Министерство образования и науки Российской Федерации Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РТФ

ОТЧЕТ

о проектной работе

по теме: Игра по информационной безопасности

по дисциплине: Проектный практикум

Команда: PIXELSQUAD

Екатеринбург

2022

# СОДЕРЖАНИЕ

[Введение 3](#_Toc106381393)

[Команда 5](#_Toc106381394)

[Целевая аудитория 6](#_Toc106381395)

[Календарный план проекта 9](#_Toc106381396)

[Определение проблемы 11](#_Toc106381398)

[Подходы к решению проблемы 12](#_Toc106381399)

[Анализ аналогов 13](#_Toc106381400)

[Требования к продукту и к MVP 16](#_Toc106381401)

[Стек для разработки 17](#_Toc106381402)

[Прототипирование 18](#_Toc106381403)

[Разработка системы 23](#_Toc106381404)

[Заключение 24](#_Toc106381405)

[Список используемых источников 27](#_Toc106381406)

Введение

Современное общество называется информационным. Широкое развитие средств вычислительной техники и связи позволило собирать, хранить, обрабатывать и передавать информацию в таких объемах и с такой оперативностью, которые были не мыслимы раньше. Благодаря новым информационным технологиям деятельность человека, его повседневная сфера общения безгранично расширяются.

Каждый человек пользуется социальными сетями, общается на форумах, пользуется различными интернет-сервисами, при этом оставляя множество своих данных в сети и возможно не подозревает, чем это может быть чревато, пока сам не столкнется с угрозой его данным, оставленных во всемирной паутине.

Актуальность данной работы заключается в том, что в связи с активным развитием цифровой сферы у людей появилась потребность защищать свои данные в сети, поэтому, чтобы обезопасить человека от сетевых угроз, необходимо посвятить его в тему информационной безопасности и научить правилам, которые необходимо соблюдать в сети, но сделать это «простым» языком, понятным человеку, не знакомому с информационным миром. В учебных и лекционных материалах используется сложная и незнакомая обычному пользователю терминология, поэтому целью нашей работы является создать образовательную игру, которая позволит в интересной и доступной каждому форме понять, как же защитить себя и свои данные в сети.

Исходя из поставленной цели в работе определены следующие задачи:

* Выявить основные виды угроз в сети для человека
* Проанализировать существующие продукты, связанные с обучением информационной безопасности
* Составить текстовый документ сетевых угроз и способов защиты от них
* Разработать обучающую защите в сети игру

Команда

* Скапинцева Виктория Викторовна РИ-110935 – тимлид
* Чекмарёв Артём Алексеевич РИ-110915 – дизайнер
* Балмошнова Ангелина Сергеевна РИ-110946 – аналитик
* Волков Дмитрий Евгеньевич РИ-110944 – программист
* Пичугин Михаил Сергеевич РИ-110932 – программист

Целевая аудитория

Для определения целевой аудитории мы использовали методику 5W Марка Шеррингтона. Это наиболее распространенный способ определения целевой аудитории и психологических характеристик, которыми обладают потенциальные потребители. Сегментация рынка проводится по 5 вопросам:

Что?

Это сегментация по типу товара: что мы предлагаем потребительской группе? Какие товары/услуги?

Мы предлагаем продукт, который в игровой форме позволит интересно и быстро усвоить теорию про информационную безопасность.

Кто?

Это сегментация по типу потребителя: кто приобретает товар/услугу? Какой пол, возраст?

Наш проект рассчитан на учеников школы с пятого по одиннадцатый класс.



Почему?

Это сегментация по типу мотивации к совершению покупки и потребления: какова потребность или мотивация клиента? какую проблему решает товар/услуга?

Исходя из опроса, проведенного среди людей (друзья, знакомые), мы выяснили, с какими проблемами, связанные с безопасностью данных, возникали в социальных сетях:



В современном мире все пользуются гаджетами и оставляю свои данные в сети, поэтому необходимо посвятить как можно больше себя в тему информационной безопасности.

Когда?

Это сегментация по ситуации, в которой приобретается продукт: когда потребители хотят приобрести товар/услугу?

Нашим продуктом потребитель может воспользоваться в любое время, когда есть желание получить знания или их закрепить.

Где?

Это сегментация по месту покупок: в каком месте происходит принятие решения о покупке и сама покупка? — имеются ввиду точки контакта с клиентом, где можно повлиять на решение.

Исходя из опроса, проведенного среди людей (друзья, знакомые, родственники), мы выяснили, что потребители в большинстве случаев используют компьютер для входа в интернет:

****

Точка контакта с клиентом – наш сайт. Наш продукт находится на сайте в открытом доступе для пользователей ПК.

Календарный план проекта

Название проекта: Образовательная игра по информационной безопасности

Руководитель проекта: Скапинцева Виктория Викторовна

Таблица 1 – Календарный план проекта

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | Название | Ответственный | Длитель-ность | Дата начала | Временный рамки проекта (недели) | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Анализ | | | | | | | | | | | | | | | | | | | |
| 1.1 | Определение проблемы | Пичугин М.С. | 1 неделя | 10.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.2 | Выявление целевой аудитории | Чекмарев А.А. | 1 неделя | 10.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.3 | Конкретизация проблемы | Пичугин М.С. | 1 неделя | 10.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.4 | Подходы к решению проблемы | Балмошнова А.С | 1 неделя | 10.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.5 | Анализ аналогов | Балмошнова А.С | 1 неделя | 17.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.6 | Определение платформы и стека для продукта | Волков Д. Е. | 1 неделя | 17.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.7 | Формулирование требований к MVP продукта | Чекмарев А. А | 3 недели | 24.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.8 | Определение платформы и стека для MVP | Волков Д. Е. | 3 недели | 24.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.9 | Формулировка цели | Скапинцева В. В. | 2 недели | 31.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.10 | Формулирование требований к продукту | Скапинцева В. В. | 2 недели | 31.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.11 | Определение задач | Скапинцева В. В. | 1 неделя | 07.04.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Проектирование | | | | | | | | | | | | | | | | | | | |
| 2.1 | Архитектура системы (компоненты, модули системы) | Волков Д. Е. | 1 неделя | 10.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.2 | Разработка сценариев использования системы | Балмошнова А.С | 1 неделя | 10.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.3 | Прототипы интерфейсов | Чекмарев А. А | 3 недели | 14.04.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.4 | Дизайн-макеты | Пичугин М. С. | 5 недель | 31.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.5 | Архитектура системы (компоненты, модули системы) | Волков Д. Е | 5 недель | 31.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Разработка | | | | | | | | | | | | | | | | | | | |
| 3.1 | Написание кода | Волков Д. Е. | 8 недель | 31.03.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.2 | Тестирование приложения | Скапинцева В. В. | 5 недель | 28.04.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Внедрение | | | | | | | | | | | | | | | | | | | |
| 4.1 | Оформление MVP | Пичугин М. С. | 4 недели | 07.04.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.2 | Внедрение MVP | Волков Д. Е | 6 недели | 28.04.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.3 | Написание отчета | Скапинцева В.В | 2 недели | 26.05.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.4 | Оформление презентации | Балмошнова А.С | 2 недели | 26.05.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Защита проекта | Скапинцева В.В. |  | 09.06.22-24.06.22 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Продолжение таблицы 1

Определение проблемы

Мы воспользовались рядом эффективных способов выявления основных проблем клиента:

1. Провели опрос, по итогу которого, выяснилось, что большинство людей проводят в сети большую часть своего дня, но мало кто знает как и зачем защищать свои данные в интернете.
2. Проанализировали поисковые запросы и тематические форумы, откуда смогли вынести проблемы, с которыми чаще всего сталкиваются пользователи в сети.
3. Изучили основных конкурентов и выявили неудобства, с которыми может столкнуться потенциальный пользователь.

Рассмотрев и обобщив данную информацию, мы выявили основную проблему – люди не знают какими способами защищать себя в сети, при поиске решения часто получают лишь кратковременное подавление проблемы, а также мы обнаружили, что многие сталкивались со взломами аккаунтов в социальных сетях и подвергались мошенничеству и вымогательству.

Подходы к решению проблемы

На основе анализа проблем пользователей и опросов мы выявили проблему угрозы данных человека в сети, частые взломы и подвергание мошенничествам. Это вызвано такими причинами, как:

* Незнание основных правил, которые нужно соблюдать в сети, чтобы обезопасить себя и свои данные
* Непонимание человеком уровня возможной угрозы от распространения своих данных
* Сложность восприятия существующих материалов для решения проблемы пользователя

Чтобы минимизировать количество проблем при использовании интернета сайты принимают следующие меры:

* Отображают шкалу «надежности» устанавливаемого пароля и способы сделать пароль более надёжным
* Предупреждают о возможном мошенничестве в сети
* Дают возможность отправить жалобу на пользователя за мошенничество, вымогательство и так далее

Однако человек может просто не понимать зачем нужны сложные пароли, которые трудно запомнить. Предупреждение о возможном мошенничестве не может обезопасить человека, так как никто не знает заранее, мошенник ли написавший человек. А блокировки пользователя в сети не дают никакой гарантии, что у человека нет другой страницы, и он не напишет снова.

Таким образом, ничто не защитит человека в сети, кроме самого пользователя, именно поэтому очень важно знать основы безопасности в интернете, чтобы минимизировать угрозы своим данным.

Анализ аналогов

При анализе рынка мы обнаружили 2 прямых конкурента, с аналогичной концепцией и рассчитанных на такую же целевую аудиторию, что и наш продукт

1. Игра-викторина «Информационная безопасность»

Достоинства:

* Различные по сложности вопросы дают разное количество очков

Недостатки:

* Игра состоит только из вопросов и ответов без предварительного объяснения материала, что значительно усложняет восприятие информации
* Нет интересного финала, основная задача только в том, чтобы ответить на большинство вопросов

1. Веб-квест по информационной безопасности

Достоинства:

* Многообразие комнат и заданий, которые нужно выполнить, чтобы выбраться
* Скрытые подсказки

Недостатки:

* Каждая комната – отдельная страница браузера
* Нет дополнительных подсказок, которые бы помогли понять куда нужно двигаться.

В целом при анализе рынка было найдено множество квест-игр в виде презентаций или веб-страниц. За последнее время множество компаний сделали огромное количество настольных игр со сценарием по информационной безопасности.

Игры которые были найдены, охватывали либо одну тему, либо несколько тем, но все же содержали трудную для понимания информацию.

По итогу, мы не нашли игру, которая позволит с одной стороны весело провести время, а с другой - в игровой форме донести полезную информацию.

В качестве конкурента также можно выделить книги, учебные пособия. Разумеется, что информация в них будет больше, но наш продукт выигрывает в подаче материла, ведь куда интереснее получать информацию играя, чем просто читать. Так же в нашем проекте подача идёт в форме диалога с персонажами, имеющими свой характер. Это создаёт ощущение общения.

Из преимуществ нашего проекта перед конкурентами можно выделить следующее:

* Удобство. Игра находится на одном сайте, переключаться между вкладками не нужно. Также, в отличие от настольных игра, ей не страшны механические повреждения.
* Большое количество теоретического материала, который будет преподноситься по мере игры, что облегчит учебный процесс и сделает его интересным.
* Информация преподноситься по средствам диалога с персонажем, что позволит создать ощущения общения.
* Большой игровой мир со спрятанными секретами, который будет интересно изучать.
* Интересные квесты для игрока вовлекут его в процесс обучения, из-за чего игрок сам захочет изучать информацию, а не будет учить её “через силу”.

Требования к продукту и к MVP

Требования систематизируются несколькими способами.

Требования клиентов

1. Получение знаний в сфере информационной безопасности.

2. Закрепить полученные знания.

3. Весело провести время во время получения информации.

4. Работа игры без ошибок, мешающих основной цели игры - получению информации.

Функциональные требования

1. Механизм подачи информации.

2. Тесты с вопросами по полученной от второстепенных персонажей информации.

3. Динамический мир, который будет интересно изучать.

4. Отсутствие багов.

Нефункциональные требования

1. Второстепенные игровые персонажами в прописанных с игроком диалогах хранят информацию.

2. Двери с контрольными вопросами.

3. Игровой персонаж, рельеф мира, враги, второстепенные персонажи с разными характерами, особые предметы, секретные места.

4. Тестирование игры.

Производные требования

1. Второстепенные персонажи имеют свои текстуры (внешность), пописанные диалоги.

Стек для разработки

Платформа для разработки игры: Godot Engine

Игра это: Web-приложение, которое находиться на сайте главного разработчика. Сайт на VDS сервере. Платформа для сайта - NGINX+Apache

Платформа для выставления задач к команде и хранению промежуточных результатов: Trello

Платформа для графики в игре: Paint.NET

Прототипирование

Прототипы игрового персонажа:



Рисунок 1. Женский персонаж

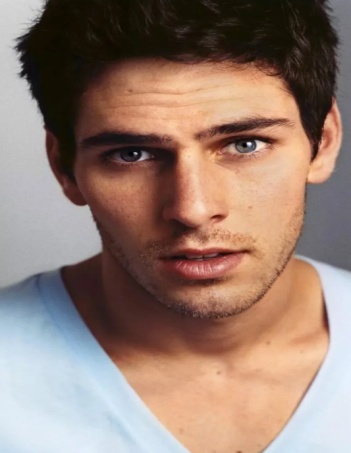


Рисунок 2. Мужской персонаж

Прототипы окружающего мира:



Рисунок . Виртуальный мир



Рисунок 4. Хаб

Прототипы врагов:



Рисунок 5. Сетевой червь

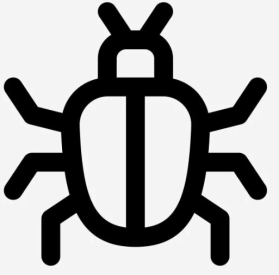


Рисунок 6. Баг

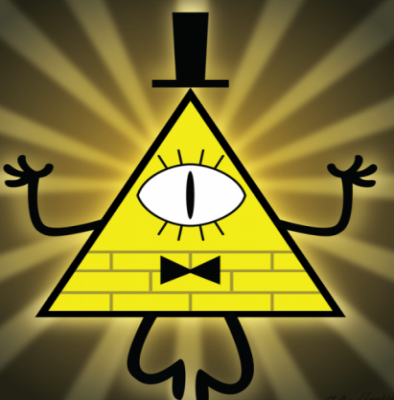


Рисунок 7. Враждебный треугольник

Прототипы второстепенных персонажей:



Рисунок 8.Кумчик

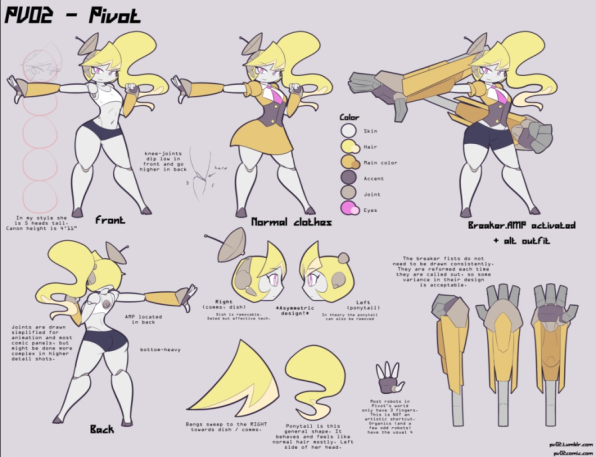


Рисунок 9.PV-02



Рисунок 10.Анонимус



Рисунок 11.Мия

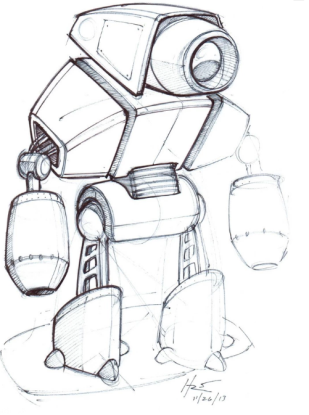


Рисунок 12.Роберт



Рисунок 13.Денис Борисович



Рисунок 14.Царь-бомба



Рисунок 15.Стасян

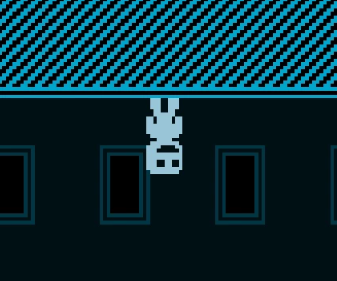


Рисунок 16.Капитан Виридиан

Разработка системы

Алгоритм работы игры:

1. Игрок появляется в виртуальном мире, где проходит обучение.

2. После обучения игроку предоставляется возможность исследовать окружающий мир как в хабе, так и в виртуальном мире, но исследование виртуального мира ограничено.

3. В виртуальном мире находится множество опасностей: разные виды врагов, препятствия в виде шипов и прыжков по отдельным блокам. Падение с высоты не снимает здоровье игрового персонажа, а вот враги и шипы могут снизить полозку здоровья до нуля, после чего придётся переигрывать с точки сохранения.

4. Взаимодействуя с второстепенными персонажами, игрок получает знания в сфере информационной безопасности.

5. Взаимодействие с второстепенными персонажами линейно, так как рядом с ними находятся запертые двери, для открытия которых необходимо прочесть теоретический материал, который предоставит именно этот персонаж.

6. Игра закончится только после взаимодействия со всеми персонажами.

7. В игре спрятаны секретные комнаты, после взлома которых можно получить кусочек перфокарты. Всего в таких комнатах можно получить 4 кусочка перфокарты, но для второй концовки нужно собрать 5. Недостающий кусочек выпадает с секретного босса.

8. В игре две концовки. Для получения первой концовки нужно просто дойти до финального босса и победить его. Для второй концовки необходимо собрать 5 кусочков перфокарты. В таком случае, в комнате перед финальным боссом можно взломать терминал, где будут предоставлены доп. вопросы, тем самым пропуская битву и уничтожая виртуальный мир.

Заключение

Рассмотренные вопросы в рамках данной проектной работы, являются основными при создании игры по информационной безопасности. Приведены определенные правила и принципы, которые позволят в дальнейшем правильно сопровождать, поддерживать, и грамотно разрабатывать новый функционал для данной разработки.

Основные технические решения, которые были предложены в данной проектной работе, включают в себя следующие аспекты:

* Платформа для разработки игры: GobotEngine – это универсальный 2D и 3D игровой движок, спроектированный для поддержки всех видов проектов. Вы можете использовать его для создания игр или приложений, которые можете затем выпускать на настольных или мобильных платформах, а также web.
* Платформа для сайта: NGINX+Apache.Apache и Nginx – это 2 самых распространенных веб-сервера с открытым исходным кодом в мире. Вместе они обслуживают более 50% трафика во всем интернете. Оба решения способны работать с разными рабочими нагрузками и взаимодействовать с другими приложениями для реализации полного веб-стека.
* Платформа для выставления задач к команде и хранению промежуточных результатов: Trello – облачная программа для управления проектами небольших групп. В ней удобно выставлять задачи, указывать на недостатки. Задание можно помечать разными тегами, например, как “Выполняется” или “Переделывается”. Это очень удобно. Также к карточкам в Trello можно прикреплять файлы, ссылки, оставлять комментарии для других участников команды, и наоборот, другие участники могут оставлять свои комментарии. Именно поэтому мы использовали Trello для хранения промежуточных результатов.
* Платформа для графики в игре: Paint.NET – растровый редактор для Microsoft Windows, разработанная на платформе .NET Framework. Его использование обусловлено тем, что он простой в использовании, многофункциональный, содержит необходимый функционал для редактирования и создания картинок, в нашем случае, графики для игры.

Используя упомянутые инструменты, мы получили продукт, подходящий для изучения тем в сфере информационной безопасности. Также функционал данных инструментов позволяет разработчикам добавить необходимый для заказчика контент, например, добавив персонажа, который прочитает лекцию по интересующей теме. Это можно отнести к перспективам проекта.

Плюсы:

* Игрок получает знания в сфере информационной безопасности, при этом весело проведя время.
* Для прохождения дальше по сюжету необходимо внимательно читать диалоги с второстепенными персонажами, в которых и заложены лекции. В противном случае игрок застрянет на одном месте, так как не сможет ответить на контрольный вопрос на дверях. Перебор вариантов ответов на дверях быстро надоест обычному игроку, так как при неправильном ответе придётся перепроходить с контрольной точки.
* Интересный и красивый игровой мир с множеством механик и предметов, который интересно исследовать.
* Игру не нужно скачивать.

Но есть и минусы:

* Ограниченный контент.
* Отсутствие возможности играть на мобильных устройствах.
* Постоянное соединение с интернетом во время игры, так как игра находится на web-сайте.

Целью проекта было создать готовый продукт, с помощью которого заказчик сможет получать информацию в сфере информационной безопасности, при этом играя.

Из цели следуют следующие задачи:

1. Проанализировать, кто будет целевой аудиторией игры, чтобы реализовать в игре баланс, выбрать сложность.
2. Проанализировать конкурентов.
3. Придумать сюжет игры. Определить, как будет преподноситься теоретический материал в сфере информационной безопасности.
4. Подготовить теоретический материал. Придать ему необходимый вид (в нашем случае – сжать информацию в диалоги второстепенных персонажей с игроком).
5. Найти прототипы персонажей, придумать им характер. Придумать врагов и препятствия.
6. Сделать текстуры игрока, игрового мира, врагов, второстепенных персонажей.
7. Реализовать структуру и физику мира, добавить персонажей, пользовательский интерфейс, сбалансировать врагов.
8. Протестировать получившийся результат, поискать и исправить баги.

В конечном итоге, нашей команде удалось выполнить поставленные задачи и реализовать готовый продукт.

список используемых источников

1. Бирюков А. «Информационная безопасность: защита и нападение» Учебное пособие. - М.: МГАП «Мир Книги», 2020. - 190 с.
2. Гродзенский С. Я. «Информационная безопасность. Учебное пособие», 2020. – 187 с.
3. Родичев Ю. «Нормативная база и стандарты в области информационной безопасности», 2016. – 352 с.
4. Сэрра Эллисон «Кибербезопасность: правила игры», 2021. – 208 с.
5. Эриксон Джон «Хакинг: искусство эксплойта», 2018. – 218 с.
6. Веб – квест по информационной безопасности:

<http://quest.school15yi.ru/>

1. Викторина «Безопасность пользователей в сети Интернет»:

<https://quiz.safe-surf.ru/>