



Киберугрозы современности: правила их распознавания и предотвращения

Березовский филиал МБОУ М – Алабушской сош
Учитель информатики: Митрофанова Н.А.
Дата проведения 06.10.2015 г.

Возможности Интернета

- * Доступ к информационным ресурсам (источник дополнительной информации для повышения эрудированности и выполнения учебных проектов);
- * Доступ к системам тестирования (контроль знаний школьников или тренажер при подготовке к ГИА);
- * Доступ к учебно-методическим материалам научного, познавательного характера;
- * Доступ к энциклопедическим и справочным ресурсам;
- * Доступ к средствам Интернет - вещания;
- * Информационное взаимодействие (процесс приема-передачи информации, коммуникационные сервисы);

СПРАВОЧНАЯ ИНФОРМАЦИЯ



Популярны следующие виды
и формы онлайн-развлечений:

- социальные сети;
- сетевые игры;
- просмотр и скачивание фильмов, клипов,
аудиофайлов, программ;
- обмен файлами;
- использование электронной почты,
сервисов мгновенного обмена
сообщениями, чатов;
- ведение блогов и пр.

НЕГАТИВНОЕ ВЛИЯНИЕ ИНТЕРНЕТА

- * Влияние на физическое здоровье человека;
- * Влияние на психическое здоровье человека;
- * Агрессия
- * Сайты с недопустимым содержанием;
- * Интернет-мошенники.



Показ социального видеоролика «Безопасный интернет – детям!»

- * Цель: расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков

Что вы знаете об угрозах, которые исходят из Интернета?



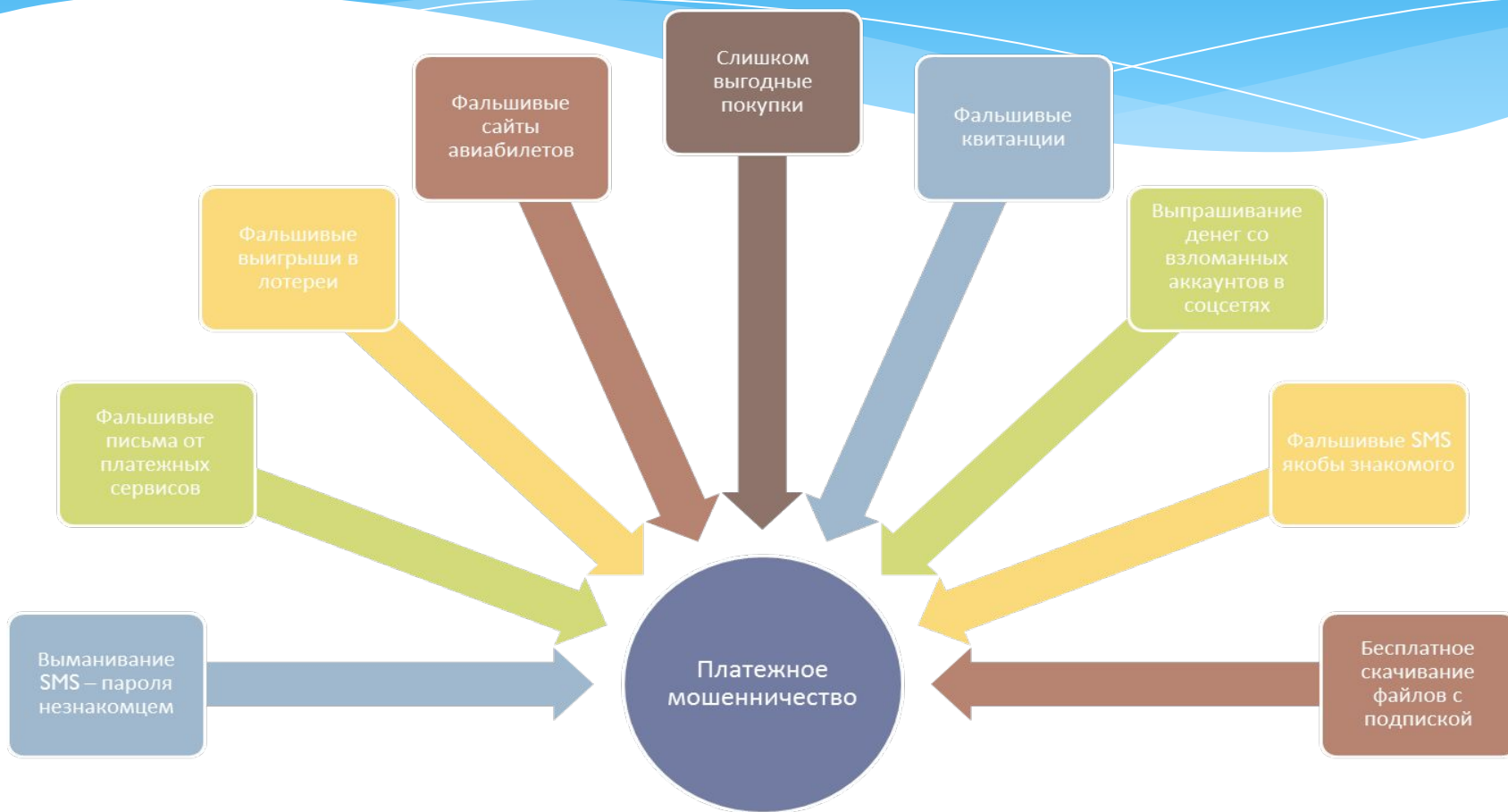
Вирусы

Мошеннические письма

Получение доступа к аккаунтам в социальных сетях и других сервисах

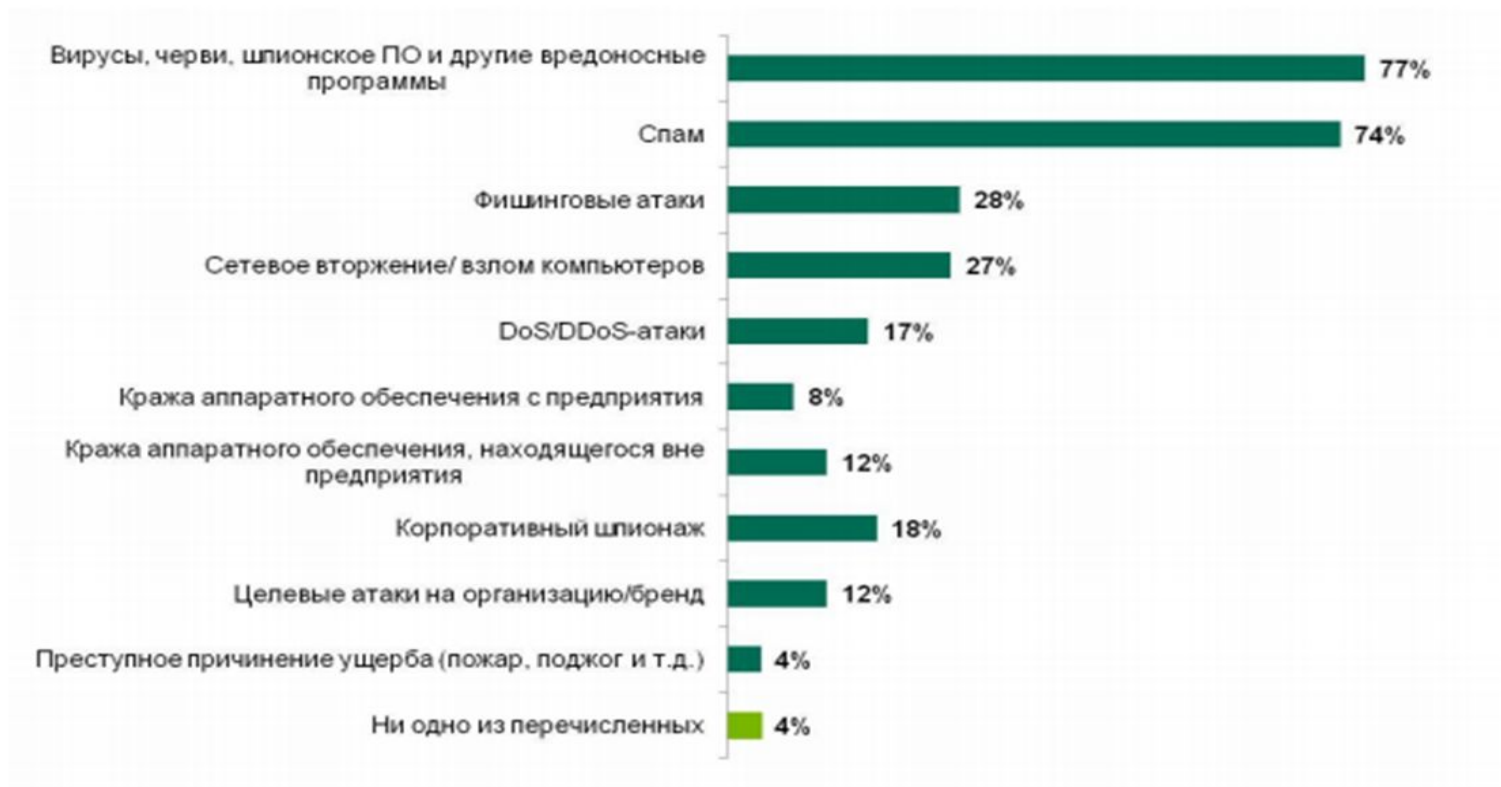


Что вы знаете об угрозах, которые исходят из Интернета?



Данные «Лаборатории Касперского»

Типы внешних угроз, с которыми сталкивались российские компании



Откуда может исходить опасность?



Основные правила защиты от киберугроз

- * 1. **Не входите** на незнакомые сайты.
- * 2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, **обязательно проверьте его на вирусы**.
- * 3. Если пришло незнакомое вложение, ни в коем случае **не запускайте** его, а лучше сразу удалите и очистите корзину.
- * 4. Никогда не посылайте никому свой **пароль**.
- * 5. Старайтесь использовать для паролей **трудно запоминаемый набор цифр и букв**.
- * 6. При общении в Интернет не указывать свои личные данные, а **использовать псевдоним (ник)**.
- * 7. Ни в коем случае **не встречаться** с людьми, с которыми познакомились в сети Интернет.
- * 8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней **не было указано** никакой личной информации.
- * 9. В настоящее время существует множество программ, которые производят **фильтрацию** содержимого сайтов. Между членами семьи должны быть доверительные отношения, чтобы вместе просматривать содержимое сайтов.
- * 10. Не всей той информации, которая размещена в Интернете, можно верить.

Практикум «Угроза 419»

- * Цель: формирование навыков распознавание спама в «нигерийских письмах»
- * Задание:
 - * 1. Внимательно прочитайте текст письма.
 - * 2. Выделите в нем моменты, указывающие на то, что это спам.
 - * 3. Перечислите факты, указанные в письме, которые кажутся вам недостоверными, подозрительными



ПОМНИТЕ!



- * Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

ИСТОЧНИКИ

- * Методические рекомендации по проведению в общеобразовательных организациях Российской Федерации тематических уроков, посвященных вопросам безопасности в сети Интернет (материалы ФГНУ "Институт информатизации образования" Российской академии образования)
- * http://go.mail.ru/search_images?q=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B3%D1%80%D0%BE%D0%B7%D1%8B#urlhash=0
- * http://www.youtube.com/watch?v=9uvNVZMdelk&feature=player_embedded
- * http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf
- * https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%BB%D0%B0%D0%B2%D0%BD%D0%B0%D1%8F_%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0