



Институт мониторинга и оценки
информационной безопасности

Аналитический отчет

«Результаты исследования поведения
работников образовательных организаций и
соблюдения ими правил информационной
безопасности при работе
в сети Интернет»

СОДЕРЖАНИЕ

АННОТАЦИЯ.....	3
I. ПРИ КАКИХ УСЛОВИЯХ И ДЛЯ ЧЕГО ИСПОЛЬЗУЕТСЯ ИНТЕРНЕТ.....	4
1.1. Использование Интернета	4
1.2. Основные цели использования сети Интернет.....	5
1.3. Основные поисковые системы	6
1.4. Устройства для входа в Интернет.....	6
II. СОБЛЮДЕНИЕ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИНТЕРНЕТА.....	7
2.1. Использование паролей.....	7
2.2. Использование резервного копирования.....	8
2.3. Интернет-угрозы	9
2.3.1. Буллинг в Интернете.....	9
III. НАЛИЧИЕ ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ, НЕОБХОДИМЫХ ДЛЯ БЕЗОПАСНОЙ РАБОТЫ В ИНТЕРНЕТЕ.....	10
3.1. Повышение компетенций в сфере информационной безопасности.....	10
3.2. Основные умения, которыми обладают респонденты.....	10
IV. СПОСОБНОСТЬ ПРОТИВОСТОЯТЬ ИНТЕРНЕТ-УГРОЗАМ.....	11
4.1. В случае получения от незнакомого человека оскорбительного сообщения в социальной сети респонденты поступят следующим образом.....	11
4.2. В случае, если на рабочий почтовый ящик придет письмо от администрации почтового сервиса с просьбой выслать пароли для восстановления доступа, респонденты поступят следующим образом.....	11
4.3. В случае, если на личную электронную почту придёт сообщение о выигрыше недели проживания в пятизвёздочном отеле на курорте, и для получения приза просят немедленно оплатить билеты, а для этого нужно прислать данные банковской карты, то респонденты поступят следующим образом.....	12
КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ.....	13
РЕКОМЕНДАЦИИ.....	14

АННОТАЦИЯ

Исследование проводилось с целью определения условий и факторов, способствующих нарушению правил информационной безопасности работниками образовательных организаций, а также на выявление у работников образовательных организаций знаний и умений, необходимых для работы в быстро меняющемся информационном пространстве Всемирной паутины и готовности противодействовать Интернет-угрозам.

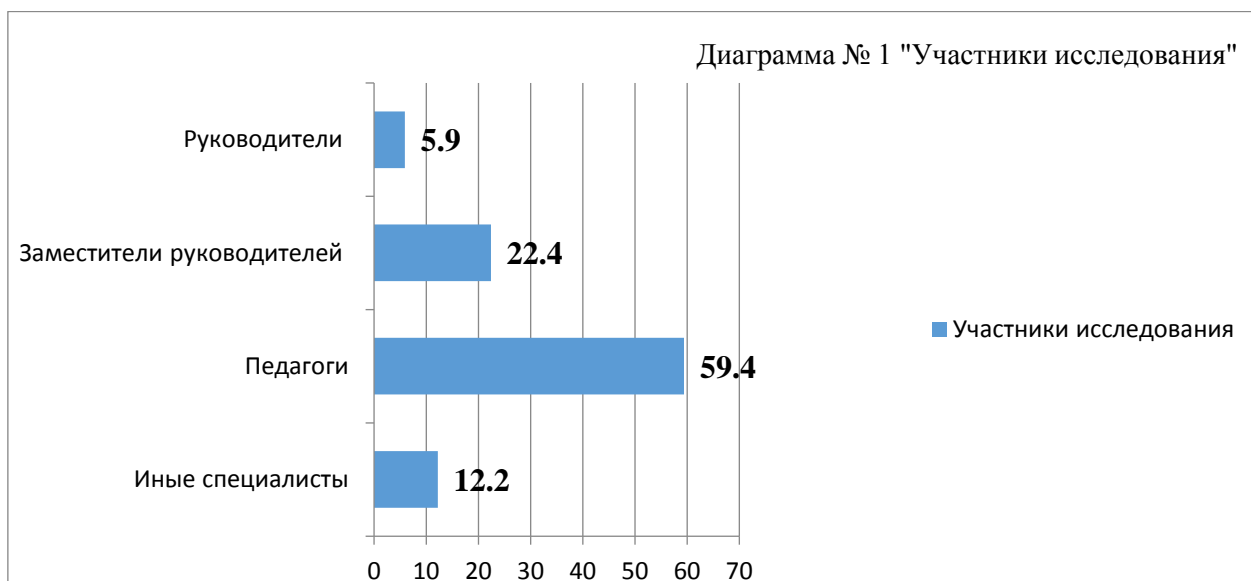
Актуальность исследования продиктована увеличивающимся количеством инцидентов в Интернете с участием представителей образовательных организаций (размещением конфиденциальной информации, конфликтами в сети, утечками паролей и персональных данных электронных журналов, взломами страниц и случаями травли учителей и учеников в социальных сетях) и т.д. Возросшей активностью в сети Интернет экстремистских, террористических группировок и деструктивных культов, пропагандирующих культы насилия и смерти, межнациональной и межконфессиональной розни. Данные факты побудили экспертов Института мониторинга и оценки информационной безопасности (г. Москва) совместно с Учебным центром «АСТА-информ» (г. Челябинск) провести исследование под названием «Безопасное поведение в Интернете».

Исследование проводилось в IV квартале 2016 года по 4 основным блокам:

- I. При каких условиях и для чего используется Интернет.
- II. Соблюдение правил информационной безопасности при использовании Интернета.
- III. Наличие знаний, умений и навыков, необходимых для безопасной работы в Интернете.
- IV. Способность противостоять основным интернет-угрозам.

Также в исследование были включены вопросы, касающиеся проведения уроков по медиабезопасности для учеников и их родителей.

Участники исследования: В исследовании приняло участие **1850** представителей образовательных организаций Тверской области, Курганской области, Свердловской области, Ростовской области, Ханты-Мансийского автономного округа, Челябинской области, Оренбургской области, из них (см. Диаграмму №1).



Эксперты провели анализ 1850 анкет, из них:

- руководителей – 5,9 %;
- заместителей руководителей – 22,4 %;
- педагогов – 59,4 %;
- иных специалистов – 12,2 %.

В ходе исследования были получены следующие результаты.

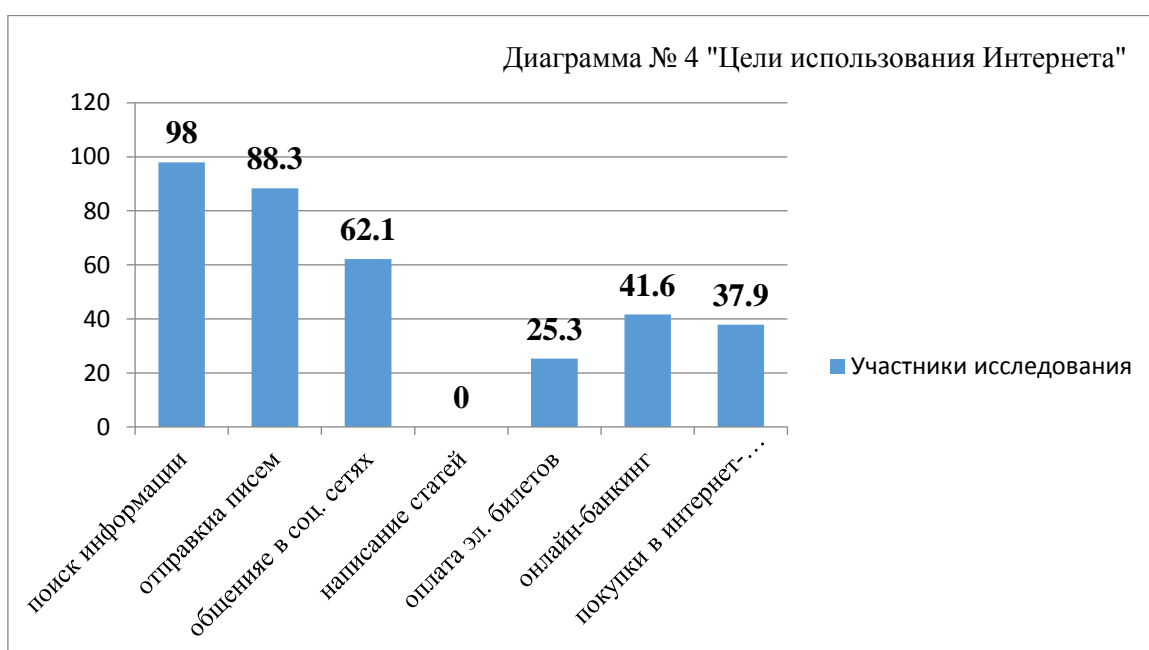
I. ПРИ КАКИХ УСЛОВИЯХ И ДЛЯ ЧЕГО ИСПОЛЬЗУЕТСЯ ИНТЕРНЕТ.

1.1.Использование Интернета на работе и дома:



- 89,7 % подавляющее большинство респондентов для подготовки уроков, поиска информации, оправки писем используют Интернет в рабочее время;
- 10,3 % респондентов в рабочее время Интернет не используют. (см. Диаграмма №2 «Использования Интернета на работе»)
- 97,2 % респондентов используют Интернет дома.
- 2,8 % респондентов дома Интернет не используют. (см. Диаграмму № 3 «Использование Интернета дома»)

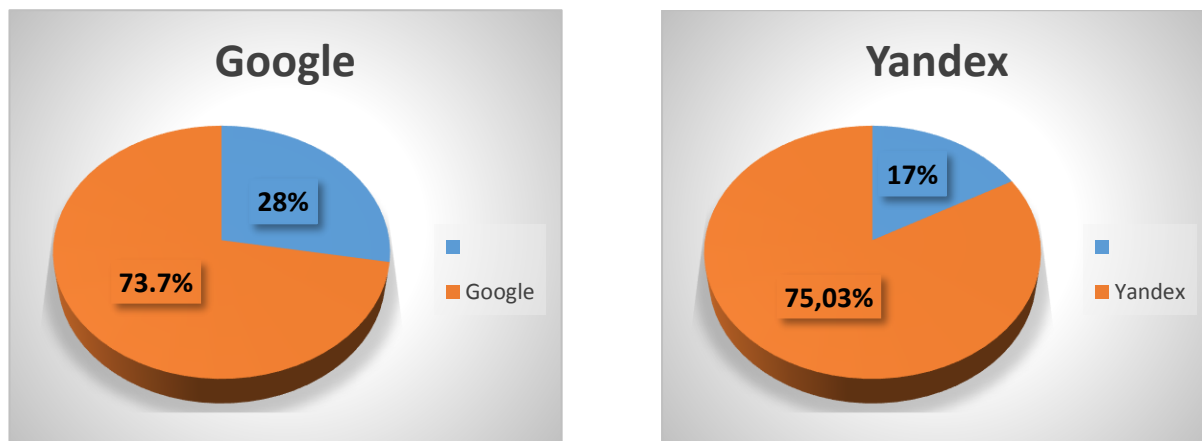
1.2. Основные цели использования сети Интернет:



- 98 % респондентов используют Интернет как средство поиска информации по своей профессиональной деятельности;
- 88,3 % респондентов осуществляют отправку электронных писем;
- 62,1 % респондентов выстраивают коммуникации и общение в социальных сетях;
- 31,4 % респондентов используют Интернет для написания статей и постов на форумах;
- 25,3 % опрошенных используют Интернет для оплаты электронных билетов;
- 41,6 % респондентов осуществляют переводы в онлайн-банках;
- 37,9 % респондентов осуществляют покупки в Интернет-магазинах. (см. Диаграмму №4 «Цели использования Интернета»)

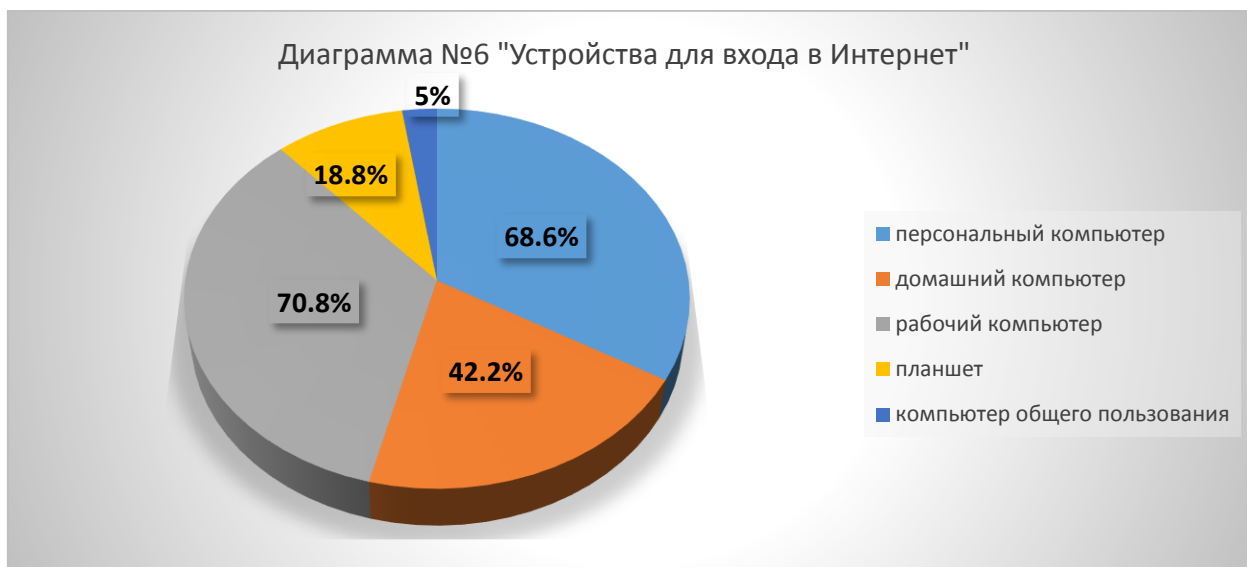
1.3. Основными поисковыми системами для респондентов являются:

Диаграмма №5 «Поисковые системы»



- Поисковик Google используют 73,7 % респондентов;
- Поисковик Yandex используют 75,03 % респондентов.

1.4. Для входа в Интернет респонденты используют различные устройства:

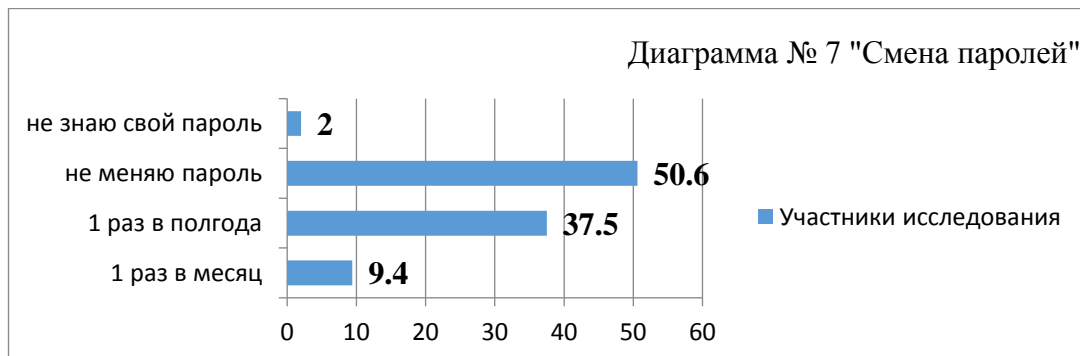


- 68,6 % респондентов работают в сети Интернет, используя свой персональный компьютер или ноутбук;
- 42,2 % пользователей используют компьютер или ноутбук, к которому имеют доступ другие пользователи (например, родственники);
- 70,8 % респондентов используют для работы в сети рабочий компьютер;
- 18,8 % респондентов используют планшет;
- 5% для работы в сети Интернет используют общественный компьютер (см. Диаграмма №6 «Устройства для входа в Интернет»).

II. СОБЛЮДЕНИЕ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИНТЕРНЕТА.

2.1. Использование паролей

Смена паролей:



- 37,5 % меняют пароли один раз в полгода и реже.

Это не может не настораживать:

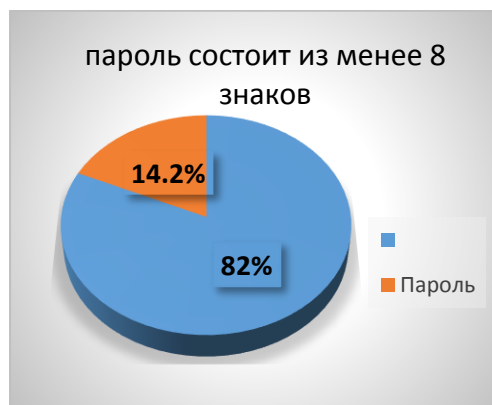
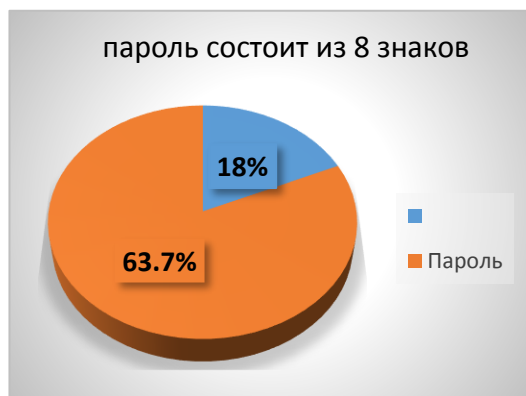
- 9,4 % респондентов меняют пароли один раз в месяц;
- 50,6 % респондентов никогда не меняли пароли,
- 2,2 % не знают свои пароли, и пароли им меняют люди из ближайшего окружения.

Резюме: Более половины респондентов **62,8% не соблюдают правила по смене и обновлению паролей для своих Интернет-ресурсов.** Так же частая смена пароля не является адекватным способом защиты, так как выбираются простые для запоминания пароли, что облегчает взлом пароля методом перебора.

Правило безопасности: пароль создается и изменяется пользователем! Пароль необходимо периодически изменять. Нельзя доверять создание и смену пароля даже своим ближайшим родственникам.

Надежность пароля:

Диаграмма №8 «Надежность пароля»

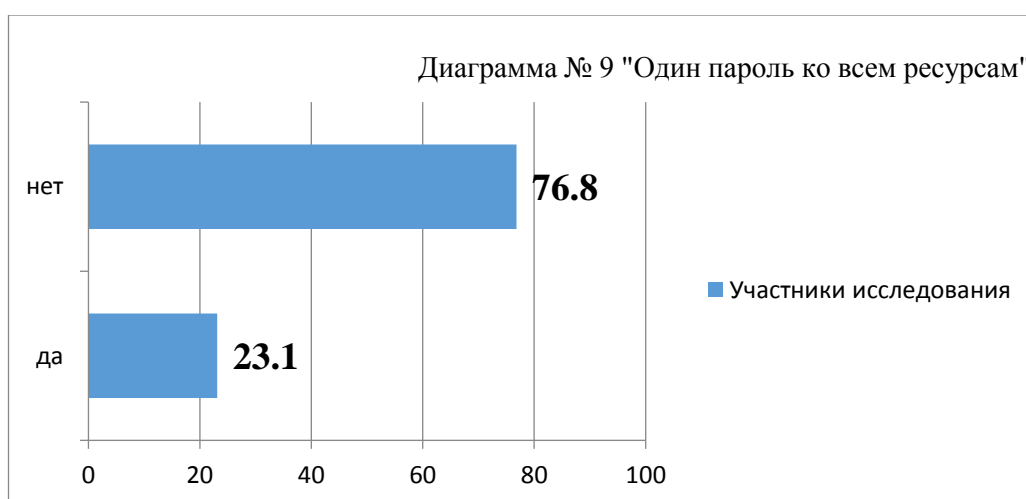


- 63,7 % респондентов подтвердили, что их пароли состоят из более чем 8 знаков, сочетающих цифры и буквы в разных регистрах;
- 14,2 % респондентов имеют более простые пароли.

Правило безопасности: Надежный пароль должен содержать не только количество знаков от 8 и более, содержать буквы и цифры в разных регистрах, но и символы, например ! " # \$ % &, тем самым увеличивая время и затрудняя взлом пароля методом перебора.

Контрольный вопрос: «У вас один и тот же логин и пароль доступа ко всем ресурсам Интернета?»

- 23,1 % респондентов ответили утвердительно «да».
- 76,8 % респондентов ответили, что имеют разные пароли к ресурсам Интернета (см. Диаграмму «Один пароль ко всем ресурсам»)



Резюме: 23,1 % респондентов в случае атаки на их информационные ресурсы

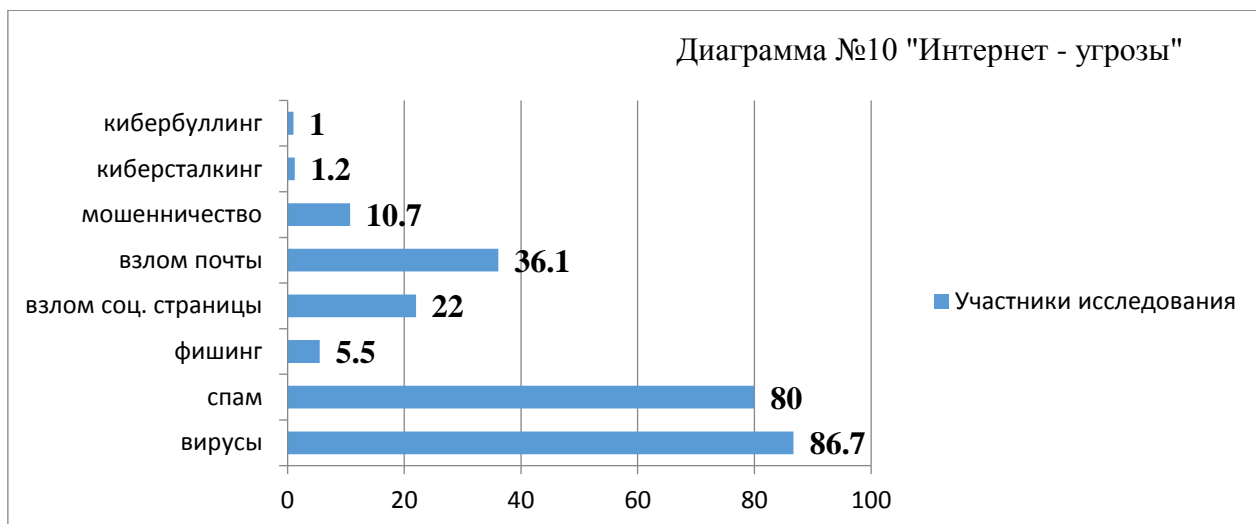
1. Потеряют доступ ко всем своим Интернет ресурсам (почте, странице в социальных сетях, онлайн-кошельку и т.д.)
2. Способствуют раскрытию конфиденциальных сведений, других пользователей, находящихся с ними в переписке и контакте.
3. Облегчают работу злоумышленникам по организации атак на информационные ресурсы других пользователей Интернета.

Правило безопасности: К каждому Интернет-ресурсу у пользователя должен быть свой отдельный надежный пароль.

2.2. Использование резервного копирования

- 68,1 % респондентов осуществляют резервное копирование и изолированное хранение важной информации;
- 31,8 % не осуществляют резервное копирование информации.

2.3. Интернет-угрозы с которыми сталкивались респонденты:



- 86,7 % респондентов сталкивались с вирусами, блокированием страниц браузера или компьютера;
- 80 % респондентов сталкивались со спам рассылкой;
- 5,5 % респондентов сталкивались с фишингом;
- 22 % взламывали или воровали страницы в социальных сетях;
- 36,1 % подвергались взлому почтового ящика;
- 10,7 % респондентов сталкивались с мошенничеством;
- 1,2 % респондентов сталкивались с киберсталкингом;
- 1 % респондентов сталкивались (см. Диаграмма №10 «Интернет-угрозы»).

2.3.1. На контрольные вопросы о буллинге, «травле» в сети (негативные письма на почту, негативные посты в социальных сетях) респонденты ответили следующим образом:



- 8,2 % респондентов образовательных организаций, подвергались «травле» в Интернете.
- 18,6 % опрошенных считают, что ученики их школ подвергались «травле» в сети Интернет.

III. НАЛИЧИЕ ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ, НЕОБХОДИМЫХ ДЛЯ БЕЗОПАСНОЙ РАБОТЫ В ИНТЕРНЕТЕ

3.1. Повышение компетенций в сфере информационной безопасности:

- 28 % респондентов повышают свою компетентность самостоятельно 1 раз в месяц;
- 9,4 % респондентов повышают компетентность 1 раз в полгода на специализированных семинарах Учебных центров;
- 28,3 % респондентов повышают квалификацию по информационной безопасности на специализированных курсах.
- 34,2 % респондентов не повышают свою компетентность.

На контрольный вопрос: «Какое ведомство ведет реестр запрещенных сайтов в РФ?»»

- 48,8 % ответили верно, что данный реестр ведет Роскомнадзор.
- **Важно:** 51,1 %, то есть более половины респондентов, не знают ответа на данный вопрос. (см. Диаграмма №12 «Реестр запрещенных сайтов ведет Роскомнадзор?»)



3.2. Основные умения, которыми обладают респонденты:

- определять, какие файлы стоит скачивать, а какие - нет 57 %
- обеспечивать защиту своей информации, хранящейся в интернете 34,8 %
- использовать безопасный поиск в поисковых системах 51 %
- при сбое подключения к интернету определять причины технических проблем 29,4 %
- очищать компьютер от вирусов, попавших в него через интернет 56,4 %
- обращаться в службы технической поддержки 59,4 %
- добавлять пользователей в «черные списки» или «банить» 53,5 %
- менять настройки конфиденциальности в социальных сетях и в сервисах для общения, чтобы их информация была доступна только определенным людям 42,7 %

- определять степень конфиденциальности и безопасности передачи личных данных при пользовании услугами через интернет 0 %
- избегать того, чтобы становиться жертвой наиболее распространенных схем мошенничества в интернете 36,2 %
- решать проблемы, возникшие при столкновении с мошенничеством в интернете 16,9 %
- затрудняюсь ответить 9,9 %

IV. СПОСОБНОСТЬ ПРОТИВОСТОЯТЬ ИНТЕРНЕТ-УГРОЗАМ

В данном разделе было задано три стандартных для таких исследований ситуационных вопроса, респонденты показали следующие модели поведения:

4.1. В случае получения от незнакомого человека оскорбительного сообщения в социальной сети респонденты поступят следующим образом:

- 61,8 % – добавляют его в «черный список» (наиболее адекватная модель поведения для данной ситуации);
- 58,7 % – проигнорируют;
- 18,9 % – напишут жалобу администрации социальной сети.

Ряд респондентов проявили неадекватные данному инциденту действия, так:

- 1,3 % респондентов ответят ему тем же, то есть часть работников готова вступить в конфликт в социальной сети;
- 2,4 % – отключат компьютер, данное действие не способствует решению ситуации;
- 3,1 % – удалят свой аккаунт из социальной сети, неадекватное угрозе решение;
- 5,8 % респондентов затрудняются ответить.

4.2. В случае, если на рабочий почтовый ящик придет письмо от администрации почтового сервиса с просьбой выслать пароли для восстановления доступа, респонденты поступят следующим образом;

Наиболее адекватная модель поведения для данной ситуации:

- 74 % – удалят письмо и поменяют пароль.

Неадекватная модель поведения для данной ситуации, свидетельствующая о незнании правил информационной безопасности:

- 4,6 % – перезагрузят компьютер;
- 10,5 % – выйдут из почты и зайдут еще раз;
- 9,4 % – затрудняются ответить;
- 1,4 % – ответят на письмо и вышлют пароль.

4.3. В случае, если на личную электронную почту придёт сообщение о выигрыше недели проживания в пятизвёздочном отеле на курорте, и для получения приза просят немедленно оплатить билеты, а для этого нужно прислать данные банковской карты, то респонденты поступят следующим образом:

- 0,2 % респондентов отправят данные карты, без пин-кода; *(неадекватные данному инциденту действия)*
- 0,1 % респондентов отправят все данные и пин-код; *(неадекватные данному инциденту действия)*
- 4,4 % - напишут в компанию, от которой пришло письмо;
- 4 % - напишу вопрос на адрес отеля;
- 3,1 % – затрудняются ответить;
- 92,3 % – удалят сообщение как спам.

На вопрос, связанный с проведением собраний, классных часов и уроков по Медиабезопасности для родителей и школьников по современным угрозам в сети Интернет, респонденты ответили следующим образом.

- 38,9 % респондентов считают, что обладают компетенциями для проведения данных уроков;
- 22,8 % респондентов считают, что не обладают компетенциями для проведения данных уроков;
- 38,2 % респондентов хотели бы пройти дополнительное обучение.

Для проведения уроков по медиабезопасности респонденты нуждаются в помощи:

- 41,7 % – в повышении осведомленности по вопросам медиабезопасности;
- 37,2 % – в повышении квалификации в сфере информационной безопасности;
- 25,1 % – в разработке презентационного материала;
- 26,1 % – в разработке методических пособий;
- 47,5 % – в получении информации об актуальных Интернет-угрозах;
- 12,7 % – не нуждаются в помощи.

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Условия и факторы, способствующие нарушению правил информационной безопасности и совершению по отношению к работникам образовательных организаций противоправных действий в сети Интернет:

1. Отсутствие знаний о правилах информационной безопасности.

- 34,2 % респондентов не повышают компетентность в сфере информационной безопасности, то есть не изучают актуальные Интернет-угрозы и способы противодействия;
- 51,1 %, более половины респондентов, не знают какое ведомство, ведет реестр запрещенных сайтов РФ.

2. Отсутствие навыков и умений в сфере информационных технологий и информационной безопасности.

- 42,9 % респондентов не умеют определять, какие стоит скачивать файлы;
- 65,1 % респондентов не умеют обеспечивать защиту своей информации, хранящейся в Интернете;
- 48,9 % респондентов не умеют использовать безопасный поиск в поисковых системах;
- 70,6 % респондентов при сбое подключения к интернету не умеют определять причины технических проблем;
- 43,5 % респондентов не умеют очищать компьютер от вирусов, попавших в него через Интернет;
- 46,4 % респондентов не умеют добавлять пользователей в «черные списки» в социальных сетях;
- 57,2 % респондентов не умеют менять настройки конфиденциальности в социальных сетях и в сервисах для общения, чтобы их информация была доступна только определенным людям;
- 100 % респондентов не умеют определять степень конфиденциальности и безопасности передачи личных данных при пользовании услугами через Интернет;
- 83 % респондентов не знают, что делать при столкновении с мошенничеством в Интернете.

3. Отсутствие знаний и навыков использования паролей.

- 50,6 % респондентов никогда не меняли пароли;
- 2,2 % респондентов не знают свои пароли, и пароли им меняют люди из ближайшего окружения;
- 14,2 % респондентов имеют простые пароли;
- 23,1 % респондентом имеют один и тот же пароль ко всем Интернет ресурсам.

4. 8,29 % респондентов подвергались «травле» в Интернете.

РЕКОМЕНДАЦИИ

Для обеспечения защищенности информационных ресурсов пользователей в сети Интернет, а так же с целью повышения общего уровня культуры в сфере информационной безопасности рекомендуется:

- Постоянно поддерживать осведомленность об актуальных Интернет – угрозах, способах противодействия им. Повышать свои компетенции в сфере информационной безопасности на специализированных семинарах, курсах повышения квалификации и конференциях.
- Доводить на общих собраниях педагогического коллектива обзоры инцидентов в сфере информационной безопасности, информацию о новых видах Интернет-мошенничества, атак, схемах и т.д.
- Проводить круглые столы с привлечением специалистов-практиков в сфере информационной безопасности совместно с педагогическим составом, родителями и учащимися о мерах по защите информационных ресурсов и правилах безопасного поведения в Интернете.
- Всегда защищать свои личные информационные ресурсы, устанавливая лицензионные программы для обеспечения безопасности, включая брандмауэры и программы для обнаружения вторжений, и регулярно обновлять их.
- Не передавать информацию через незащищенные каналы, беспроводные сети в общественных местах.
- Использовать надежные пароли к своим информационным ресурсам, периодически их изменяя.
- Не открывать, не скачивать, не запускать, не копировать программы, сообщения и любой другой контент, который не проверен на наличие вирусов, признаков фишинга и т.д.
- Защищать свою частную жизнь в Интернете. Не указывать пароли, телефоны, адреса, дату рождения и другую личную информацию в социальных сетях.
- Не размещать и не указывать информацию в сети, которая может скомпрометировать вашу репутацию или репутацию образовательной организации.
- Всегда создавать резервные копии важной для вас информации.



**Институт мониторинга и оценки
информационной безопасности**

Телефон: 8 (495) 268-13-42

E-mail: info@imoib.ru

Адрес: 119454, г. Москва, пр. Вернадского 14А

**ЧОУ ДПО Учебный центр
«АСТА-информ»**

Телефон: 8 (499) 130-06-34

8 (351) 222-45-00; 247-82-00

Факс: 8 (351) 232-85-36

E-mail: uc@asta74.ru

Адрес: 454048, г. Челябинск, ул. Яблочкина, д. 9, оф. 10.



Телефон: 8 (351) 222-45-00; 247-82-00; 232-84-29

Факс: 8 (351) 232-85-36

E-mail: info@asta74.ru,

Адрес: 454048 г. Челябинск, ул. Яблочкина 9, оф. 10.