защищать?

Формирование режима информационной безопасности — проблема комплексная. Меры по ее решению можно разделить на четыре уровня:

- законодательный (законы, нормативные акты, стандарты и прочее);
- административный (действия общего характера, предпринимаемые руководством организации);
- процедурный (конкретные меры безопасности, имеющие дело с людьми);
- программно-технический (конкретные технические меры).

Проработка каждого режимного уровня требует особого внимания, ведь изъян хотя бы одной детали целостной конструкции, обеспечивающей безопасность информационного ресурса, позволит злоумышленнику не только завладеть и использовать в своих целях данные, но и может нанести огромный ущерб владельцу информации. Здесь, под ущербом следует понимать не только денежные потери, но и временные затраты как на работу с самим рассматриваемым объектом, так и на обеспечение его защиты. Более того, нельзя забывать и о человеческих трудозатратах.

Реализация каждого метода выполняется за счет различных средств защиты информации.

Формальные (выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека):

- технические (физические и аппаратные);
- программные;
- специфические (например, криптографические).

Неформальные (регламентируют деятельность человека):

- законодательные (нормативно-правовые);
- организационные (административные);
- морально-этические.

В идеальном представлении каждая компонента системы ИБ должна безукоризненно выполнять поставленные перед ней задачи, при этом работать в единой согласованной структуре со всеми остальными компонентами.

Таким образом, одной из наиважнейших задач, поставленных перед образовательным процессом в части информационной безопасности, является подготовка высококвалифицированных специалистов. Такие специалисты должны обладать не только программно-техническими знаниями и навыками, но и в полной мере владеть как теоретической, так и практической организационно-правовой базой информационной защиты.

Так, рассмотрим на примере криптографические методы защиты ИБ.

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

- защиту конфиденциальности;
- защиту целостности.

Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы:

- шифрование;
- стеганография;
- кодирование;
- сжатие.

Специалисту области шифрования необходимо обладать высоким уровнем математических знаний, умений, применяемых на практике. Например, проведение математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляется в виде хаотического набора букв, цифр, других символов и двоичных кодов. Для шифрования информации используются алгоритм преобразования и ключ. Исходными данными для алгоритма шифрования служит информация, подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемых при реализации алгоритма шифрования. Кроме того, важным условием наличия навыка любого криптоаналитика является владение языком(ами) программирования в подходящей среде разработки. Этот навык необходим для обеспечения практической реализации задач данного раздела криптографической защиты.

При этом методы шифрования должны отвечать ряду требований:

- криптостойкость (вскрытие шифра осуществляется только полным перебором ключей);
- секретность ключа;
- шифртекст не существенно превосходит по объему исходную информацию;
- ошибки, возникающие при шифровании, не приводят к искажениям и потерям информации;
- не большое время шифрования;
- согласование стоимости шифрования со стоимостью закрываемой информации.

Стеганографические методы позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В основе всех методов стеганографии лежит сокрытие секретной информации среди открытой. Так, специализацией данной области становится обработка мультимедийных файлов в информационных ресурсах. Специалист должен иметь представление о графической и звуковой информации в числовом виде, уметь, например, кодировать объекты графического изображения, правильно подбирать алгоритмы преобразования к объекту, на котором помещается скрытый файл. По средствам стеганографии осуществляется маскировка текстов, изображений, речи, электронной подписи, зашифрованных сообщений.

В связи с несовершенствами любой защиты, применяются комбинированные методы, что многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации. Например, скрытый файл может быть зашифрован.

Отсюда делаем выводы, что знаний узкой направленности зачастую может быть просто недостаточно, чтобы осуществлять манипуляции в области ИБ.

Кодировщики информации должны не только осуществлять замену исходного смысла сообщения (слов, предложений) кодами, но и применять программно-аппаратные средства для повышения достоверности передаваемой информации.

Часто кодирование и шифрование ошибочно принимают как тождественные понятия, забыв о том, что для восстановления закодированного сообщения, достаточно знать правило замены, в то время как для расшифровки сообщения помимо знания правил шифрования, требуется ключ к шифру.

Сжатие информации требует наличие не только навыков всех вышеуказанных областей криптографического преобразования информации, но и обладание теоретико-практическими знаниями в области сокращения объема информации [2].

Выше, мы рассмотрели лишь небольшую часть области криптографического воздействия.

Одной из потенциально-важных идей (проблем) современного, не только научного мира, является создание не просто квантового компьютера, а так называемого универсального квантового компьютера. Это связано с огромным потенциалом данного оборудования для решения задач, которые лежат в основе современных информационных технологий.

Одной из важнейших проблем этой области является передача информации защищенным образом, начиная с осуществления покупок в интернет-магазинах банковской картой, заканчивая банальной перепиской в социальных сетях. И для реализации подобных действий применяется шифрование с ключом.

Данной областью (формирование ключа в частности) занимается криптография с открытым ключом. Происходит обмен какой-то информацией между субъектами через сервер, производится ряд вычислений и утверждается, что с использованием информации, которую мы огласили, очень трудно найти тот ключ, который мы сгенерировали, однако никем не утверждается обратное (нет такой математической теоремы, которая бы говорила, что это сделать невозможно). И примерами таких задач являются: дискретное логарифмирование или факторизация, на которых построены современные криптографические алгоритмы с открытым ключом Диффи-Хеллмана и RSA. Более подробно информацию можно изучить в статье [3].

Однако в 1996 году Питером Шором было показано, что при использовании в качестве элементарных вычислительных объектов не биты, а квантовые биты или кубиты и операции над ними, можно получить квантовый алгоритм факторизации, который работает принципиально быстрее, чем классические алгоритмы.

В настоящее квантовый компьютер еще не создан, но, в случае создания, он действительно потенциально может решать задачи факторизации и дискретного логарифмирования. Уже разработаны не универсальные прототипы, исследованиями которых занимается в частности Google [1].

Помимо прочего, криптографы зачастую используют алгоритмы, основанные на природных системах, методы моделирования отжига, генетические алгоритмы, эволюционные методы, алгоритмы роевого интеллекта и т.д. В моделях и алгоритмах эволюционных вычислений ключевым элементом является построение начальной модели и правил, по которым она может изменяться (эволюционировать). В настоящее время разнообразные схемы эволюционных вычислений, в том числе генетический алгоритм, генетическое программирование, эволюционные стратегии, эволюционное программирование активно разрабатываются, применяются и модернизируются в технологически-научных кругах.

Революционные изменения в жизни общества ставят новые и все более трудоемкие задачи в области информационных технологий. Защите же данного ресурса выделяют, если не ключевую, однозначно главенствующую роль. Но, помимо современных угроз, остро ощущаются сложности в освоении квантовых технологий в общем и, как следствие, в квантовой криптографии в частности. "Живая" криптография активно развивается и эволюционирует в современной информационно-защищаемой среде. Находят свое применение в области информационной безопасности, как генетические, так и биоинспирированные алгоритмы. Данная область является весьма перспективной в плане развития и применения технологий на практике. Более того, данные алгоритмы в криптографии возможно перенести даже в область квантовой защиты, как возможную перспективу. «Гонкой за вооружением» в ИБ занимаются не только страны-разработчики, но сам факт создания вычислительно сложных и мощных устройств требует специалистов высокого уровня. Более того, даже прогнозирование предметной области ИБ является трудоёмкой задачей.

Список литературы

1. Бёрд Киви Суета заранее, или Постквантовые тайны криптографии / А. И. Дирина [Электронный ресурс] // 3DNews Offсянка : сетевой журн. – 2016. – Режим доступа: http: //3dnews.ru/940050 (дата обращения:04.10.2016).

2. Технологии защиты информации в компьютерных сетях [Криптографические методы защиты информации]: для всех / Андрей Пролетарский [и др.] — Московский государственный университет им. Н.Э. Баумана.

3. Большакова А.А. Электронная подпись — обучающие и тестирующие комплексы/ А.А. Большакова// Информационные технологии в образовании и науке: материалы Междунар. науч.-практ.конф., 5-7 нояб. 2016 г., г. Казань. / КФУ — Казань, 2016. — С. 12–19.

4. Потапова Н.В. Дистанционное образование, как электронный документооборот/ Н.В. Потапова// Информационные технологии в образовании и науке: материалы Междунар. науч.-практ.конф., 5-7 нояб. 2016 г., г. Казань. / КФУ — Казань, 2016. — С. 166–172.

УДК 378:001.891

В. В. Братищенко

МОДЕЛЬ С ЛАТЕНТНЫМИ ПАРАМЕТРАМИ ДЛЯ ОЦЕНКИ КОМПЕТЕНЦИЙ

Братищенко Владимир Владимирович
vbrat56@mail.ru
ФГБОУ ВО «Байкальский государственный университет», Россия, г. Иркутск

MODEL WITH LATENT PARAMETERS FOR THE ASSESSMENT OF COMPETENCES

Bratishchenko Vladimir Vladimirovich
Baikal State University, Russia, Irkutsk

Аннотация. *В статье обосновывается подход к оцениванию компетенций на основе текущей успеваемости. Предлагается каждое задание разбить на компоненты и связать каждую компоненту с определенной компетенцией. Разработаны структуры данных системы учета текущей успеваемости и архитектура системы. Для регистрации оценок разработано приложение для мобильных устройств. Оценивание компетенций предлагается проводить на основе теории латентных переменных (Item Response Theory).*