Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт педагогики, психологии и социологии
Кафедра информационных технологий обучения и непрерывного образования

УТВЕРЖДАЮ
Заведующий кафедрой
_____ О.Г. Смолянинова
подпись
« ____» _____ 2016 г.

БАКАЛАВРСКАЯ РАБОТА

44.03.01 Педагогическое образование
44.03.01.09 Информатика и информационные технологии в образовании

Разработка дистанционного курса «Методы и средства защиты информации в облачных технологиях и сети интернет» для старшей школы

Руководитель _____ доцент, канд. пед. наук Д.Н. Кузьмин
подпись, дата

Выпускник _____ И.В. Копейкин
подпись, дата

Красноярск 2016

Содержание

Введение

Актуальность:

Мы живём в 21-ом веке. В веке технологического прогресса, когда каждый день изобретают что-то новое. Когда почти каждый день появляются новые разные сервисы. Когда хранить информацию в сети интернет считается одной из удобных и безопасных функций. Всё это привело к тому, что большинство людей и организаций стали хранить информацию в электронном виде. Конечно, способы защиты информации постоянно меняются, как меняется наше общество и технологии – соответственно возникла потребность в защите такой информации.

Проблема – достаточная ли степень защиты информации и персональных данных в различных сервисах (у облачных технологий) на сегодняшний день?

Объект исследования – информационная безопасность.

Предмет исследования – дистанционный курс «Методы и средства защиты информации в сети интернет и облачных технологиях».

Цель – разработать дистанционный курс для детей старшей школы на базе сервиса Google Blogger – Методы и средства защиты информации в облачных технология и сети интернет.

Задачи:

1. Охарактеризовать методы и средства защиты информации в сети, их классификацию и особенности применения;
2. Изучить современные средства дистанционного обучения, а также проанализировать существующие дистанционные курсы;
3. Разработать серию уроков по Методам и средствам защиты информации в облачных технологиях и сети интернет;
4. Провести проверку:
   - проведение финального анкетирования;
   - проведение нескольких контрольных тестирований;
   - описание результатов проведения анкетирования и тестирования.

Гипотеза – предполагается, что если осуществить разработку дистанционного курса по Методам и средствам защиты информации в облачных технологиях и сети интернет, то у детей старшей школы появится понимания о том, что такое информационная безопасность в сети интернет и облачных сервисах.

Методы исследования дипломной работы:

- анализ литературы;
- анализ документов;
- сравнение;
- изучение и обобщение отечественной и зарубежной практики.

1. Текущее положение вещей в сфере защиты информации

1.1. Анализ методов и средств защиты информации в сети интернет и облачных технологиях

Предлагаем начать с рассмотрения методов и средств защиты информации непосредственно в сети интернет. Разберём некоторые термины, основные задачи и принципы работы методов и средств защиты информации.

В современных условиях деятельность большинства организаций в значительной степени автоматизирована. Электронный документооборот часто преобладает над бумажным; электронная почта, программы видеоконференцсвязи на сегодняшний день стали неотъемлемой частью делового общения [2].

Защита информации в компьютерных системах — это регулярное использование средств и методов, принятие мер и осуществление мероприятий в целях системного обеспечения требуемой надежности информации, хранимой и обрабатываемой с использованием средств вычислительной техники [5].

Под информационной безопасностью понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности [24].

Средства защиты информации – это технические, программные, программно-технические средства, предназначенные или используемые для защиты информации [16].

Известно, что объект информатизации, а также создаваемая для обеспечения его информационной безопасности система защиты информации подвержены воздействию угроз информационной безопасности. Непосредственное обеспечение информационной безопасности достигается за счет использования средств защиты информации [23].

Множественные угрозы, возникающие в отношении информационной безопасности, предусматривают использование разных методов и способов организационного, инженерно-технического, программно-аппаратного,

правового, криптографического характера и т.п. Мы же рассмотрим программно-аппаратные и криптографические способы противодействия угрозам безопасности.

Программно-аппаратные средства защиты непосредственно применяются в компьютерах и компьютерных сетях (далее КС), содержат различные встраиваемые в КС электронные и электромеханические устройства. Специальные пакеты программ или отдельные программы реализуют такие функции защиты, как разграничение и контроль доступа к ресурсам, регистрация и анализ протекающих процессов, событий, пользователей, предотвращение возможных разрушительных воздействий на ресурсы и другие [12].

Криптографическая защита же преобразовывает информацию к зашифрованному виду с помощью различных алгоритмов или аппаратных средств.

Разработка политики безопасности является ключевым этапом построения защищенной информационной системы или сети. Следует отметить, что составление политики безопасности или политик является только началом осуществления общей программы обеспечения безопасности организации [28].

А теперь обратимся к основным программным методам защиты информации от наиболее часто встречаемых угроз непосредственно в сети интернет. А именно:

– несанкционированный доступ;
– копирование различных данных;
– вредоносные программы (вирусы).

Основным способом защиты вашего компьютера от несанкционированного доступа считается использование так называемых средств «3А». Ниже немного поподробней об этих средства:

– авторизация — процедура, по которой пользователь при входе в систему опознается и получает права доступа, разрешенные системным администратором, к вычислительным ресурсам (компьютерам, дискам, папкам, периферийным устройствам);

– аутентификация — проверка подлинности, то есть того, что предъявленные данные действительно принадлежат пользователю. Происходит проверка имени пользователя и пароля. После аутентификации пользователь получает доступ к ресурсам системы;

– администрирование — это регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. Для своевременного пресечения несанкционированных действий [24].

Чаще всего к применяемым методам авторизации относят методы, основанные на использовании паролей. Пароль можно установить, как на запуск программы, так и на отдельные действия на компьютере или в сети.

Также, несанкционированное копирование информации может быть заблокировано различными методами. Немного подробнее о методах ниже:

– метод, работает как функция, которая затрудняет считывание скопированной информации. Основан метод на создании в процессе записи информации на накопителях такие особенности, которые не позволяют считывать полученную копию на других накопителях. Если говорить проще, этот метод обеспечивает совместимость накопителей только внутри данной компьютерной системы;

– метод, затрудняющий использование информации, полученной копированием программ и данных. Другим методом противодействия несанкционированному копированию программ является использование блока контроля среды размещения программы. Он создается при установке программы и включает характеристики среды, в которой размещается программа [3].

Для защиты компьютерных систем от вирусов разрабатываются специальные антивирусные программы. Антивирусная программа обнаруживает вирусы, предлагая вылечить файлы, а при невозможности — удалить. Существует несколько разновидностей антивирусных программ:

– сканеры или программы-фаги — это программы поиска в файлах, памяти, загрузочных секторах дисков сигнатур вирусов (уникального программного кода именно этого вируса), проверяют и лечат файлы;

– мониторы (разновидность сканеров) — проверяют оперативную память при загрузке операционной системы, автоматически проверяют все файлы в момент их открытия и закрытия, чтобы не допустить открытия и запись файла, зараженного вирусом; блокирует вирусы;

– иммунизаторы — предотвращают заражение файлов, обнаруживают подозрительные действия при работе компьютера, характерные для вируса на ранней стадии (до размножения), и посылают пользователю соответствующее сообщение;

– ревизоры — запоминают исходное состояние программ, каталогов до заражения и периодически (или по желанию пользователя) сравнивают текущее состояние с исходным;

– доктора — не только находят зараженные вирусами файлы, ни и «лечат» их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние;

– блокировщики — отслеживают события и перехватывают подозрительные действия (производимые вредоносной программой), запрещают действие или запрашивают разрешение пользователя.

Эффективным средством борьбы с различными угрозами информационной безопасности является сокрытие информации методами криптографического преобразования. В результате преобразования информация становится недоступной для использования пользователям, не имеющих доступа к тем или иным файлам. Также, криптографические методы разделены на следующие виды:

– шифрование — процесс маскирования сообщений или данных в целях скрытия их содержания, ограничения доступа к содержанию других лиц. Заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Для шифрования используются алгоритм преобразования и ключ.

Так, при перехвате зашифрованных сообщений и постоянном ведении криптоанализа нарушитель накапливает информацию об используемом методе шифрования, что в отсутствие смены ключей шифрования приводит к снижению уровня защищенности передаваемых сообщений и увеличению вероятности несанкционированного доступа (НСД) к ним нарушителя [14];

– стеганография — метод защиты компьютерных данных, передаваемых по каналам телекоммуникаций, путем скрытия сообщения среди открытого текста, изображения или звука в файле-контейнере. Позволяет скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы;

– кодирование — замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари, хранящиеся в секрете. Кодирование широко используется для защиты информации от искажений в каналах связи;

– сжатие информации — сокращение объемов информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Поэтому сжатые файлы подвергаются последующему шифрованию;

– рассечение-разнесение заключается в том, что массив защищаемых данных делится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделенные таким образом элементы данных разносятся по разным зонам ЗУ или располагаются на различных носителях;

– электронная цифровая подпись представляет собой строку данных, которая зависит от некоторого секретного параметра (ключа), известного только подписывающему лицу, и от содержания подписываемого сообщения, представленного в цифровом виде. Используется для подтверждения целостности и авторства данных, нельзя изменить документ без нарушения целостности подписи [5].

Для защиты приложений, с практической точки зрения, можно воспользоваться двумя вариантами проверки не только наличия, но и соответствия ключа приложению: генерация электронной цифровой подписи и ее проверка, генерация массива ответов ключа на запросы программы по одному из алгоритмов шифрования [13].

Чтобы блокировать угрозы, исходящие от общедоступной системы, используется специальное программное или аппаратно-программное средство, которое получило название межсетевой экран или Брандмауэр (firewall). Брандмауэр позволяет разделить сеть на две части или более, а также реализовать набор правил, которые определяют условия прохождения пакетов с данными через стену межсетевого экрана из одной части общей сети в другую. Бывает такое, что сетевая защита может полностью заблокировать трафик, поступающий снаружи во внутрь, но оставляет права пользователям на свободный доступ в сеть интернет. Обычно брандмауэр защищает внутреннюю сеть пользователя от вторжений из глобальной сети Интернет. Таким образом, можно выделить четыре основные функции межсетевого экрана:

- фильтрация данных на разных уровнях;
- использование так называемых прокси-серверов, которые являются программами-посредниками и обеспечивают соединение между двумя пользователями (и более), а затем пересылает информацию, осуществляя контроль и регистрацию;
- трансляция адресов предназначена для скрытия от внешних угроз настоящих внутренних адресов;

– регистрация событий в специальных журналах. Анализ записей позволяет зафиксировать попытки нарушения установленных правил обмена информацией в сети.

Многие задачи информационной безопасности хорошо теоретически описаны и с ними справляются операторы систем. Эти операторы действуют по заранее разработанным инструкциям и алгоритмам принятия решения. Конечно, не все задачи информационной безопасности можно описать в таком виде [26].

В любом случае, все эти меры безопасности меркнут перед самой главной уязвимостью в безопасности – человеческий фактор. Какие бы меры предосторожности ни были применены, человек всегда может посчитать, что устройство безопасно, и разрешить подключение, тем самым открыв прямую дорогу уязвимости [18].

Таким образом, можно сделать следующий вывод. Актуальность вопросов защиты информации возрастает с каждым годом. На сегодняшний день, многие пользователи сети интернет считают, что данную проблему можно решить установкой антивирусных программ и брандмауэра, но для обеспечения надежной защиты в первую очередь необходима информация о существовании таких угроз и методах борьбы с ними. Это также относится не только к специалистам, работающим в области информационных технологий, но и ко всем, пользователям сети интернет.

Во-второй части первого параграфа, мы рассмотрим методы и средства защиты информации уже непосредственно в облачных технологиях. Принцип работы будет примерно таким же, как и в первом части.

Не секрет, что облачные технологии сейчас находятся на волне популярности: экономичность, легкость развертывания, многопользовательская архитектура – все это способствует быстрому распространению облаков и захвату ими большей части рынка информационных технологий. На сегодняшний день, экономичность облаков делает их особенно популярными для хранения различной информации.

Современные интернет-технологии стали доступными и занимают важное место практически во всех областях человеческой деятельности, включая и образование. Опираясь на опыт развитых зарубежных стран, отличным решением для оптимизации учебного процесса являются облачные технологии, доступ к которым осуществляется через сеть Интернет [17].

Основной принцип облачных технологий заключается в том, что информация хранится и обрабатывается средствами веб-сервера, а результат данных вычислений предоставляется пользователю посредством веб-браузера. Пользователи получают возможность создавать и редактировать текстовые документы, математические таблицы, простые векторные изображения, редактировать графические файлы, создавать и демонстрировать компьютерные презентации, использовать дисковое пространство провайдера для хранения резервных копий данных [8]

Одним из необходимых условий для перехода к использованию облачных технологий является модернизация информационно-телекоммуникационной инфраструктуры, обычно скрытой от пользователя [15].

Но, к сожалению, облачные сервисы также представляют повышенные риски и более ограниченную возможность контроля. Именно в этом заключаются главные проблемы облачных технологий.

Технологии облачных вычислений позволяют избегать привязки физических серверов к конкретным приложениям и отдельным пользователям. Работая в облаке, пользователь выбирает те программные приложения, которые ему необходимы для работы [9].

Возникает следующий вопрос – так как же убедить пользователей, что их данные будут в безопасности? Решением будет являться тот факт, который обеспечивает соответствие облачных технологий требованиям нормативных документов и стандартов в области обеспечения информационной безопасности. К сожалению, в российском законодательстве пока нет нормативных стандартов, которые бы описывали принципы построения защиты информации в облачных технологиях. Отсюда следует, что люди, которые создают и предоставляют

пользователям различные облачные услуги вынуждены сами выбирать способы защиты информации из различных готовых решений, представленных на рынке. Но все средства защиты должны учитывать особенности облачных технологий [1].

Самыми важными элементами облачной системы являются:

- гипервизор, управляющий виртуальной средой облака;
- центр обработки данных, на котором содержится большая часть конфиденциальной информации;
- канал связи между пользователем облачного сервиса;
- ПО, установленное на компьютере пользователем (в частности, интернет-браузер).

Все выше перечисленные элементы, к сожалению, могут быть подвержены различным атакам со стороны злоумышленников. Например, при успешной атаке на любой из элементов облачной системы каждый аспект безопасности информации может быть нарушен.

Ключевым моментом для возможности предоставления облачных сервисов широкому спектру устройств является создание двусторонней информированности между облаком и клиентом. Очевидно, что, с одной стороны, не все клиентские устройства имеют одинаковые возможности, с другой – облако в разных ситуациях имеет разную доступность для клиентских устройств. Поэтому единая модель предоставления сервисов не может быть эффективной [20].

Сегодня такие крупнейшие мировые ИТ-корпорации как Amazon, Google, Microsoft и др. активно занимаются облачными технологиями, предоставляя пользователям платно либо бесплатно (в рекламных целях) многочисленные сервисы, которые сводятся к следующим блокам или типам:

- инфраструктура как услуга (IaaS) – предоставление в аренду оборудования, главным образом серверов;
- платформа как услуга (PaaS) – предоставление в аренду операционных систем, систем управления базами данных;

– программное обеспечение как услуга (SaaS) – предоставление в аренду программного обеспечения.

Другими примерами сервисов могут быть хранение информации как услуга (STaaS), системы безопасности как услуга (SECaaS) и т.д [6].

Как и любая другая система, функционирующая посредством сети Интернет, облачные технологии подвержены атакам. Основные виды атак приведены ниже:

– традиционные атаки на ПО;
– атаки на пользователя;
– сетевые атаки;
– атаки на серверы облака.

Спланированная удаленная атака на облачную инфраструктуру может классифицироваться как киберпреступление и осуществляться в виде организации несанкционированного доступа к конфиденциальной информации или внедрения вредоносного кода с целью нарушить работоспособность системы информационной безопасности [11].

Использование технологии облачных вычислений осуществляется на основе виртуализации программных и технических ресурсов, что добавляет новые слои технологий и приводит к возрастанию управленческих затрат на обеспечение безопасности и требует привлечения дополнительных специализированных мер и средств защиты информации [7].

В системах защиты, связанных с облачными вычислениями, можно выделить два основных направления:

– технологии защиты, использующие в своей основе архитектуру облачных вычислений и/или предоставляющие сервисы, функционирующие на основе облака;
– технологии, предназначенные для защиты облачных систем (платформ или сервисов).

Данные направления достаточно тесно связаны между собой, поскольку различия между атаками на облако и атаками на обычные системы незначительны и реальные системы могут сочетать в себе оба подхода [10].

Для обеспечения информационной безопасности облаков система защиты информации должна включать в себя:

- подсистему обеспечения безопасности информации на стороне пользователя;
- подсистему обеспечения сетевой безопасности;
- подсистему обеспечения безопасности виртуальных сред;
- подсистему обеспечения безопасности центров обработки данных.

Как и в любой другой системе защиты информации, безопасность системы в целом зависит от безопасности всех ее частей. Далее подробнее рассмотрим каждую подсистему в отдельности.

Подсистема обеспечения безопасности информации на стороне пользователя. Пользователи работают с сервисом облачных технологий с помощью интернет-браузера, поэтому подвержены таким атакам, как межсайтовый скриптинг (Cross-site-scripting), фишинг (fishing), а также вирусы и трояны.

Таким образом, подсистема обеспечения безопасности информации на стороне пользователя состоит из следующих элементов:

- антивирусные средства защиты информации;
- средства шифрования данных на диске;
- встроенный в ОС персональный брандмауэр;
- безопасно настроенный интернет-браузер.

Подсистема обеспечения сетевой безопасности. Для защиты данных в публичном облаке используется туннель виртуальной частной сети (VPN), который обеспечивает связь между пользователем и сервером для получения публичных облачных услуг. VPN туннель предоставляет безопасное соединение и позволяет использовать единое имя и пароль для доступа к разным облачным

ресурсам. В качестве средства передачи данных в публичных облаках VPN-соединение пользуется общедоступными ресурсы, такими как Интернет.

Подсистема обеспечения безопасности виртуальных сред. При успешной атаке на гипервизор нарушитель может незаметно для традиционных систем защиты информации (далее СЗИ), работающих в виртуальных машинах:

- копировать и блокировать весь поток данных, идущий на все устройства;
- читать и изменять данные на дисках виртуальных машин, даже когда они выключены и не работают, без участия программного обеспечения этих виртуальных машин.

Для защиты гипервизора необходимы разграничение прав доступа к серверу, своевременная установка обновлений ПО среды виртуализации, ограничение запуска программ.

Виртуальная машина исполняется на сервере виртуализации, а ее диск хранится на SAN/NAS. Следовательно, необходимо защитить данные виртуальных машин путем разграничения доступа к дискам виртуальных машин, реализуемого сертифицированными СЗИ от НСД и межсетевыми экранами, контролирующими протоколы и файловые форматы виртуальной инфраструктуры [30].

Получив доступ к средствам администрирования, нарушитель имеет возможность похитить, уничтожить или испортить любые данные во всей виртуальной инфраструктуре. В связи с чем, возникает потребность в надёжной защите сети администрирования путем разграничения доступа к серверам виртуальных машин и средствам управления инфраструктурой.

Виртуальные машины одного физического сервера могут обмениваться трафиком напрямую, без участия физических сетевых коммутаторов. Таким образом, использование физических межсетевых экранов не будет эффективным.

По сети репликации виртуальных машин передаются сегменты их оперативной памяти. Возможность перехвата этих данных – прямая угроза

безопасности. Сеть репликации должна быть изолирована от других сетей, а также необходимо использовать сертифицированные VPN для канала репликации.

Простота создания и ввода в эксплуатацию виртуальных машин может привести к проблемам для безопасности, если к ним не применяется политика безопасности.

Требуется организация централизованного процесса управления жизненным циклом виртуальных машин, согласующегося с политикой безопасности организации [27].

Подсистема обеспечения безопасности центров обработки данных. Центр обработки данных (далее ЦОД) обеспечивает гарантированную безотказную работу информационной системы с заданными уровнями безопасности, надежности и доступности. Использование такой технологии позволяет создавать резервные хранилища данных без потери функциональности информационной системы.

Основными объектами защиты в ЦОД являются оборудование, конфиденциальная информация и ПО. Подсистема обеспечения безопасности центров обработки данных включает в себя следующие элементы:

- охранное видеонаблюдение;
- охранно-пожарная сигнализация;
- система контроля и управления доступом;
- система резервного копирования и восстановления данных;
- система защиты информации в ЦОД.

Системы охранного видеонаблюдения позволяют сотрудникам службы безопасности осуществлять визуальный контроль обстановки на объекте. Видеонаблюдение дает возможность не приставлять к каждому серверу своего охранника: контроль объекта ведется дистанционно, круглосуточно, без выходных и праздников. Кроме того, запись видео с камер позволяет в любое

время организовать просмотр того или иного инцидента с целью выявления нарушения.

При обеспечении безопасности ЦОД должно уделяться внимание таким угрозам, как пожар, задымление и т. п., и необходимо оперативное оповещение о них сотрудников организации и службы безопасности. Следовательно, автоматическая система пожаротушения – один из самых эффективных методов экстренного пожаротушения. Данная система воздействует на очаг возгорания еще в процессе его зарождения, позволяет избежать распространения огня на большой площади и, соответственно, минимизирует ущерб.

Система контроля и управления доступом осуществляет автоматическое управление входами-выходами и призвана разграничивать доступ людей на определенные территории, вести подсчет посетителей, фиксировать их перемещения по территории и т. д. Система также способна распознавать лица, цвета, автомобильные номерные знаки и т. п. и на основе полученной информации принимать решение о доступе объекта или предмета, обладающего данными признаками, к определенной зоне [4].

В качестве компонентов системы информационной безопасности ЦОД должны выступать следующие элементы:

- система централизованного управления средствами защиты информации;
- средства обнаружения и предотвращения вторжений;
- средства антивирусной безопасности;
- средства криптографической защиты информации (шифрование файлов, прозрачное шифрование жестких дисков, шифрование выбранных полей в БД);
- средства межсетевого экранирования;
- средства разграничения доступа;
- средства мониторинга и управления событиями;
- средства контроля целостности информации и приложений.

Облачные вычисления представляют собой значительный прогресс в сфере развития информационных технологий и сервисов. Обеспечивая по требованию

пользователя доступ к общим источникам вычислительных ресурсов в автономном, динамично масштабируемом и выверенном режиме, облачные вычисления предлагают очевидные преимущества в скорости, оперативности и эффективности.

Для успешного развития проектов, связанных с переходом к облачным вычислениям, необходимо уделять вопросам обеспечения информационной безопасности повышенное внимание. В частности, для общедоступного типа облаков наиболее актуальными становятся вопросы управления доступом пользователей и хранения информации ограниченного доступа, в частности, персональных данных, в зашифрованном или обезличенном виде [21].

Таким образом, можно сделать следующий вывод – в данной технологии безопасность играет важнейшую роль, этой проблеме специалисты уделяют особое внимание. Но, несмотря на все сложности в области безопасности, преимущества предоставляемых через Интернет сервисов перевешивают возможные риски и облачные вычисления будут широко востребованы на рынке информационных технологий.

1.2. Обзор современных средств дистанционного обучения и существующих дистанционных курсов по выбранной тематике

Чтобы рассмотреть средства дистанционного обучения, предлагаю сначала ознакомиться с понятием самого Дистанционного обучения.

Под дистанционным обучением следует понимать способ реализации учебного процесса, основанный на использовании современных информационных и коммуникационных технологий, а также специальных дидактических принципов, позволяющих осуществлять обучение на расстоянии без непосредственного, личного контакта между преподавателем и обучающим [29].

Объединение компьютеров в единую глобальную сеть даёт возможность систематического взаимодействия преподавателя и обучающихся, а также обучающихся между собой. К Интернет-технологиям взаимодействия можно отнести электронную почту, видеоконференции реального времени, форумы, чаты, а также среды дистанционного обучения (например, Moodle). Остановимся на дистанционном обучении.

Динамика информационных технологий стимулирует развитие системы дистанционного обучения, которые характеризуются высоким уровнем интерактивности и позволяют участвовать в процессе обучения в любое удобное время людям, находящимся в разных странах и имеющим выход в Интернет в удобном для человека ритме познавательной деятельности. Как и все активно развивающиеся технологии, облачные технологии ввиду своих явных плюсов проникают во все сферы человеческой жизни. Разумеется, в разных областях их внедрение происходит с разной скоростью [22].

Современные технологии позволяют разрабатывать новые средства обучения. Например, учебники с компьютерной поддержкой, учебно-информационные видео и аудиоматериалы, обучающие веб-сайты и презентации, компьютерные обучающие программы, включающие в себя электронные учебники, тренажеры, лабораторные практикумы, тестовые системы.

Далее предлагаем рассмотреть непосредственно преимущества дистанционного обучения.

В настоящее время благодаря развитию современных электронных и телекоммуникационных средств обучения стало популярным создавать различные дистанционные курсы, которые могли бы облегчить процесс получения знаний как людям, у которых нет возможности по той или иной причине обучаться в вузах, так и для тех, кому удобней получать знания, не выходя из дома, в своей привычной и спокойной обстановке. Также стремительно увеличивается объём информации, что влечёт за собой необходимость непрерывного обучения.

При рассмотрении процесса дистанционного обучения можно отметить различные форма и модели организации обучения, но при всех своих различиях и особенностях, они направлены на преодоление ограничений, который связаны с традиционным обучением. А именно:

- относительно невысокая численность студентов, обучающихся в традиционных учебных заведениях и невозможность принять на обучение всех желающих;
- большой объем аудиторных занятий и связанная с этим необходимость поездок и присутствия в образовательном учреждении;
- расписание занятий, которое может не позволять совместить обучение с другой деятельностью студента.
- дистанционное обучение позволяет организовать учебный процесс на принципах:
- открытости – приём всех желающих обучаться;
- гибкости – обучаемый сам организует свой индивидуальный учебный план;
- дистанционности – возможность обучения по месту жительства или работы.

В систему дистанционного образования входят такие базовые принципы как: стандартизация, универсальность и открытость. На основе данных принципов можно выделить следующие характеристики:

- системность;
- интерактивность взаимодействия с обучаемым;
- многофункциональность;
- высокая адаптивность обучаемых к разнообразию требований;
- технологическая мобильность.

Дистанционное обучение даёт возможность студентам получения второго образования, а также позволяет осуществлять подготовку и переподготовку, повышение квалификации специалистов по дополнительным профессиональным образовательным программам вне зависимости от места жительства.

Данный способ обучения организует доступ студентов к нетрадиционным источникам информации, а также повышает их мотивацию к самостоятельной работе, дает новые возможности для творческой деятельности, обретения и закрепления различных профессиональных навыков.

Далее предлагаем перейти непосредственно к разбору некоторых платформ для организации дистанционного обучения.

Анализ платформ для дистанционного обучения будет происходить следующим образом:

- кем была разработана данная платформа;
- возможности платформы;
- плюсы платформы;
- недостатки платформы.

Moodle. Разработка австралийских программистов стала самой популярной и массово используемой в мире, в т.ч. России, готовой платформой для LMS. Пользователями системы являются более восемнадцати млн.человек, а количество созданных с ее помощью курсов приближается к двум млн.

Представляет собой готовое коробочное решение, является полностью бесплатной и ее можно свободно скачать в сети Интернет.

Возможности платформы:

- учет учащихся, возможности их персонализации и разграничения прав доступа к учебным материалам;
- создание и проведение онлайн-курсов;
- ведение отчетности и статистики по обучению;
- контроль и оценка уровня знаний;
- анкетирование и создание опросов;
- возможность интеграции с другими информационными системами.

Основные преимущества платформы Moodle:

- доступность;
- простота использования;
- высокая производительность;
- поскольку платформа распространяется в открытом исходном коде, имеется возможность ее адаптации под конкретные нужды;
- простота инсталляции и обновления.

Некоторые недостатки:

- отсутствие понятия семестра в базовой версии системы и как следствие невозможность составить итоговую ведомость по всем дисциплинам семестра;
- невозможность создания учебных групп по уровням, создание групп обучаемых возможно только внутри курса.

Вместе с тем, среди бесплатных платформ для дистанционного обучения Moodle является наиболее удачным ПО, не уступающим по своим возможностям платным программам.

WebTutor. Одна из наиболее популярных платформ дистанционного обучения российского разработчика – компании WebSoft. Состоит из нескольких модулей:

- модуля управления дистанционным обучением (с встроенным редактором учебных курсов, интерактивных упражнений и тестов/контрольных вопросов);
- модуля управления учебным порталом (имеет редактор информационных материалов, хранилище организационной структуры, управляет и модерирует форумы);
- шлюза для обмена с информацией с другими системами (возможность загрузки данных из систем учета персонала, интеграция с другими платформами, экспорт данных в хранилище и пр.).

Преимуществами платформы WebTutor является наличие готовых курсов, масштабируемость, поддержка формата SCORM, позволяющая обеспечить совместимость компонентов и их многократное использование в различных учебных курсах.

К недостаткам пользователи относят:

- не очень удобный интерфейс;
- слабая кастомизация сервиса;
- необходимость докупать дополнительные модули (например, базовая версия не содержит модуль для проведения онлайн-конференций, а является отдельной услугой).

IBM Lotus Workplace Collaborative Learning (LWCL). Разработка компании IBM. Представляет собой универсальную, надежную, гибкую и легко масштабируемую платформу для организации традиционного дистанционного электронного обучения, управления учебными ресурсами и материалами. Может использоваться как для профессионального обучения и повышения квалификации в крупных компаниях и холдингах, так и в учебных заведениях.

Возможности:

- широкие возможности для управления учебным процессом (причем как традиционным, так и дистанционным и смешанным);
- создание календарей и составление расписаний учебных занятий;

– возможность создания и импорта учебных материалов, управление каталогом курсов;
– возможность составления и отслеживания программ обучения;
– отслеживание результатов обучения и тестирования;
– возможность ведения дискуссий и обмена сообщениями.

К недостаткам системы можно отнести привязку к решениям IBM и ограниченную русскоязычную локализацию.

Прометей. Еще одна разработка российских специалистов. Представляет собой готовый продукт или разработку системы обучения под нужды конкретного заказчика, реализуемую по системе Saas.

Система имеет модульную архитектуру, поэтому предоставляет хорошие возможности для расширения и модернизации продукта.

Количество базовых модулей достаточно велико. Основными из них являются:

– типовой Web-узел, представляющий собой набор HTML страниц с информацией об учебном центре, списке курсов, дисциплин и тьюторов;
– АРМ «Администратор». С этого модуля администратор выполняет управление системой, предоставляет права доступа, регистрирует новых тьюторов и т.д.;
– АРМ «Организатор». Формирует группы обучающихся, регистрирует слушателей, контролирует оплату обучения, осуществляет рассылку учебных материалов;
– АРМ «Тьютор». Обеспечивает консультирование обучающихся, контролирует успеваемость, осуществляет проведение тестирований, проставление оценок и направление отчета об успеваемости слушателя его непосредственному руководителю;
– АРМ «Слушатель». Обеспечивает обучающегося всеми учебными материалами, организует процесс выполнения лабораторных работ, сдачи тестов, работы над ошибками.

Существуют также модули:

- трекинг – для контроля и создания отчета о тех, кто читал или просматривал курсы;
- курс – обеспечивает доступ слушателей к курсам;
- регистрация;
- тест;
- дизайнер тестов;
- учет;
- отчеты;
- дизайнер курсов.

К недостаткам платформы можно отнести привязку к продуктам Microsoft и недостаточную масштабируемость.

Shareknowledge. Разработка компании Competentum. Представляет собой бесплатное коробочное решения. Основное преимущество – возможность самостоятельной организации всего цикла дистанционного обучения, от разработки курсов, и подготовки и проведения до управления занятиями и контроля уровня знаний слушателей. В качестве учебных материалов могут использоваться любые текстовые и мульмедийные файлы.

Отдельно хочется отметить системы, предназначенные для краткосрочного дистанционного обучения в виде конференций, вебинаров и тренингов. Лучшими, по мнению большинства пользователей, платформами в данном сегменте являются:

- платформы Webinar и Comdi от компании «Вебинар-Комди», позволяющие организовывать онлайн-конференции с числом участников до 500 человек;
- платформа iMind, разработка компании Mind Labs. Предназначена для проведения вебинаров и видеосовещаний;
- «Виртуальный класс» от компании WebSoft (может использоваться в качестве дополнительного платного модуля для платформы WebTutor);

– Acrobat Connect Pro, разработка компании Adobe Systems Incorporated. Предоставляет широкие возможности для проведения онлайн-конференций. Доступен в версиях Premium Basic (рассчитана на число участников до 5 человек и сохранение 10 документов в формате PDF) и Premium Plus (до 21 участника и без ограничений по загружаемым документам).

Claroline LMS. Это платформа для электронного обучения (eLearning) и электронной деятельности (eWorking), позволяющая учителям создавать эффективные онлайн-курсы и управлять процессом обучения и совместными действиями на основе веб-технологий. Переведённая на 35 языков, Claroline LMS обладает обширным сообществом пользователей и разработчиков по всему миру.

Claroline LMS выпущена на основе лицензии с Открытым Кодом (Open Source). Она применяется в сотнях организаций 90 стран мира. Она позволяет создавать и администрировать курсы в режиме онлайн.

Каждый курс содержит ряд инструментов, позволяющих преподавателю:

– указать описание курса;
– опубликовать документы в любом формате (текст, PDF, HTML, видео);
– администрировать публичные и приватные форумы;
– разрабатывать пути обучения;
– объединять студентов в группы;
– подготавливать для обучающихся онлайн упражнения (задания);
– управлять повесткой дня с задачами и сроками выполнения;
– публиковать анонсы (так же и по эл.почте);
– вывешивать онлайн информацию о текущих заданиях;
– просматривать статистику активности пользователей;
– использовать технологию wiki для совместного написания документов.

Claroline LMS используется не только школами и университетами, но также и тренинговыми центрами, ассоциациями и компаниями. Платформа настраиваемая и предлагает гибкую среду для разработки под конкретный заказ.

Google Blogger. Google Blogger является полностью бесплатной для использования. Вы сможете создать свой собственный веб-сайт с отличным дизайном и полной функциональности без каких-либо инвестиций. Более того, платформа дает вам бесплатный хостинг с выбранным доменным именем.

Возможности Google Blogger:

- интуитивно-понятный интерфейс, который можно легко освоить. Всё подписано, имеется подробная справка, никакие элементы при нажатии не разъезжаются в стороны, можно делать предварительный просмотр во время любого редактирования;
- дизайн редактора постов и панели управления упрощены донельзя. Это позволяет полностью сконцентрироваться на посте, не обращать внимания на ненужные кнопки и элементы интерфейса;
- быстродействие редактора позволяет практически мгновенно сохранять, просматривать, форматировать пост, действия выполняются на высокой скорости. Работает без перебоев даже на не очень высокой скорости интернет-соединения;
- можно мгновенно сделать репост в Google+, чтобы твои друзья/коллеги/участники кругов могли обнаружить новое сообщение и прочесть его на блоге;
- шаблоны, которые можно настраивать, выглядят красиво и ярко. Любой веб-дизайнер оценит. Иными словами, блог можно без особого труда сделать привлекательным и запоминающимся для пользователя.

Недостатки Google Blogger:

- мало шаблонов. Этот минус весьма мал, но некоторым пользователям, возможно, придётся не по вкусу.

В заключении можно сказать, что любая выбранная для организации дистанционного обучения платформа будет иметь свои достоинства и недостатки. Удобство использования платформы зависит от степени ее адаптации к вашим умения использовать все существующие возможности и функции системы.

Далее перейдём к разбору дистанционных курсов. На сегодняшний день, нами были просмотрены некоторые дистанционные курсы. Анализ курсов будет происходить по следующим критериям:

- название курса и его описание;
- основные темы курса;
- продолжительность курса;
- доступность курса.

Ниже описание некоторых из них:

1. Дистанционный курс «Технологии и средства защиты информации на объектах информатизации» предлагает рассмотреть перечень мер по построению системы защиты объекта информатизации и разработке политики безопасности.

   Основные темы курса:

   - теоретические основы компьютерной безопасности;
   - методология построения системы защиты информационных систем;
   - криптографические средства и методы защиты информационных систем;
   - сетевые атаки. Межсетевые экраны;
   - защита информации в операционных системах;
   - защита информации в вычислительных сетях;
   - защита информации в сетях беспроводной связи;
   - защита программ и данных;
   - борьба с внутренними нарушителями информационной безопасности;
   - государственная система защиты информации, обрабатываемой техническими средствами;
   - правовое обеспечение защиты информации в России и за рубежом;
   - лицензирование, стандартизация и сертификация деятельности по защите информации.

Курс рассчитан на 102 часа, стоимость курса составляет сорок девять тысяч, пятьсот рублей.

2. Дистанционный курс «Пользователь системы защиты информации ViPNet» рассматривает теоретические и практические вопросы, связанные с обеспечение информационной безопасности и организации защищенных компьютерных сетей, позволяет овладеть навыками работы в защищённой сети, знакомит с основными особенностями работы с системой защиты информации ViPNet.

   Содержание курса:

   – общие положения об информационной безопасности для телекоммуникационных систем;
   – основные компоненты системы защиты информации;
   – VPN: определение, состав, характеристики, требования;
   – система защиты информации ViPNet: общие сведения;
   – технология ViPNet — концепция защиты и разграничения доступа;
   – программный комплекс ViPNet;
   – ViPNet Client;
   – «Деловая почта», автопроцессинг, ЭЦП;
   – типовые схемы применения ПО ViPNet;
   – дополнительные модули ПО ViPNet.

Продолжительность курса 14 дней, цена – семнадцать тысяч семьсот рублей.

3. Дистанционный курс «Способы и средства технической защиты информации» помогает получить специалистами теоретические и практические знания по способам и средствам технической защиты информации, по вопросам разработки организационно-распорядительных и технических документов по технической защите информации.

   Программа мероприятия:

   – Раздел №1. Организационно-правовые и организационно-технические основы технической защиты информации;

- Тема №1. Организационно-правовые и методические основы обеспечения защиты информации в Российской Федерации;
- Тема №2. Угрозы безопасности информации, методы их выявления и оценки опасности на объектах;
- Тема №3. Возможные технические каналы утечки информации ограниченного доступа на объектах;
- Раздел №2. Способы и средства технической защиты информации;
- Тема №4. Основы организации технической защиты информации на предприятии (в организации, учреждении);
- Тема №5. Мероприятия и средства защиты информации от утечки по техническим каналам на объектах информатизации;
- Тема №6. Способы и средства защиты информации от несанкционированного доступа и от программно-математических воздействий;
- Тема №7. Контроль выполнения и оценка эффективности мероприятий по технической защите информации;
- Итоговый зачет.

Курс рассчитан на пять дней. Стоимость – тридцать пять тысяч рублей.

4. Дистанционный курс «Безопасность компьютерных сетей». В курсе рационально чередуются систематизированные теоретические сведения и более 20 практических работ. Подробно рассматриваются источники угроз и причины появления уязвимостей систем, возможности и недостатки основных защитных механизмов, демонстрируются типичные приемы и инструменты, используемые нарушителями, моделируются хакерские атаки на сетевые протоколы и службы, предлагаются решения по обеспечению безопасности корпоративной сети и рациональному выбору средств защиты информации в компьютерных сетях. Значительная часть курса посвящена практической работе со средствами поиска уязвимостей систем и обнаружения атак (как свободно распространяемых, так и

коммерческих) на специальных реконфигурируемых стендах, позволяющих моделировать реальные корпоративные сети предприятий.

Программа курса:

- краткое введение в безопасность компьютерных сетей;
- безопасность физического и канального уровней;
- проблемы безопасности протокола разрешения адресов ARP;
- стандарт 802.1x;
- безопасность сетевого уровня модели OSI;
- защита периметра сети;
- введение в прикладную криптографию;
- виртуальные частные сети;
- проблемы безопасности протокола IP версии 6;
- безопасность транспортного уровня модели OSI;
- анализ защищённости корпоративной сети как превентивный механизм защиты;
- защита трафика на прикладном уровне;
- обнаружение сетевых атак;
- общие проблемы безопасности служб прикладного уровня;
- Honeynet или сеть-приманка для изучения поведения нарушителей;
- Итоговый зачет.

Курс рассчитан на четыре дня, стоимость – двадцать девять тысяч девятьсот рублей.

Более подробно нам не удалось рассмотреть данные курсы, так как все они являются платными.

На сегодняшний день все крупные компании, занимающиеся разработкой и продажей программных продуктов, устремились в эти технологии. Годовой рост рынка этих сервисов составляет по оценке специалистов 40-50% [19].

Можно с большой уверенностью утверждать, что облачные технологии в ближайшие годы станут основным поставщиком информационных ресурсов.

Уже сегодня созданы крупные Дата-центры, обеспечивающие тысячам пользователей доступ к программным ресурсам через облачные сервисы. Конкуренция в этой сфере заставляет разработчиков постоянно совершенствовать технологии и снижать стоимость услуг.

2. Разработка дистанционного курса по методам и средства защиты информации в сети интернет и облачных технологиях

2.1. Структура дистанционного курса. Разработка заданий, необходимых для освоения методов и средств защиты информации

В данном параграфе будет описан созданный дистанционный курс, а также описание разработанных заданий по тематики курса.

Электронный учебный курс должен строиться по следующим пунктам:

- формулировка целей;
- определение того, что будет знать, уметь и какие навыки получит учащийся после изучения курса;
- определение целевой аудитории курса;
- определение знаний, на которых основывается изучение курса;
- определение того, что является результатом изучения курса;
- выбор модели обучения (репродуктивная (энциклопедическая), творческая, комбинированный подход);
- выбор методов и приемлемых средств обучения (учебные материалы в
- варианте для печати, в гипертекстовом формате и т.д.) [25].

Ниже представлено описание разработанного дистанционного курс по теме «Методы и средства защиты информации в сети интернет и облачных технологиях».

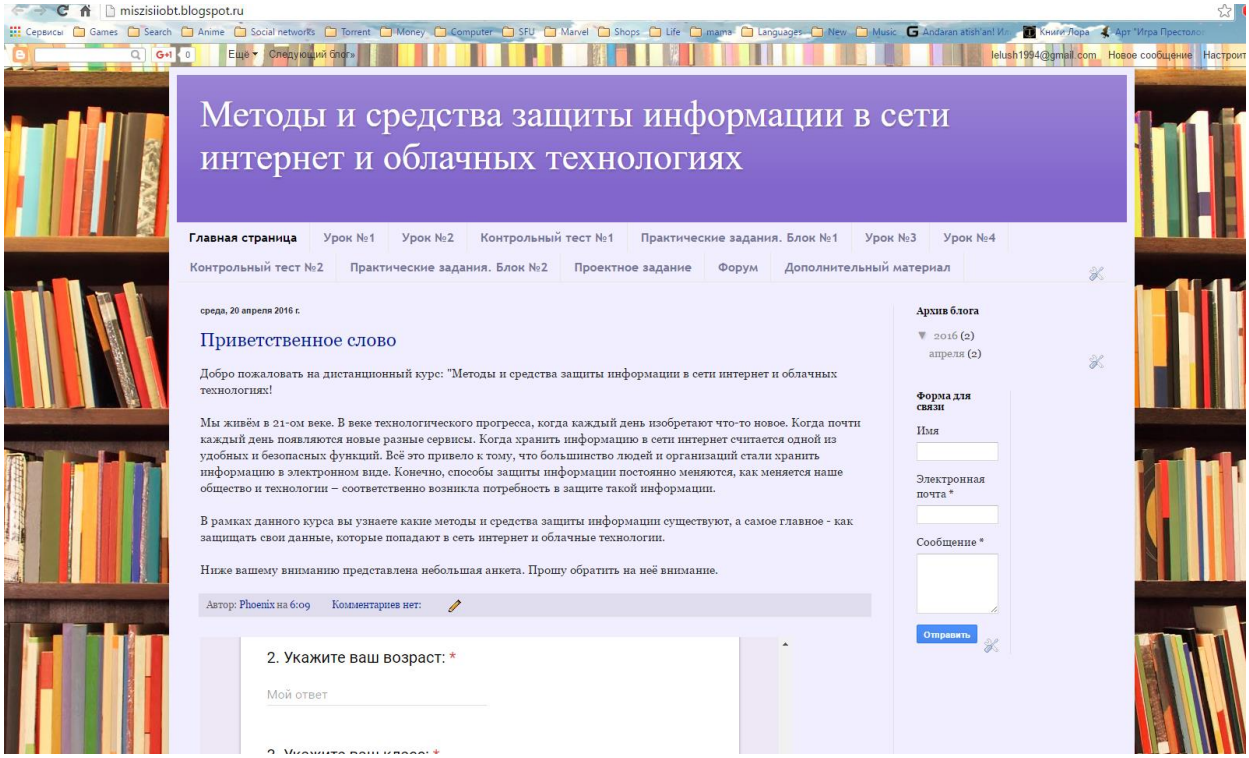


Рисунок 1 - Дистанционный курс «Методы и средства защиты информации в сети интернет и облачных технологиях»

Курс состоит из следующих страниц:

- Главная страница – предназначена для того, чтобы участники курса могли ознакомиться с актуальной информацией на данный момент;
- Урок №1 – страница предназначена для ознакомления с теоретическим материалом по теме: «Методы и средства защиты информации в сети интернет»;
- Урок №2 – продолжение ознакомления с теоретическим материалом по теме: «Методы и средства защиты информации в сети интернет»;
- Контрольный тест №1 – тестовое задание по пройденному материалу 1-го и 2-го уроков;
- Блок заданий №1 – практические задания по пройденному материалу 1-го и 2-го уроков;
- Урок №3 – страница предназначена для ознакомления с теоретическим материалом по теме: «Методы и средства защиты информации в облачных технологиях»;

- Урок №4 – продолжение ознакомления с теоретическим материалом по теме: «Методы и средства защиты информации в сети интернет»;
- Контрольный тест №2 – тестовое задание по пройденному материалу 3-го и 4-го уроков;
- Блок заданий №2 – практические задания по пройденному материалу 3-го и 4-го уроков;
- Проектное задание – итоговое практическое задание;
- Страница форума – данный элемент курса предназначен для общения между участниками курса;
- Дополнительный материал – данная страница предназначена исключительно для дополнительного материала по тему дистанционного курса.

Целевая аудитория данного курса – ученики старшей школы (10, 11 классы).

Режим занятий:

- курс рассчитан на максимальное количество часов - 10 ч;
- количество часов на практические занятия - 6 ч;
- количество часов на теоретические занятия - 4 ч.

Рекомендуемый режим работы: по 2 часа в неделю.

Данный курс является бесплатным.

Наиболее значимые отличия от подобных курсов:

- доступность – те курсы, которые нам удалось рассмотреть на сегодняшний день являются платными. Наш же курс будет бесплатным;
- не было обнаружено курсов по методам и средствам защиты информации непосредственно в облачных технологиях. Наш курс будет рассматривать эти сервисы тоже.

Предлагаем рассмотреть более подробно учебные элементы. В созданном курсе существует четыре учебных элемента. Ниже приведена таблица с описанием этих элементов:

Таблица 1 - Учебные элементы

<table>
<tr><th colspan="4">Учебные элементы</th></tr>
<tr><th>Лекция</th><th>Контрольный тест</th><th>Практические задания</th><th>Проектное задание</th></tr>
<tr><td>Урок №1. «Методы и средства защиты информации в сети интернет. Часть 1</td><td rowspan="2">Контрольный тест №1</td><td rowspan="2">Практические задания. Блок 1</td><td rowspan="4">Проектное задание по изученному материалу</td></tr>
<tr><td>Урок №2. «Методы и средства защиты информации в сети интернет. Часть 2</td></tr>
<tr><td>Урок №3. «Методы и средства защиты информации в облачных технологиях. Часть 1</td><td rowspan="2">Контрольный тест №2</td><td rowspan="2">Практические задания. Блок 2</td></tr>
<tr><td>Урок №4. «Методы и средства защиты информации в облачных технологиях. Часть 2</td></tr>
<tr><th colspan="4">Описание заданий</th></tr>
<tr><td>Дан лекционный материал, с которым должны ознакомиться участники курса. Лекции были разделены на две части, в каждой из которых весь материал предоставляется грамотно выстроенным и структурированным.</td><td>Участникам курса предлагается пройти два контрольных теста. В каждом тесте по пятнадцать вопросов. Тесты проверяют освоенность материала по двум урокам.</td><td>Практические задания предлагают выполнить учащимся некую творческую работу, которая позволить применить полученные ими знания на практике. Каждый блок содержит по два задания.</td><td>Финальное проектное задание (в парах), в котором проверяются все полученные задания за пройденный курс.</td></tr>
</table>

2.2. Проверка усвоения знаний по пройденному курсу

Сравнение полученных результатов на разных этапах исследования предоставляет возможность сделать вывод о том, что разработанные и реализованные занятия по методам и средствам защиты информации достаточно эффективны, так как:

- курс позволяет дополнить и углубить базовое образование по предмету «Информатика»;
- обеспечивает развитие уровня знаний, умений и навыков по методам и защиты информации в сети интернет и облачных технологиях;
- позволяет применять полученные знания на практике.

Ниже будут подробно описаны результаты, получение при проведении анкетирования и контрольных тестов.

В общей сложности, в курсе приняло участие шесть человек:

- четыре человека – представители мужского пола, два человека – представители женского;
- четырём участникам курса – по шестнадцать лет, оставшимся двум – по семнадцать.
- все участники данного курса были из одного класса – десятый.

1. Анкета №1

В первых трёх вопросах нужно было написать своё ФИО, возраст и класс.

Перейдём сразу к четвёртому вопросу, который звучал следующим образом: Что Вам известно о «Методах и средствах защиты информации в сети интернет и облачных технологиях»? На данный вопрос, участники курса ответили не однозначно, ответы представлены ниже:

- Можно сказать, что это комплекс способов, которые направлены на предотвращения кражи информации. А облачные технологии - это сервисы по обработке информации.
- Какие - то общие определения.
- Совсем немного. Знаю, что существуют антивирусы, которые помогают защитить мой компьютер.

– Существуют различные антивирусы для защиты компьютеров.
– Известны некоторые общие термины и определения. Известно о различных антивирусах. Про облачные технологии практически ничего не известно.
– В настоящее время существует множество понятий, связанных с информационной безопасностью, например, такие понятия как «компьютерная война», «информационная война», «информационное противоборство», «информационное оружие», «информационный терроризм» и др. Поэтому производится разработка, использование и совершенствование средств защиты информации, создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации, а также выявление технических устройств и программ, представляющих опасность для нормального функционирования IT-систем.

Пятый вопрос данной анкеты звучал следующим образом: Для чего Вы записались на данный курс?

Ответы участников курса представлены ниже:

– Чтобы бесплатно получить доступ к необходимым мне ресурсам.
– Мне интересно узнать про защиту информации.
– Чтобы улучшить свою знания и практические навыки.
– Хочу узнать о методах защиты информации больше.
– Я записался на данный курс для того, чтобы узнать больше о способах защиты компьютера.
– Хотелось бы знать больше о методах защиты информации.

Шестой вопрос данной анкеты звучал следующим образом: Чему Вы хотите научиться после прохождения данного курса?

Ответы участников курса представлены ниже:

– Хочу ознакомиться со способами защиты информации на моем компьютере, чтобы родители не имели доступ к моим личным файлам.
– Уметь защищать информацию в интернете.

– Защищать информацию самостоятельно.
– Научиться защищать личную информацию в облачных технологиях;
– Я хочу научиться различать и правильно удалять вирусы.
– Уметь пользоваться методами защиты информации, а также разбираться в облачных технологиях.

На этом вопросы первой анкеты заканчиваются. Данная анкета нужна для того, чтобы отслеживать количество участников данного курса и узнать общую информацию. Анкета заполняется один раз.

2. Контрольный тест №1

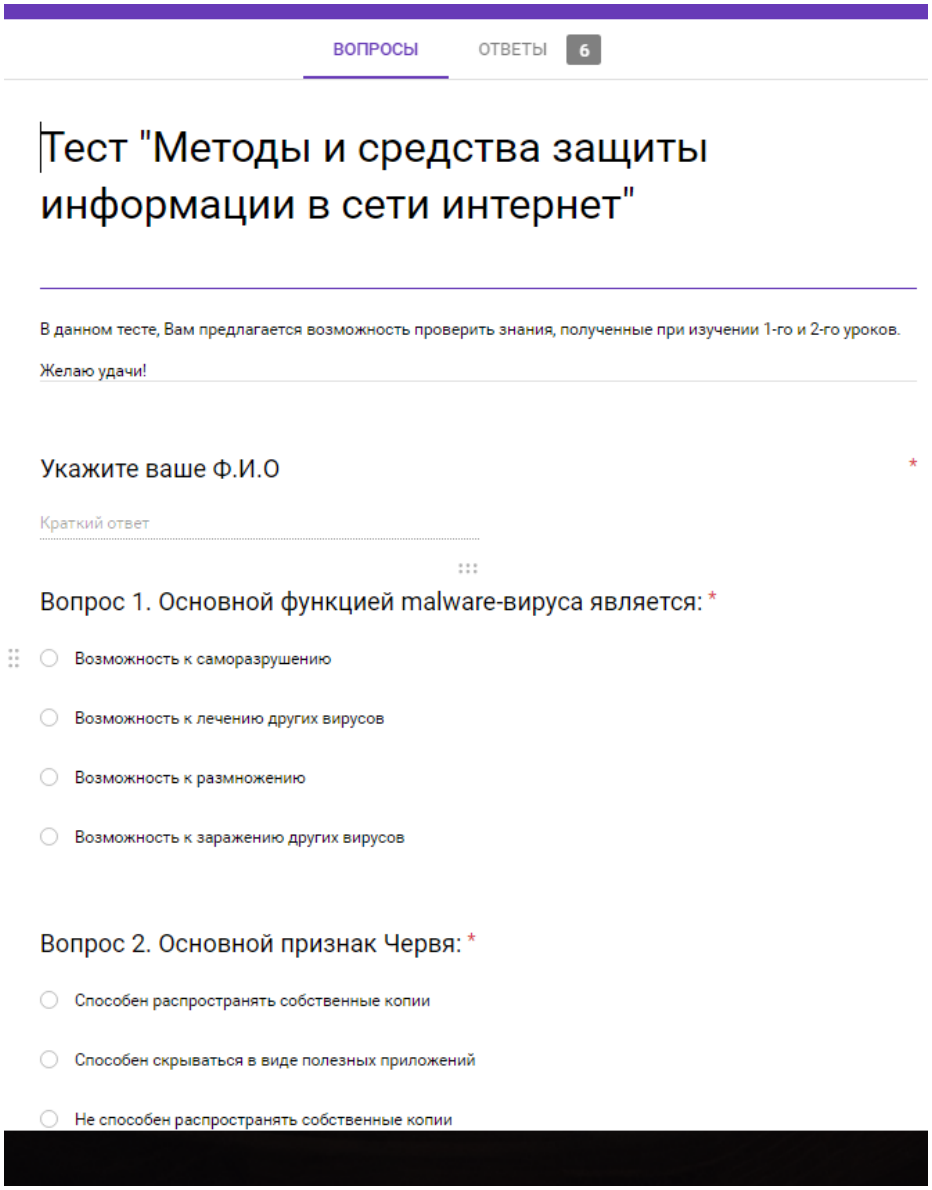


Рисунок 2 - Контрольный тест №1

Ниже предлагаем рассмотреть ответы участников дистанционного курса на контрольный тест №1, тема: «Методы и средства защиты информации в сети интернет». Более подробно можете посмотреть на графики, которые находятся в приложении А.

Первый вопрос звучал следующим образом: Основной функцией malware-вируса является (участникам тестирования предлагалось выбрать один из четырёх предложенных ответов):

- возможность к саморазрушению – данный ответ выбрали 0% участников тестирования;
- возможность к лечению других вирусов – данный ответ выбрали 0% участников тестирования;
- возможность к размножению – данный ответ выбрали пять участников тестирования (83.3%);
- возможность к заражению вирусов – данный ответ выбрал всего один участник тестирования (16,7%).

Второй вопрос звучал следующим образом: Основной признак Червя (участникам тестирования предлагалось выбрать один из четырёх предложенных ответов):

- способен распространять собственные копии – данный ответ выбрали пять участников тестирования (83.3%);
- способен скрываться в виде полезных приложений – данный ответ выбрал всего один участник тестирования (16,7%);
- не способен распространять собственные копии – данный ответ выбрали 0% участников тестирования;
- способен запускаться в фоновом режиме и фиксировать нажатия всех кнопок – данный ответ выбрали 0% участников тестирования.

Третий вопрос звучал следующим образом: Основной признак Трояна (участникам тестирования предлагалось выбрать один из четырёх предложенных ответов):

– может показывать всплывающие рекламные сообщения на компьютере (данный ответ выбрали 0% участников тестирования);
– является антивирусной программой (данный ответ выбрали 0% участников тестирования);
– способен восстанавливать утерянные файлы (данный ответ выбрали 0% участников тестирования);
– способен скрываться в виде полезных приложений (данный ответ выбрали шесть участников тестирования – 100%).

Четвёртый вопрос звучал следующим образом: Для того, чтобы защитить свой компьютер от вредоносных программ, нужно (участникам тестирования предлагалось выбрать несколько вариантов ответа из четырёх предложенных):

– использовать лицензионную операционную систему (данный ответ выбрали пять участников тестирования – 83,3%);
– использовать не лицензионные программы (данный ответ выбрали 0% участников тестирования);
– регулярно обновлять базу данных Антивируса (данный ответ выбрали четыре участника участников тестирования – 66,7%);
– использовать лицензионный Антивирус (данный ответ выбрали пять участников тестирования – 83,3%).

Можно заметить, что не все участники тестирования выбрали нужные ответы. Из шести участников только четыре человека справились с задачей.

Пятый вопрос звучал следующим образом: В каком месте можно хранить резервные копии важных данных (участником тестирования предлагалось выбрать несколько вариантов ответа из четырёх предложенных):

– на облачных серверах (данный ответ выбрали пять участников тестирования – 83,3%);
– в созданной папке на рабочем столе вашего компьютера (данный ответ выбрали 0% участников тестирования);
– на съемном носителе (данный ответ выбрали шесть участников тестирования – 100%);

– в созданном архиве на рабочем столе вашего компьютера (данный ответ выбрали 0% участников тестирования).

Обратите внимание, что в этом вопросе, как и в предыдущем, не все участники тестирования смогли справиться с задачей. Из шести участников только пять человек справились с задачей.

Шестой вопрос звучал следующим образом: Авторизация с двойной защитой называется (участникам тестирования предлагалось выбрать один из четырёх предложенных ответов):

– факторной аутентификацией (данный ответ выбрали 0% участников тестирования);
– смешанной аутентификацией (данный ответ выбрали два участника тестирования – 33,3%);
– одноразовой аутентификацией (данный ответ выбрал один участник тестирования – 16,7%);
– двухфакторной аутентификацией (данный ответ выбрали три участника тестирования – 50%).

Повторяется та же ситуация, что и с предыдущими двумя вопросами. Не всем участникам тестирования удалось справиться с задачей. Из шести участников только три человека смогли справиться с задачей.

Седьмой вопрос звучал следующим образом: Пароль может состоять из (участникам тестирования предлагалось выбрать один из пяти предложенных ответов):

– цифр, букв (данный ответ выбрали 0% участников тестирования);
– отпечатков пальца (данный ответ выбрали 0% участников тестирования);
– голосовой проверки (данный ответ выбрали 0% участников тестирования);
– сканирования сетчатки глаза (данный ответ выбрали 0% участников тестирования);

– все варианты верны (данный ответ выбрали шесть участников тестирования – 100%).

Восьмой вопрос звучал следующим образом: Брутфорс – это (участникам тестирования предлагалось выбрать один из четырёх предложенных ответов):

– метод перебора символов (данный ответ выбрали три участника тестирования – 50%);
– алгоритм создания любого вируса (данный ответ выбрали 0% участников тестирования);
– метод восстановления пароля без участия пользователя (данный ответ выбрали 0% участников тестирования);
– метод кражи пароля через сеть WiFi (данный ответ выбрали три участника тестирования – 50%).

Не все участники тестирования смогли справиться с данный вопросом. Из шести участников только три смогли дать правильный ответ.

Девятый вопрос звучал следующим образом: Если адрес начинается с https и в адресной строке стоит значок замка, значит (участникам тестирования предлагалось выбрать один из четырёх предложенных ответов):

– сайту можно доверять (данный ответ выбрали два участника тестирования – 33,3%);
– сайту доверять нельзя (данный ответ выбрал один участник тестирования – 16,7%);
– такого сайта не существует (данный ответ выбрал один участник тестирования – 16,7%);
– верных ответов нет (данный ответ выбрали два участника тестирования – 33,3%).

С задачей справились не все участники тестирования. Только два участника из шести смогли дать правильный ответ.

Десятый вопрос звучал следующим образом: Зачем привязывать к своему аккаунту актуальный номер мобильного телефона (участникам тестирования предлагалось выбрать несколько вариантов ответа из четырех предложенных):

– эта процедура помешает мошенникам поменять ваш пароль (данный ответ выбрали три участника тестирования – 50%);
– код восстановления будет приходить вам на телефон (данный ответ выбрали шесть участников тестирования – 100%);
– злоумышленники не смогут заразить ваш компьютер вирусами (данный ответ выбрали два участника тестирования – 33,3%);
– злоумышленники не смогут установить на ваш компьютер вредоносное ПО (данный ответ выбрали 0% участников тестирования).

Обратите внимание, что с задачей справились не все участники тестирования. Только три участника из шести смогли правильно дать ответы на данный вопрос.

Одиннадцатый вопрос звучал следующим образом: Источники антропогенного характера – это (участникам тестирования предлагалось выбрать один из четырёх предложенных вариантов ответа):

– незаконное вторжение постороннего лица из внешней сети общего назначения (данный ответ выбрали 0% участников тестирования);
– действия изнутри объекта. Например со стороны сотрудника компании (данный ответ выбрали два участника тестирования – 33,3%);
– оба варианта ответа не верны (данный ответ выбрал один участник тестирования – 16,7%);
– оба варианта ответа верны (данный ответ выбрали 3 участника тестирования – 50%).

В данном случае, с задачей справились не все участники тестирования. Из шести участников, только трое смогли дать верный ответ на поставленный вопрос.

Двенадцатый вопрос звучал следующим образом: Перечислите причины, по которым происходит утечка информации (участникам тестирования предлагалось выбрать несколько вариантов ответа из пяти предложенных):

– к серверу аппаратуры или линии связи может быть осуществлено незаконное подключение (данный ответ выбрали шесть участников тестирования – 100%);
– неправильное хранение архивных данных (данный ответ выбрали три участника тестирования – 50%);
– внедрение компьютерного вируса (данный ответ выбрали пять участников тестирования – 83,3%);
– фальсификация авторства (данный ответ выбрали три участника тестирования – 50%);
– модификация информации (данный ответ выбрали три участника тестирования – 50%).

Несмотря на то, что все варианты ответов были верны, с данным задание смогли справиться не все участники тестирования. Только три участника смогли полностью справиться с заданием.

Тринадцатый вопрос звучал следующим образом: К средствам аппаратного характера относятся (участникам тестирования предлагалось выбрать один из четырёх предложенных вариантов ответа):

– электронными (данный ответ выбрали 0% участников тестирования);
– механическими (данный ответ выбрали 0% участников тестирования);
– электромеханическими (данный ответ выбрали два участника тестирования – 33,3%);
– все варианты верны (данный ответ выбрали четыре участника тестирования – 66,7%).

С поставленным вопросом смогли справиться не все участники тестирования. Из шести только четверо смогли ответить правильно на поставленный вопрос.

Четырнадцатый вопрос звучал следующим образом: Программные меры защиты могут (участникам тестирования предлагалось выбрать несколько вариантов ответа из четырёх предложенных):

– проводить идентификацию пользователей (данный ответ выбрали четыре участника тестирования – 66,7%);
– воспрепятствовать физическому проникновению на сервер данных (данный ответ выбрал всего один участник тестирования – 16,7%);
– замаскировать данные, если доступ на сервер все же был открыт (данный ответ выбрали два участника тестирования – 33,3%);
– тестировать контроль системы защиты информации (данный ответ выбрали четыре участника тестирования – 66,7%).

В данном вопросе смогли выполнить поставленную задачу не все участники тестирования. Только четыре участника тестирования из шести смогли выполнить задачу.

Пятнадцатый вопрос звучал следующим образом: Гаммирование – это (участникам тестирования предлагалось выбрать один из четырёх предложенных вариантов ответа):

– смешивание, в котором могут использовать длинную маску (данный ответ выбрали 0% участников тестирования);
– смешивание, в котором могут использовать короткую маску (данный ответ выбрал один участник тестирования – 16,7%);
– смешивание, в котором могут использовать неограниченную маску (данный ответ выбрали два участника тестирования – 33,3%);
– все варианты верны (данный ответ выбрали три участника тестирования – 50%).

Несмотря на то, что все ответ в задании были верны, не всем участникам тестирования удалось дать верный ответ. Из шести участников только три смогли ответить верно.

3. Контрольный тест №2

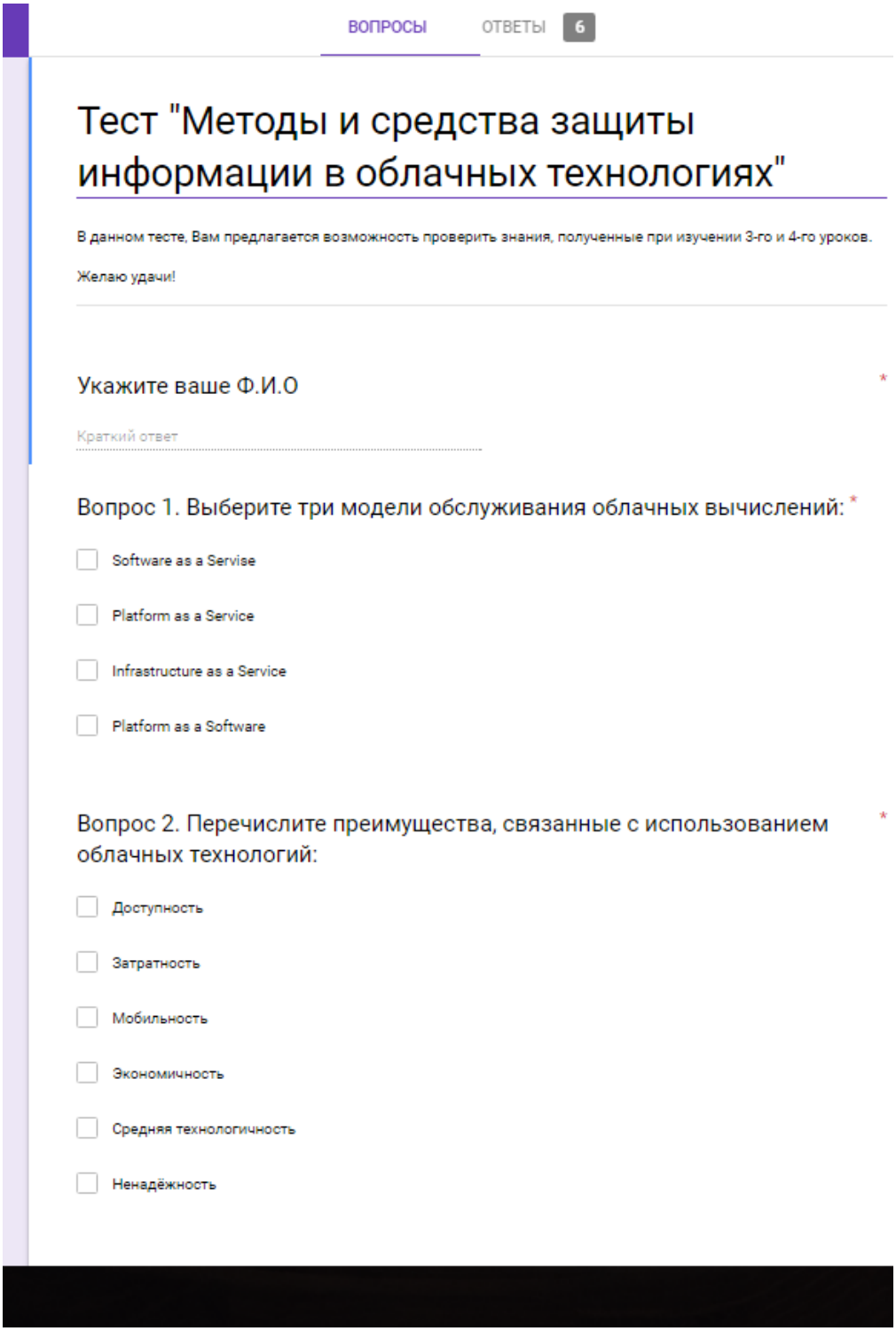


Рисунок 3 - Контрольный тест №2

Ниже предлагаем рассмотреть ответы участников дистанционного курса на контрольный тест №2, тема: «Методы и средства защиты информации в облачных технологиях». Более подробно можете посмотреть на графики, которые находятся в приложении Б.

Первый вопрос звучал следующим образом: Выберите три модели обслуживания облачных вычислений (участникам тестирования предлагалось выбрать несколько вариантов ответа из четырёх предложенных):

- Software as a Service (данный ответ выбрали шесть участников тестирования – 100%);
- Platform as a Service (данный ответ выбрали шесть участников тестирования – 100%);
- Infrastructure as a Service (данный ответ выбрали четыре участника тестирования – 66,7);
- Platform as a Software (данный ответ выбрал всего один участник тестирования – 16,7).

Следует обратить внимание на то, что с заданием смогли справиться не все участники тестирования. Только четыре участника из шести смогли дать правильные ответы.

Второй вопрос звучал следующим образом: Перечислите преимущества, связанные с использованием облачных технологий (участникам тестирования предлагалось выбрать несколько вариантов ответа из шести предложенных):

- Доступность (данный ответ выбрали пять участников тестирования – 83.3%);
- Затратность (данный ответ выбрали 0% участников тестирования);
- Мобильность (данный ответ выбрали шесть участников тестирования – 100%);
- Экономичность (данный ответ выбрали пять участников тестирования – 83.3%);
- Средняя технологичность (данный ответ выбрали 0% участников тестирования);
- Ненадёжность – данный ответ выбрали двое участников тестирования (33,3%).

С данным вопросом смогли справиться не все участники тестирования. Пять участников из шести смогли верно дать ответы на поставленный вопрос.

Третий вопрос звучал следующим образом: Каков объем бесплатного пространства на облачном диске Google (участникам тестирования предлагалось выбрать один вариант ответа из четырёх предложенных):

- 10 ГБ (данный ответ выбрали 0% участников тестирования);
- 30 ГБ (данный ответ выбрали 0% участников тестирования);
- 15 ГБ (данный ответ выбрали шесть участников тестирования – 100%);
- 20 ГБ (данный ответ выбрали 0% участников тестирования).

Четвёртый вопрос звучал следующим образом: Выберите основной недостаток облачных сервисов (участникам тестирования предлагалось выбрать один вариант ответа из четырёх предложенных):

- Проблема неконтролируемых данных (данный ответ выбрал один участник тестирования – 16,7%);
- Проблема интеграции данных (данный ответ выбрал один участник тестирования – 16,7%);
- При использовании виртуального ПО информация автоматически попадает в руки разработчика (данный ответ выбрали три участника тестирования – 50%);
- Все варианты верны (данный ответ выбрал один участник тестирования – 16,7%).

С данным вопросом смогли справиться не все участники тестирования. Пять участников из шести смогли верно дать ответы на поставленный вопрос.

Пятый вопрос звучал следующим образом: Модели развертывания облачных технологий (участникам тестирования предлагалось выбрать несколько вариантов ответа из четырёх предложенных):

- Частные облака (данный ответ выбрали шестеро участников тестирования – 100%);
- Облака с частичной открытостью (данный ответ выбрал один участник тестирования – 16,7%);
- Гибридные облака (данный ответ выбрали пятеро участников тестирования – 83,3%);

– Публичные облака (данный ответ выбрали четверо участников тестирования – 66,7%).

С данным вопросом смогли справиться не все участники тестирования. Четверо участников из шести смогли верно дать ответы на поставленный вопрос.

Шестой вопрос звучал следующим образом: Какое утверждение является верным (участникам тестирования предлагалось выбрать один ответ из пяти предложенных вариантов):

– Облако – это только виртуализация (данный ответ выбрал один участник тестирования – 16,7%);
– Облако – как источник экономии (данный ответ выбрали 0% участников тестирования);
– Частное облако не всегда внедрено у заказчика (данный ответ выбрали пять участников тестирования – 83,3%);
– Частное облако не может перестать быть частным (данный ответ выбрали 0% участников тестирования);
– Все ответы верны (данный ответ выбрали 0% участников тестирования).

С данным вопросом смогли справиться не все участники тестирования. Пятеро участников из шести смогли верно дать ответ на поставленный вопрос.

Седьмой вопрос звучал следующим образом: Основные свойства облачных технологий – это (участникам тестирования предлагалось выбрать несколько вариантов ответа из пяти предложенных):

– Возможность в высокой степени автоматизированного самообслуживания системы со стороны провайдера (данный ответ выбрали пять участников тестирования – 83,3%);
– Наличие системы Broad Network Access (данный ответ выбрали четыре участника тестирования – 66,7%);
– Сосредоточенность ресурсов на отдельных площадках для их эффективного распределения (данный ответ выбрали пять участников тестирования – 83,3%);

– Медленная масштабируемость (данный ответ выбрали 0% участников тестирования);
– Не управляемый сервис (данный ответ выбрали 0% участников тестирования).

Несмотря на больше количества правильных ответов, не все смогли справится с поставленным вопросом. Только четыре участника из шести смогли полностью ответить на данный вопрос.

Восьмой вопрос звучал следующим образом: Самыми важными элементами облачной системы являются (участникам тестирования предлагалось выбрать один ответ из четырёх предложенных вариантов):

– Гипервизор, управляющий виртуальной средой облака (данный ответ выбрали 0% участников тестирования);
– Центр обработки данных, на котором содержится большая часть конфиденциальной информации (данный ответ выбрали 0% участников тестирования);
– Канал связи между пользователем облачного сервиса (данный ответ выбрали два участника тестирования – 33,3%);
– Все ответы верны (данный ответ выбрали четыре участника тестирования – 66,7%).

С данным вопросом смогли справиться не все участники тестирования. Четверо участников из шести смогли верно дать ответ на поставленный вопрос.

Девятый вопрос звучал следующим образом: Каким атакам подвержены облачные технологии (участникам тестирования предлагалось выбрать несколько вариантов ответа из четырёх предложенных):

– сетевые атаки (данный ответ выбрали шесть участников тестирования – 100%);
– атаки на пользователя (данный ответ выбрали шесть участников тестирования – 100%);
– атаки на серверы облака (данный ответ выбрали пять участников тестирования – 83,3%);

– традиционные атаки ПО (данный ответ выбрали четыре участника тестирования – 66,7%).

Несмотря на то, что все варианты ответов были верны, не все смогли справиться с задачей. Только четверо из шести участников смогли полностью ответить на данный вопрос.

Десятый вопрос звучал следующим образом: Для обеспечения информационной безопасности облаков система защиты информации должна включать в себя (участникам тестирования предлагалось выбрать один ответ из пяти предложенных вариантов):

– подсистему обеспечения безопасности информации на стороне разработчика (данный ответ выбрал один участник тестирования – 16,7%);
– подсистему обеспечения локальной безопасности (данный ответ выбрали 0% участников тестирования);
– подсистему обеспечения безопасности виртуальных сред (данный ответ выбрали четверо участников тестирования – 66,7%);
– подсистему обеспечения частной безопасности (данный ответ выбрали 0% участников тестирования);
– подсистему обеспечения безопасности сети (данный ответ выбрал один участник тестирования – 16,7%).

С данным вопросом смогли справиться не все участники тестирования. Четверо участников из шести смогли верно дать ответ на поставленный вопрос.

Одиннадцатый вопрос звучал следующим образом: Элементы обеспечения безопасности информации на стороне пользователя (участникам тестирования предлагалось выбрать один ответ из четырёх предложенных вариантов):

– антивирусные средства защиты информации (данный ответ выбрал один участник тестирования – 16,7%);
– встроенный в ОС персональный брандмауэр (данный ответ выбрали 0% участников тестирования);

– безопасно настроенный интернет-браузер (данный ответ выбрал один участник тестирования – 16,7%);
– все ответы верны (данный ответ выбрали четыре участника тестирования – 66,7%).

С данным вопросом смогли справиться не все участники тестирования. Четверо участников из шести смогли верно дать ответ на поставленный вопрос.

Двенадцатый вопрос звучал следующим образом: Для защиты гипервизора необходимо (участникам тестирования предлагалось выбрать один ответ из четырёх предложенных вариантов):

– ограничить права доступа к серверу (данный ответ выбрал один участник тестирования – 16,7%);
– своевременная установка обновлений ПО среды виртуализации (данный ответ выбрал один участник тестирования – 16,7%);
– разграничение запуска программ (данный ответ выбрал один участник тестирования – 16,7%);
– нет правильного ответа (данный ответ выбрали три участника тестирования – 50%).

Обратим внимание на то, что с поставленной задачей справились не все участники тестирования. Только один участник из шести смог дать правильный ответ.

Тринадцатый вопрос звучал следующим образом: Подсистема обеспечения безопасности ЦОД включает в себя следующие элементы (участникам тестирования предлагалось выбрать несколько вариантов ответа из четырёх предложенных):

– охранное видеонаблюдение – данный ответ выбрали шесть участников тестирования (100%);
– система резервного копирования и удаления данных – данный ответ выбрали три участника тестирования (50%);
– система контроля и управления доступом – данный ответ выбрали шесть участников тестирования (100%);

– система открытой информации в ЦОД – данный ответ выбрал один участник тестирования (16,7%).

В данном случае, было два правильных ответа. Казалось бы, что все участники тестирования справились с задачей. На самом деле, только трое участников из шести смогли справиться с задачей.

Четырнадцатый вопрос звучал следующим образом: Элементы системы информационной безопасности ЦОД (участникам тестирования предлагалось выбрать несколько вариантов ответа из пяти предложенных):

– средства криптографической защиты информации (данный ответ выбрали пять участников тестирования – 83,3%);
– средства локального экранирования (данный ответ выбрал один участник тестирования – 16,7%);
– средства ограничения доступа (данный ответ выбрал один участник тестирования – 16,7%);
– средства антивирусной безопасности (данный ответ выбрали пять участников тестирования – 83,3%);
– средства обнаружения и предотвращения вторжений (данный ответ выбрали пять участников тестирования – 83,3%).

Несмотря на большое количество правильных ответов, не все участники тестирования смогли справиться с поставленный перед ними задачей. Только пять участников из шести смогли справиться с задачей.

4. Вторичное тестирование

В первых трёх вопросах, как и в первичном тестировании, нужно было написать своё ФИО, возраст и класс.

Перейдём сразу к четвёртому вопросу, который звучал следующим образом: Был ли для Вас изученный материал новым и актуальным? Если нет, опрос для Вас окончен, если да - перейдите к следующему вопросу. Ниже будут представлены варианты ответов на данный вопрос, а также варианты ответов участников тестирования:

– да (данный ответ выбрали шесть участников тестирования – 100%);

– нет (данный ответ выбрали 0% участников тестирования);
– скорее да, чем нет (данный ответ выбрали 0% участников тестирования);
– скорее нет, чем да (данный ответ выбрали 0% участников тестирования).

Пятый вопрос звучал следующим образом: Чему Вы смогли научиться после прохождения данного курса? Ответы участников тестирования на данный вопрос были очень разными. Ниже будут представлены ответы:

– Я узнала о типах вредоносных программ, как защитить свой компьютер. Как защитить свой аккаунт - очень полезная информация. Узнала много интересного об облачных технологиях. Их преимущества и недостатки. Тестирование и практические задания помогли проверить мне свои знания.
– Как лучше защитить свой электронный почтовый ящик.
– я теперь знаю, как можно защищать свою информацию в сети.
– Я узнал больше о способах защиты компьютера, о видах и особенностях вирусов, об особенностях защиты своих аккаунтов.
– Я узнал о разновидностях вируса, а также о разновидностях антивирусных программ. О том, как лучше защитить свой компьютер и свои аккаунты в интернете. А также узнал о том, что из себя представляют облачные технологии, о их плюсах и минусах.
– Я смог научиться максимально возможно защищать личную информацию в облачных технологиях.

По результатам прохождения контрольных тестов и анкетирования, можно сделать следующие выводы:

Несмотря на то, что оба теста были составлены исключительно по материалам уроков, далеко не все участники тестирования смогли справиться с поставленной передними задачей. В наших тестах, как и в многих других, нет таких участников тестирования, которые полностью смогли ответить на все вопросы правильно. Ведь на то это и тесты, они существуют для проверки своих знаний и для того, чтобы потом исправлять свои ошибки.

Если сравнивать ответы, которые участники курса дали на вопросы в двух анкетах, можно заметить, что для каждого участника это был полезный курс. Все участники начинали с определёнными знаниями по теме: «Методы и средства защиты информации в сети интернет и облачных технологиях» и каждый, в итоге, вынес что-то полезное и новое для себя. Что-то, что пригодится как для обыденной жизни, так и для профессиональной деятельности.

Заключение

На сегодняшний день разновидность методов и средств защиты информации с каждым днём становиться всё больше, также, как и с каждым днём появляются новые технологии. Следить за работоспособностью данных методов и средств очень сложно, особенно, если это касается защиты не только вашего персонального компьютера, но и, например, облачных сервисов. В законодательстве РФ отсутствует определенный перечень методов и средства защиты информации в облачных технологиях, что порождает на практике определенные проблемы использования сервиса данного вида.

Существенным пробелом является, на наш взгляд, отсутствие положений об условиях защиты информации для данного сервиса. На сегодняшний день применяются аналогические методы и средства защиты информации в сети интернет для облачных технологий. Таким образом, можно сделать следующий вывод – в облачной технологии безопасность играет важнейшую роль, этой проблеме специалисты уделяют особое внимание. Но, несмотря на все сложности в области безопасности, преимущества предоставляемых через Интернет сервисов перевешивают возможные риски и облачные вычисления будут широко востребованы на рынке информационных технологий.

В самом исследовании была предпринята попытка повысить знания о методах и средствах защиты информации в сети интернет и облачных технологиях у детей старшей школы. В приложении к дипломной работе, нами представлены результаты реализованной попытки повышения знаний о методах и средствах защиты информации в сети интернет и облачных технологиях у детей старшей школы. Если сравнивать ответы, которые участники курса дали на вопросы в двух анкетах, можно заметить, что для каждого участника это был полезный курс. Все участники начинали с определёнными знаниями по теме: «Методы и средства защиты информации в сети интернет и облачных технологиях» и каждый, в итоге, вынес что-то полезное и новое для себя. Что-то, что пригодится как для обыденной жизни, так и для профессиональной деятельности.

Подводя итог исследованию, касающемуся методов и средств защиты информации в сети интернет и облачных технологиях, нами сделан вывод о том, что несмотря на большое количество трудов специалистов о методах и средства защиты информации, вопросы теории методов и средств защиты информации, являются весьма актуальными, требующими законодательного урегулирования, путем внесения изменений в соответствующие нормативно-правовые акты.

Список используемых источников

1. Peter Mell, Thimothy Grance. «The NIST Definition of Cloud Computing (Draft)» // Recommendations of the National Institute of Standards and Technology, Special Publication 800 – 145 (Draft), сентябрь 2011 год.
2. Ажмухамедов И.М., Князева О.М. Оценка состояния защищенности данных организации в условиях возможности реализации угроз информационной безопасности / И.М. Ажмухамедов, О.М. Князева // Прикаспийский журнал: Управление и высокие технологии. – 2015. – № 3. – С. 24-39.
3. Бакулин В.М. Основные вопросы информационной безопасности / В.М. Бакулин // Вестник волгоградской академии МВД России. – 2010. – № 4. – С. 126.
4. Безопасность ЦОД [Электронный ресурс] // Компания «Флайлинк». – 2016. – Режим доступа: http://www.flylink.ru/info/articles/553/1404.
5. Гаврилов, М.В. Информатика и информационные технологии : учебник для бакалавров / М.В. Гаврилов, В.А. Климов. – 3-е изд., перераб. и доп. – М. : Юрайт, 2013. – 378 с. – (Бакалавр. Базовый курс).
6. Горожанов А.И. Эволюция «облачных» технологий: cloud computing – cloud intelligence – cloud university / А.И. Горожанов // Филологические науки. Вопросы теории и практики. – 2013. – № 1(19). – С. 66-68.
7. Душкин А.В. Оценка безопасности информационных процессов при применении перспективных облачных технологий в УИС / А.В. Душкин, Ю.В. Щербакова // Вестник воронежского института ФСИН России. – 2014. – № 1. – С. 21-25.
8. Идрисова А.А. Внедрение современных информационных технологий в образовательный процесс на примере облачных технологий / А.А. Идрисова // European Research. – 2015. – № 10(11). – С. 122-123.
9. Ковшов Е.Е. Разработка информационной системы для управления инновациями на основе "облачных" программных технологий / Е.Е.

Ковшов, П.Н. Мартынов // Межотраслевая информационная служба. – 2012. – № 4. – С. 37-42.

10. Кондратьев А.А. Методологическое обеспечение интеллектуальных систем защиты от сетевых атак / А.А. Кондратьев, А.А. Талалаев, И.П. Тищенко, В.П. Фраленко, В.М. Хачумов // Современные проблемы науки и образования. – 2014. – № 2. – 119 с.
11. Кораблев А.В. Технология анализа и оценки системы управления информационными рисками облачных вычислений / А.В. Кораблев // Проблемы совершенствования организации производства и управления промышленными предприятиями: межвузовский сборник научных трудов. – 2014. № 1. – С. 75-83.
12. Коуров Л.В. «Информационные технологии» : учебное пособие / Л.В. Коуров. - Мн : Амалфея, 2000. - 192 с.
13. Кравченко А.С. Аппаратно-программные средства и информационные процессы защиты систем предоставления пользователям доступа к программным ресурсам / А.С. Кравченко, С.В. Родин, Т.Е. Смоленцева // Современные проблемы науки и образования. – 2015. – № 1-1. – 357 с.
14. Мальцев Г.Н. Исследование вероятностных характеристик изменения защищенности информационной системы от несанкционированного доступа нарушителей / Г.Н. Мальцев, А.В. Панкратов, Д.А. Лесняк // Информационно-управляющие системы. – 2015. – № 1(74). – С. 50-58.
15. Мотышина М.С. О самоподобии облачных технологий как элемента иерархии информационного пространства / М.С. Мотышина // Информационные технологии в бизнесе. – 2013. – С. 190-193.
16. Нурдинов Р.А Подходы и методы обоснования целесообразности выбора средств защиты информации / Р.А. Нурдинов, Т.Н. Батова // Современные проблемы науки и образования. – 2013. – № 2. – 395 с.
17. Ошурков В.А. Механизмы защиты обучающихся от киберэкстремизма в условиях развития облачных образовательных сервисов / В.А. Ошурков,

В.Н. Макашова, Л.С. Цуприк // Фундаментальные исследования. – 2014. – № 12-5. – С 1089-1092.

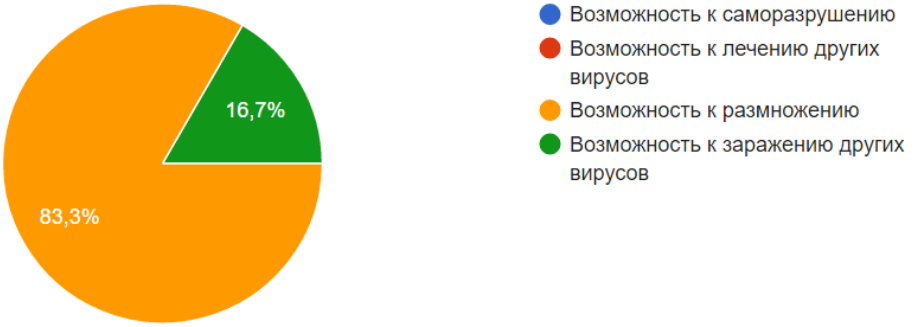
18. Полежаев П.Н. «Ахиллесова пята» USB-устройств: атака и защита / П.Н. Полежаев, А.К. Малахов, А.М. Сагитов // Философские проблемы информационных технологий и киберпространства. – 2015. – № 1. – С. 106-117.
19. Прохоренков П.А. Использование облачных технологий в дистанционном обучении / П.А. Прохоренко, И.Ю. Явойш, А.Т. Прохоренкова // Инновации: Бизнес. Образование. – 2014. С. 201-205.
20. Разумников С.В. Анализ существующих методов оценки эффективности информационных технологий для облачных ИТ-сервисов / С.В. Разумников // Современные проблемы науки и образования. – 2013. – № 3. – 84 с.
21. Сабанов А.Г. Особенности аутентификации при доступе к облачным сервисам / А.Г. Сабанов // Вестник нижегородского университета им. Н.И. Лобачевского. – 2013. – № 2-1. – С. 45-51.
22. Сироткин А.Ю. Применение облачных технологий в системе дистанционного обучения / А.Ю. Сироткин // Психолого-педагогический журнал Гаудеамус. – 2013. – № 1(21). – С. 69-74.
23. Соколовский Е.П., Финько О.А. Информационная поддержка управления запасами средств защиты информации в условиях неопределенности / Е.П. Соколовский, О.А. Финько // Известия ЮФУ. Технические науки. – 2014. – № 2. – С. 120-128.
24. Тараканов О.В. Анализ методов контроля целостности файлов / О.В. Тараканов // Перспективы развития информационных технологий. – 2015. № 23. – С. 184-188.
25. Устюгова В.Н. О процессе создания системы дистанционного обучения в Татарском государственном гуманитарно-педагогическом университете (ТГГПУ) / В.Н. Устюгова, Р.А. Валитов // Образовательные технологии и общество. – 2011. – № 2. – С. 225-239.

26. Чибирова М.О. Новые информационные технологии обеспечения безопасности общества: реализация универсального решателя задач на основе облачных и миварных технологий / М.О. Чибирова, Г.С. Сергушин, О.О. Варламов Д.В. Елисеев // Информационное противодействие угрозам терроризма. – 2013. – № 20. – С. 19-29.
27. Что такое фишинг [Электронный ресурс] // АО «Лаборатория Касперского». – 2016. – Режим доступа: http://www.securelist.com/ru/threats/spam?chapter=164.
28. Шаньгин В.Ф. Информационная безопасность и защита информации : учебное пособие / В.Ф. Шаньгин. – Москва : ДМК Пресс, 2014. – 702 с.;
29. Шерина, Н.С. Модель технического учебника как перспективное средство дистанционного обучения / Н.С. Шерина // Вестник Адыгейского государственного университета. Серия 3: Педагогика и психология. – 2010. – № 4. – С. 70-73.
30. Ширманов А. Безопасность виртуализации при обработке данных ограниченного доступа // Москва, ЭКСПОЦЕНТР, InfoSecurity Russia. – 2009.

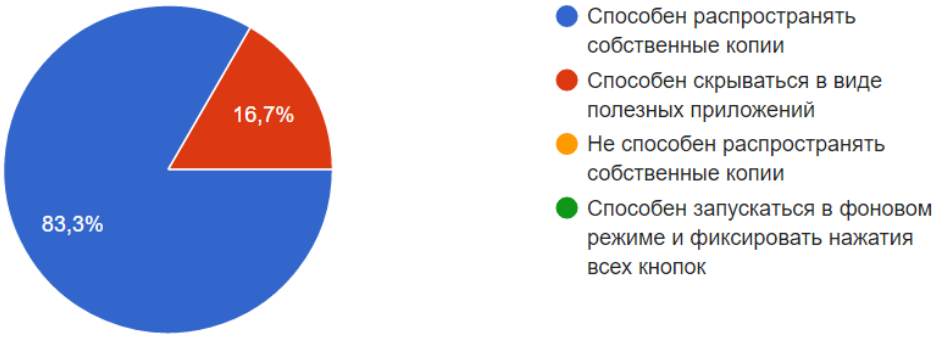
Приложение А

Контрольный тест №1

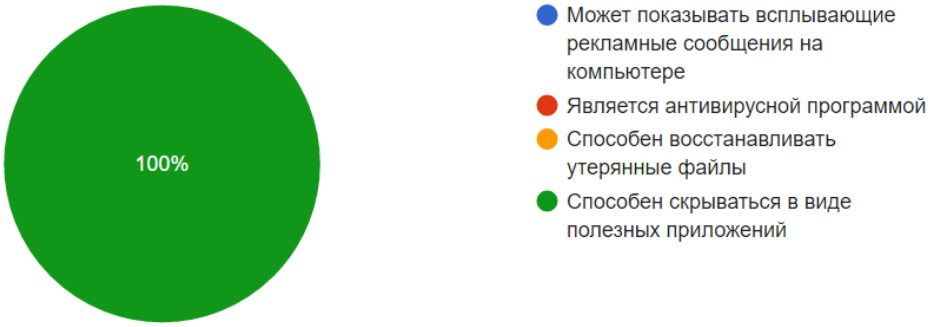
Вопрос 1. Основной функцией malware-вируса является: (6 ответов)



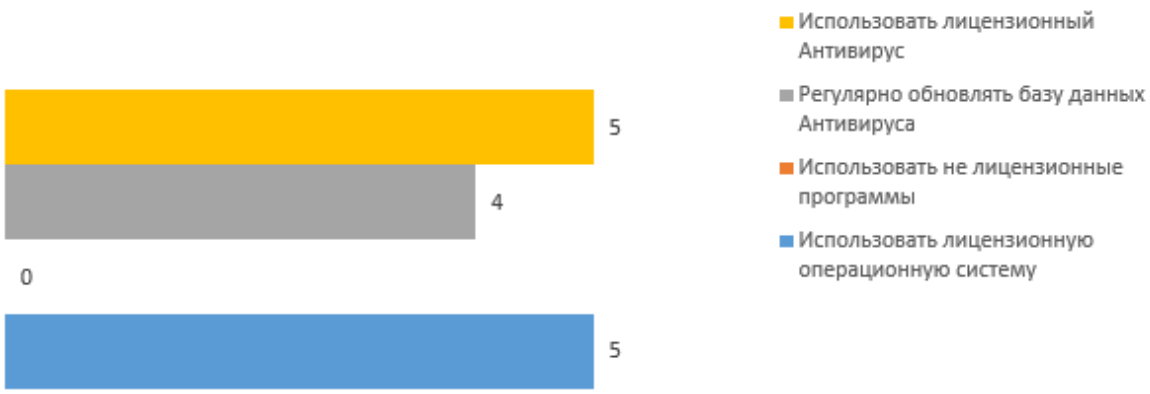
Вопрос 2. Основной признак Червя: (6 ответов)



Вопрос 3. Основной признак Трояна: (6 ответов)

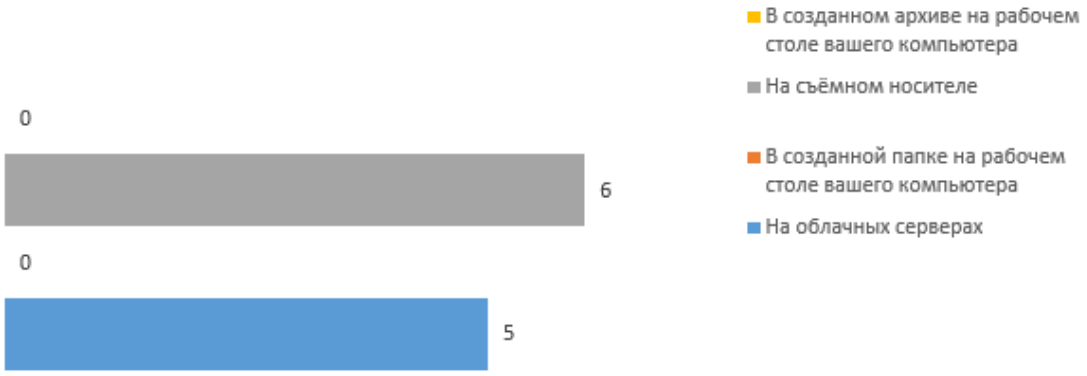


Вопрос 4. Для того, чтобы защитить свой компьютер от вредоносных программ, нужно:



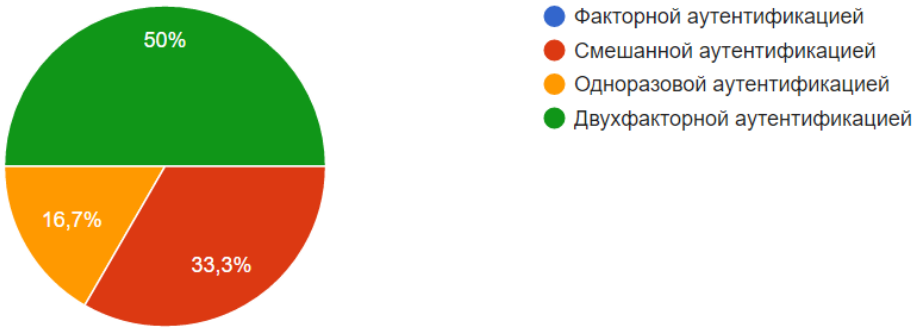
Количество человек, вырбав тот или иной ответ

Вопрос 5. В каком месте можно хранить резервные копии важных данных?

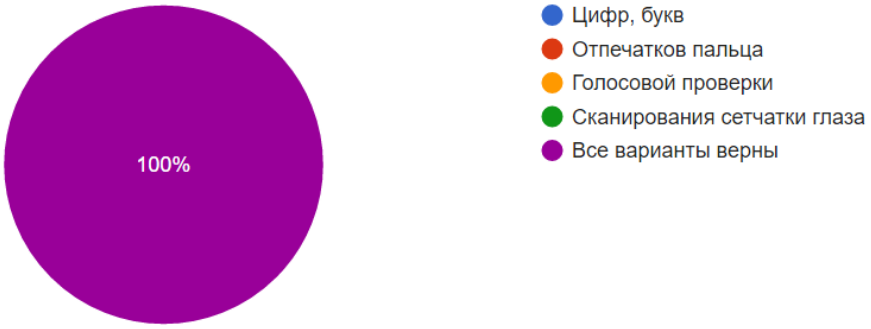


Количество человек, вырбав тот или иной ответ

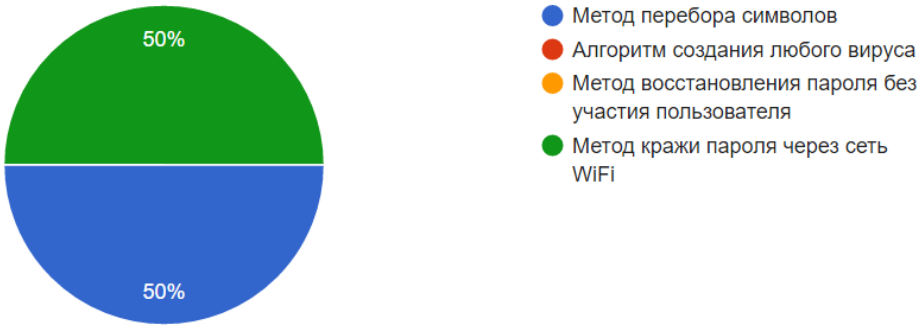
Вопрос 6. Авторизация с двойной защитой называется: (6 ответов)



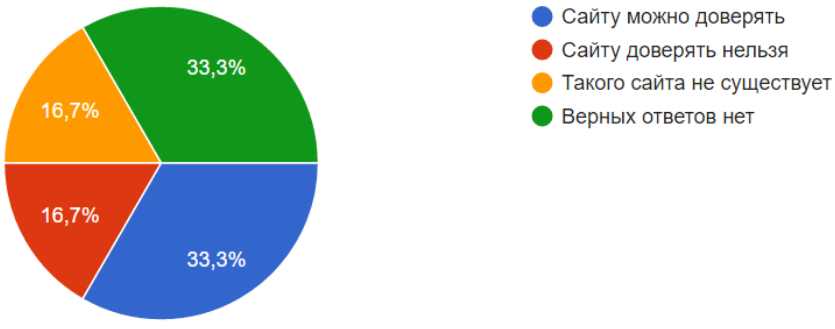
Вопрос 7. Пароль может состоять из: (6 ответов)



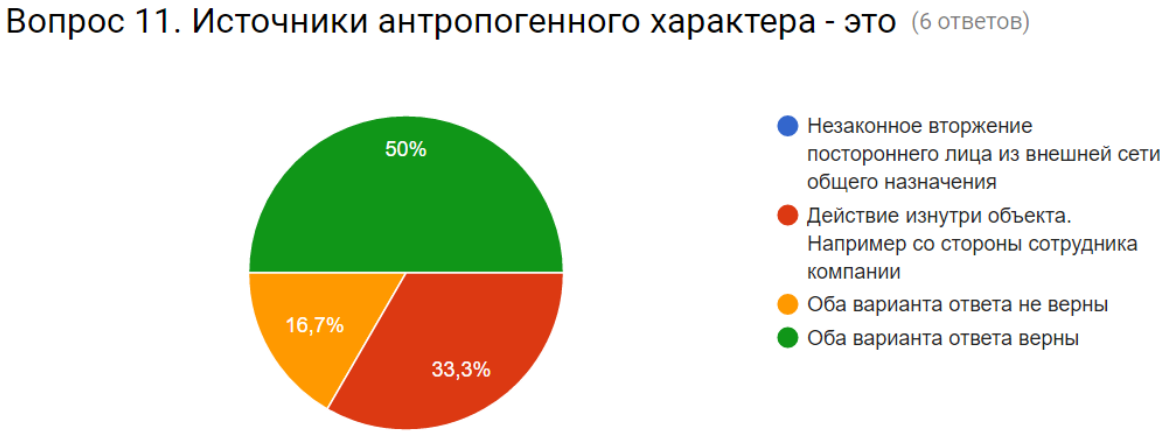
Вопрос 8. Брутфорс - это: (6 ответов)



Вопрос 9. Если адрес начинается с https и в адресной строке стоит значок замка, значит:
(6 ответов)

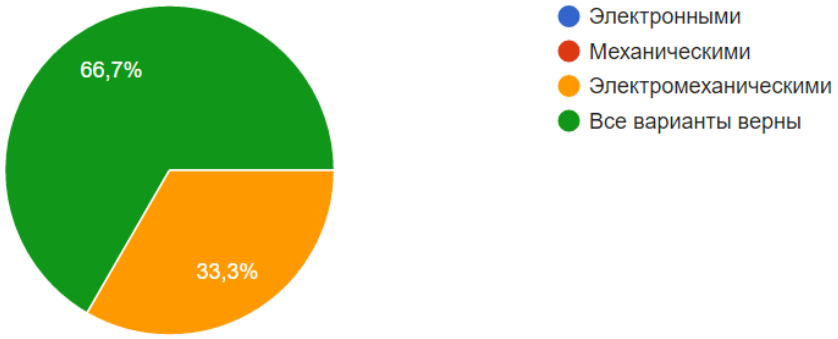



Вопрос 10. Зачем привязывать к своему аккаунту актуальный номер мобильного телефона?
0
2
6
3
Злоумышленники не смогут установить на ваш компьютер вредоносное ПО
Злоумышленники не смогут заразить ваш компьютер вирусами
Код восстановления будет приходить вам на телефон
Эта процедура помешает мошенникам поменять ваш пароль
Количество человек, вырбав тот или иной ответ

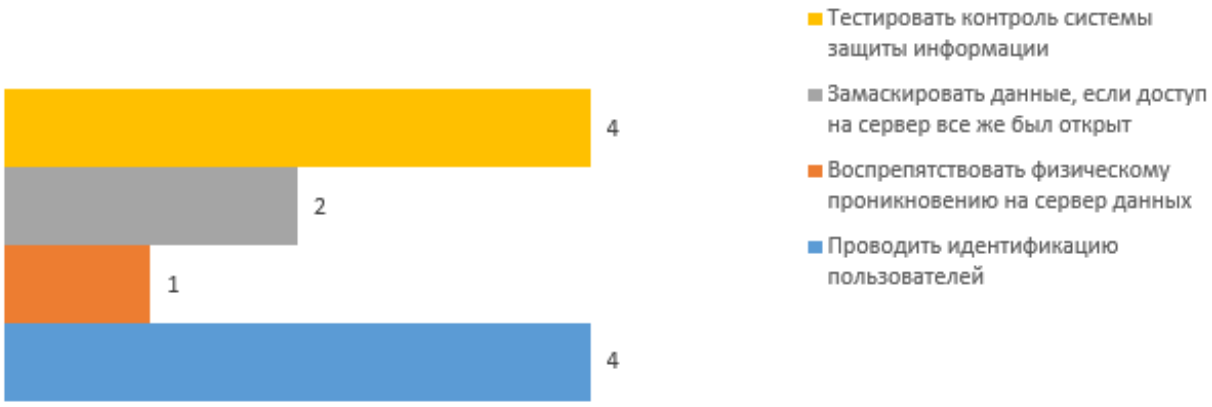

Вопрос 11. Источники антропогенного характера - это (6 ответов)
50%
16,7%
33,3%
Незаконное вторжение постороннего лица из внешней сети общего назначения
Действие изнутри объекта. Например со стороны сотрудника компании
Оба варианта ответа не верны
Оба варианта ответа верны


Вопрос 12. Перечислите причины, по которым происходит утечка информации:
3
3
5
3
6
Модификация информации
Фальсификация авторства
Внедрение компьютерного вируса
Неправильное хранение архивных данных
К серверу аппаратуры или линии связи может быть осуществлено незаконное подключение
Количество человек, вырбав тот или иной ответ

Вопрос 13. К средствам аппаратного характера относятся: (6 ответов)

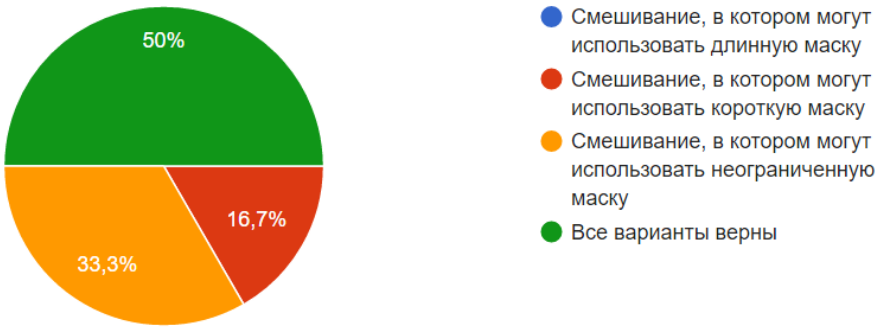


Вопрос 14. Программные меры защиты могут:



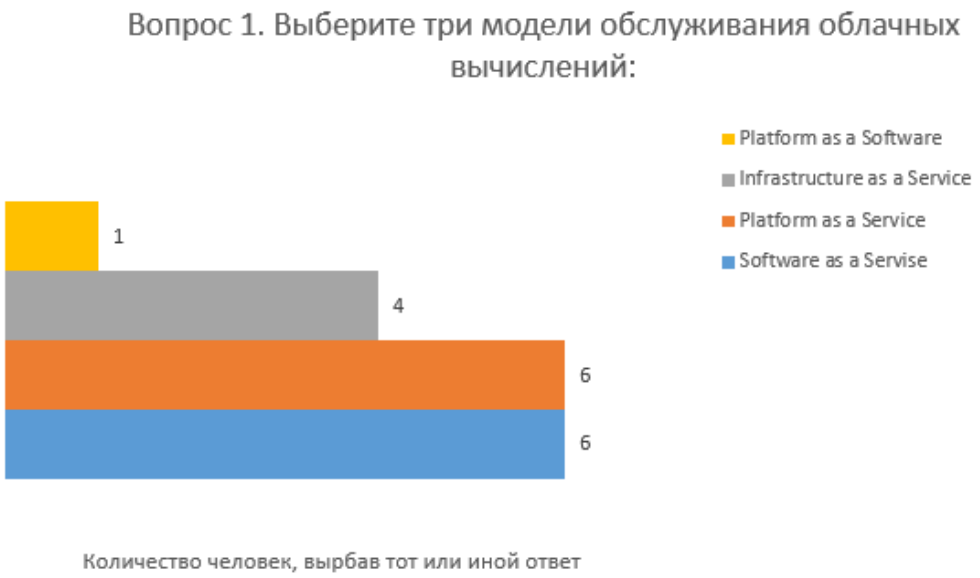
Количество человек, вырбав тот или иной ответ

Вопрос 15. Гаммирование - это (6 ответов)



Приложение Б

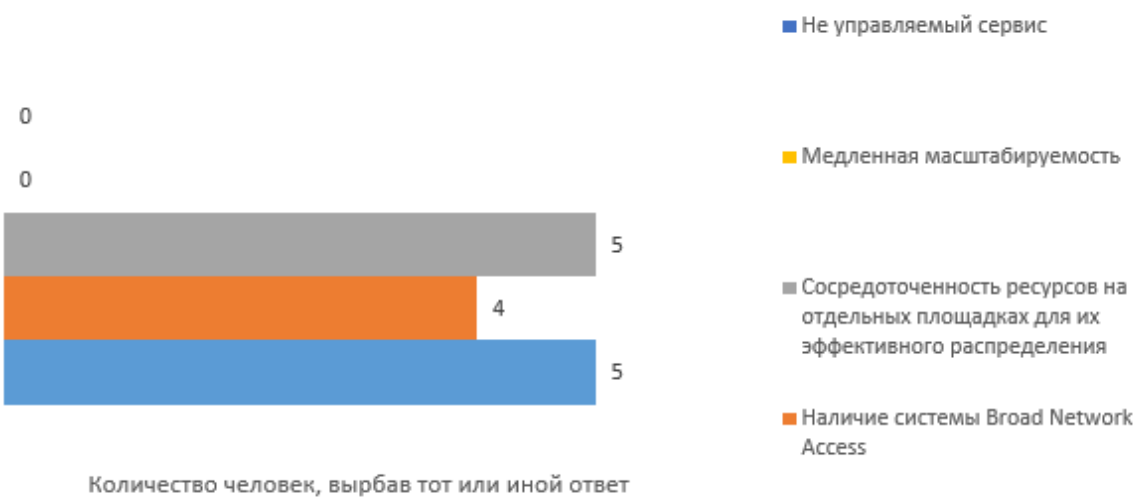
Контрольный тест №2



Вопрос 4. Выберите основной недостаток облачных сервисов: (6 ответов)

Вопрос 6. Какое утверждение является верным: (6 ответов)

Вопрос 7. Основные свойства облачных технологий - это:

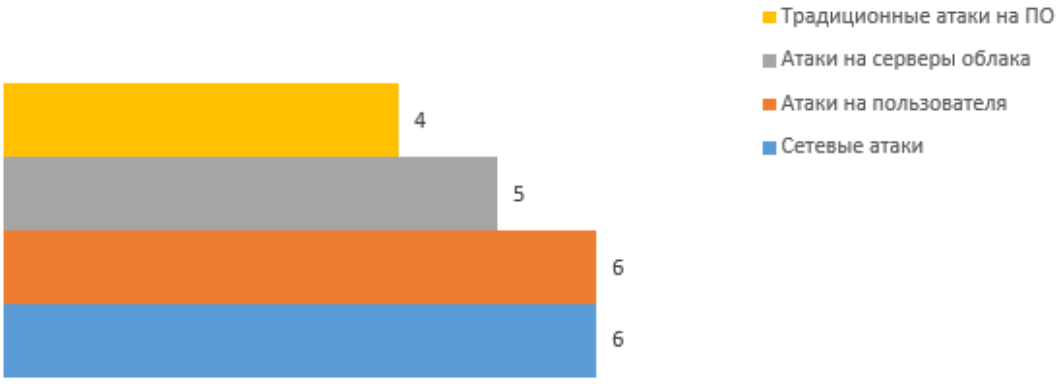


Количество человек, вырбав тот или иной ответ

Вопрос 8. Самыми важными элементами облачной системы являются:

(6 ответов)

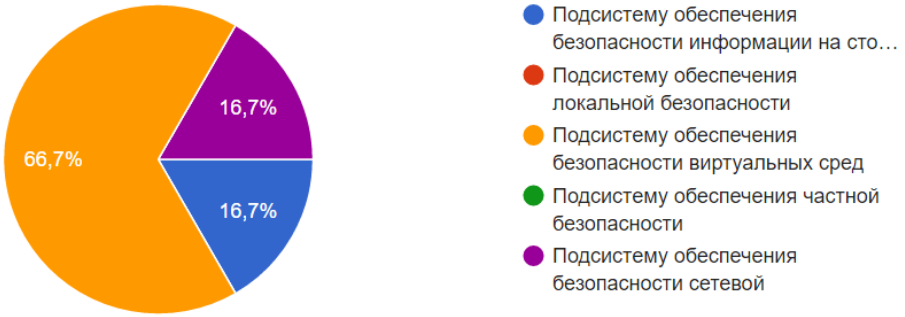
Ответ 9. Каким атакам подвержены облачные технологии?



Количество человек, вырбав тот или иной ответ

Вопрос 10. Для обеспечения информационной безопасности облаков система защиты информации должна включать в себя:

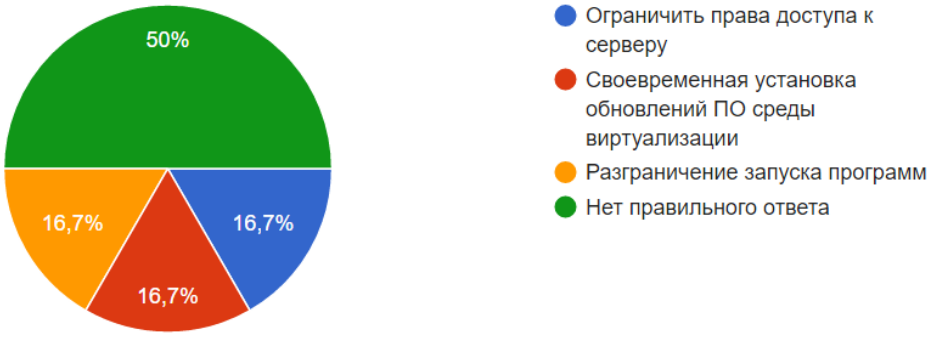
(6 ответов)



Вопрос 11. Элементы обеспечения безопасности информации на стороне пользователя

(6 ответов)

Вопрос 12. Для защиты гипервизора необходимо: (6 ответов)




Вопрос 13. Подсистема обеспечения безопасности ЦОД включает в себя следующие элементы:
Система открытой информации в ЦОД
Система контроля и управления доступом
Система резервного копирования и удаления данных
Охранное видеонаблюдение
1
5
3
6
Количество человек, вырбав тот или иной ответ


Вопрос 14. Элементы системы информационной безопасности ЦОД:
Средства обнаружения и предотвращения вторжений
Средства антивирусной безопасности
Средства ограничения доступа
Средства локального экранирования
Средства криптографической защиты информации
5
5
1
1
5
Количество человек, вырбав тот или иной ответ