Интеллектуальная игра «Что? Где? Когда?»

для школьников 8-9 классов

Тема. Информационная безопасность

**Автор:** *Бойко Татьяна Павловна – учитель информатики*

**Цель**

•Сформировать и развить интеллектуальное движение учащихся.   
•Выявить сильнейшие команды.   
•Развить конкурентные качества школьников.  
**Условия проведения игры**:  
•В игре принимают участие команды 8-9 классов.  
•Состав команды- 6 человек.  
**Оформление:**мультимедийное оборудование для выбора вопросов.

**Ход игры:**  
**Ведущая:**

Добрый день! Мы рады вас приветствовать на игре « Что? Где? Когда?».

Игра проводится между знатоками и зрителями.  
Напомню правила игры: программа случайным образом выбирает вопрос, вам даётся одна минута для обсуждения. По истечении минуты, вы даёте ответ.  
Затем я произношу правильный ответ, и результаты вносятся в таблицу. Если команда правильно ответила на вопрос, она получает один балл. Игра продолжается до шести очков. Каждая команда играет отдельно. Победа присуждается команде, набравшей большее количество очков.   
**Минутная готовность   
Ни пуха, ни пера.**  
**Вопросы:**  
1 *Источники взлома серверов.*

**Внешний источник** Им пользуются конкуренты либо хакеры, которым не терпится завладеть какими-либо секретными данными конкретной организации. Как правило, при взломах такого рода в сеть компьютеров запускается вирус, который передает всю нужную информацию «хозяину». Или же, что сейчас довольно актуально, серверы компании просто подвергаются массовому наплыву спама, из-за чего отключаются и сеть остается без должной защиты. К слову, именно таким образом была отключена сеть компьютеров крупной организации, занимавшейся борьбой с вредоносными программами.

**Смешанный источник** можно охарактеризовать как взаимно выгодный тандем между фирмой-конкурентом и, например, сотрудником компании, у которой и нужно выкрасть данные. Здесь все очень просто: конкурент ищет сотрудника в требуемой организации, который за определенную плату может выкрасть какие-либо важные данные. Такого рода проблемы носят действительно глобальный характер, ведь подавляющая часть таких преступлений совершается именно этим способом. Выявить неблагонадежных работников очень трудно и зачастую даже невозможно, так что остается лишь надеяться на защищенность самой системы.

2 *Модели безопасности компьютерных систем*

. Организационная сторона вопроса- полный контроль над доступом к главным компьютерным сетям, так называемых третьих лиц, которые не обладают должными правами. Этот пункт обеспечения информационной безопасности является одним из главных, ведь зачастую именно недобросовестные работники становятся виновниками утечки важной информации;

- Техническая сторона вопроса - включает в себя множество пунктов информационной безопасности, таких, как кража важных данных с помощью вирусов, различных физических носителей. Этот пункт тоже является важным при обеспечении информационной безопасности, ведь зачастую выкрасть данные, просто скопировав их, у хакера не получится. Информационную безопасность компьютерных систем обеспечивают, прежде всего, специальные антивирусы, которые следят за общим состоянием безопасности компьютерной системы круглосуточно.

Определение того, что к компьютеру подключено какое-либо стороннее устройство, выполняется посредством специальных продуктов, которые также могут заблокировать использование различных новых устройств, если они не находятся в списках доверенных.

3 *Методы улучшения защиты от вредоносного ПО и безопасности компьютера.*

**Установите антивирусные и антишпионские программы из надежных источников**

**Регулярно обновляйте программное обеспечение**

**Используйте надежные пароли и храните их в секрете.**

**Никогда не отключайте брандмауэр.**

**Осторожно используйте флеш-накопители.**

Не соглашайтесь на загрузку, предлагаемую вредоносным ПО.

4 *Надежный пароль.*

Надежность любого пароля зависит от того, насколько разнообразные символы вы используете в нем, общей длины пароля, а также от того, можно ли его найти в словаре. Длина пароля должна составлять восемь или более знаков.

5 *Что такое фишинг?*

(от английского слова «fish», что означает «рыба» или «рыбачить»), так как их цель – «выудить» у вас ваши персональные данные.

6 *Как распознать фишинг-атаку?*

сведения, вызывающие тревогу, или угрозы, например, закрытия ваших банковских счетов;

обещания большой денежной выгоды с минимальными усилиями или вовсе без них;

сведения о сделках, которые слишком хороши, для того, чтобы быть правдой;

запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;

грамматические и орфографические ошибки.

7 *Популярные фишинговые схемы.*

**Мошенничество с использованием бренда Microsoft или других известных компаний.** В таких мошеннических схемах используются поддельные сообщения электронной почты или веб-сайты, содержащие название корпорации Microsoft. В них могут сообщать о победе в каком-либо конкурсе, проводимом компанией, о том, что Microsoft требуются ваши учетные данные и пароль, о том, что к вам обращается представитель Microsoft, чтобы помочь в решении проблем с компьютером, и т.п. Подобные мошеннические схемы от лица службы технической поддержки также могут производиться по телефону.

**Подложные лотереи.** Вы можете получить сообщения, в которых говорится о том, что вы выиграли в лотерею, которая проводится корпорацией Microsoft. Внешне эти сообщения могут выглядеть так, как будто они были отправлены от лица одного из высокопоставленных сотрудников компании

**Ложные антивирусы и программы для обеспечения безопасности.** Подобное мошенническое ПО, также известное под названием «scareware», – это программы, которые выглядят так, как будто они обеспечивают безопасность вашего ПК, хотя, на самом деле, все обстоит совсем наоборот. Такие программы генерируют ложные уведомления о различных угрозах, а также пытаются завлечь пользователя в мошеннические транзакции. Вы можете столкнуться с ними в электронной почте, онлайн объявлениях, в социальных сетях, в результатах поисковых систем и даже во всплывающих окнах на компьютере, которые имитируют системные сообщения.



8 *Действия при подозрении фишинговой атаки.*

Смените пароли или PIN-коды во всех своих онлайн-аккаунтах, которые могли быть скомпрометированы.

Добавьте предупреждение о мошенничество в свои отчеты по кредитам. Если вы не знаете, как это сделать, обратитесь в банк или к финансовому консультанту.

Обратитесь в банк или в интернет-магазин напрямую. Не переходите по ссылкам в фишинговом сообщении.

Если вам стало известно о мошенническом доступе к счетам или открытии счетов, закройте их.

Ежемесячно просматривайте банковские выписки и отчеты по операциям с кредитной картой, обращая внимание на необъяснимые траты или запросы, которые вы не инициировали.

9 *Защита своей конфиденциальности в сети Интернет.*

**Сначала прочтите политику конфиденциальности сайта**

**Не давайте больше данных, чем необходимо**

* Не публикуйте никакой информации в сети, которую вы не хотите сделать общедоступной.
* Сократите количество деталей, которые идентифицируют вас или ваше местонахождение.
* Храните номера своих счетов, имена пользователей и пароли в секрете.
* Давайте свой адрес электронной почты или имя в системе мгновенных сообщений только тем, кого вы знаете, а также организациям с прочной репутацией. Старайтесь не указывать свой адрес или имя в интернет-каталогах, а также на сайтах с объявлениями о вакансиях.
* Вводите только ту информацию в регистрационных и других формах, которая является обязательной. Часто соответствующие поля помечены звездочкой (\*).

**Выбор степени конфиденциальности профиля или блога**

## Контроль материалов, публикуемых другими пользователями

* Поищите свое имя в Интернете, используя как минимум две поисковые системы. Выполните текстовый поиск и поиск по изображениям. Если вы найдете секретную информацию о себе на каком-либо веб-сайте, найдите контактную информацию этого сайта и отправьте запрос на удаление этой информации.
* Регулярно проверяйте, что другие пишут о вас в блогах и на сайтах социальных сетей. Попросите друзей не публиковать фотографии вас и вашей семьи без вашего разрешения. Если вам не нравится информация или фотографии, которые опубликованы на веб-сайтах других пользователей, попросите их удалить.

11 *Что такое Информационная безопасность*

Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

12 *Перечислите Нормативные документы в области информационной безопасности.*

Акты федерального законодательства:

* Международные договоры РФ;
* Конституция РФ;
* Законы федерального уровня (включая федеральные конституционные законы, кодексы);
* Указы Президента РФ;
* Постановления Правительства РФ;
* Нормативные правовые акты федеральных министерств и ведомств;
* Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

13 *Что такое Криптография.*

это наука о том, как обеспечить секретность сообщения.

14 *Что такое Электронная подпись.*

это реквизит электронного документа, предназначенный для его защиты от подделки. ЭП позволяет определить владельца подписи, а также определить отсутствие изменений в электронном документе после его подписания.

15 *Назначение межсетевых экранов.*

Межсетевые экраны (firewall, брандмауэр) делают возможной фильтрацию входящего и исходящего трафика, идущего через вашу систему. Межсетевой экран использует один или более наборов <<правил>> для проверки сетевых пакетов при их входе или выходе через сетевое соединение, он или позволяет прохождение трафика или блокирует его. Правила межсетевого экрана могут проверять одну или более характеристик пакетов, включая но не ограничиваясь типом протокола, адресом хоста источника или назначения и портом источника или назначения.

Межсетевые экраны могут серьезно повысить уровень безопасности хоста или сети. Они могут быть использованы для выполнения одной или более нижеперечисленных задач:

* Для защиты и изоляции приложений, сервисов и машин во внутренней сети от нежелательного трафика, приходящего из внешней сети интернет.
* Для ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети интернет.
* Для поддержки преобразования сетевых адресов (network address translation, NAT), что дает возможность задействовать во внутренней сети приватные IP адреса и совместно использовать одно подключение к сети Интернет (либо через один выделенный IPадрес, либо через адрес из пула автоматически присваиваемых публичных адресов).

16 *Что такое Анализатор трафика.*

сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.