МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, ИННОВАЦИЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН

КОМИТЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕР-БЕЗОПАСНОСТИ

РЕКОМЕНДАЦИИ

В целях определения уровня осведомленности населения об угрозах информационной безопасности (кибербезопасности) по заказу Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан с октября по ноябрь 2022 года было проведено социологическое исследование среди населения.

В процессе исследования было охвачено:

среди населения в возрасте 18 лет и старше.

Анализируя результаты опроса, можно отметить, что на сегодняшний день угроза информационной безопасности является актуальной проблемой в Республике Казахстан.

Показатели осведомленности населения об угрозах информационной безопасности (кибербезопасности)

НА ЗАЩИТЕ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Вопросам развития сферы информационной безопасности в Казахстане уделяется значительное внимание. И результат работы, проводимой совместно государственными органами, неправительственными организациями и бизнесом – это тенденция последних лет, когда наша страна стремительно улучшает свои позиции в глобальном индексе кибербезопасности. Сейчас Казахстан занимает в нём 31 место. Обогнав в этом рейтинге такие страны, как КНР, Дания, Хорватия, Словакия, Израиль и Швейцария.

За прошедшие годы в стране были выработаны базовые концептуальные подходы к развитию сферы кибербезопасности страны. Утверждена концепция кибербезопасности ("Киберщит Казахстана") до 2022 года.

По поручению Главы государства Республики Казахстан разработана новая Концепция развития цифровой экосистемы на 2023 – 2027 годы («Киберщит - 2»).

В целях развития сферы информационной безопасности («кибербезопасности») вступили в действие целый ряд законодательных актов и отраслевых ведомственных актов. Помимо этого, созданы испытательные лаборатории в сфере информационной безопасности, запущен Национальный координационный центр информационной безопасности, создан государственный оперативный центр информационный безопасности, отраслевой оперативный центр информационной безопасности, имеются 3 службы реагирования на компьютерные инциденты, созданы 35 оперативных центров информационной безопасности, имеются 3 профильных общественных организаций, задействованы в порядке 50 отечественных компаний в сфере информационной безопасности, увеличено количество образовательных грантов по специальности информационной безопасности и т.д.

ПОЧЕМУ ВАЖНО ПОДДЕРЖИВАТЬ КИБЕРБЕЗОПАСНОСТЬ?

Подготовлено на основании социологического исследования

Обеспечение информационной безопасности и защита персональных данных является важной составляющей частью работы уполномоченного органа в лице Комитета по информационной безопасности.

«ОСВЕДОМЛЕННОСТЬ НАСЕЛЕНИЯ ОБ УГРОЗАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КИБЕРБЕЗОПАСНОСТИ)»

“В Глобальном индексе кибербезопасности (GCI) Казахстан стремительно улучшает свою позицию. Например, в 2019 году Казахстан поднялся сразу на *42 пункта — до 40- го места.* *29 июня 2021 года в последнем отчете Казахстан разместился на 31 месте, значительно превысив ожидаемый результат, поднявшись на 9 пунктов выше по сравнению с прошлогодним рейтингом.* Это *результат совместной работы государственных органов*, неправительственных организаций и бизнеса.”

НЕМНОГО ВАЖНОЙ ИНФОРМАЦИИ

Информационная безопасность является неотъемлемой частью нашей
Под информационной безопасностью подразумевают, как правило, собл
трех важных принципов:

Что это такое?

Конфиденциальность

Доступность

Целостность

- *Доступ к информации должен быть только у того, кто имеет на это право.*
- *Информация должна быть доступна в любой момент, когда она нужна.*
- *Информация должна быть достоверной.*

Нарушение одного из принципов может привести к нарушению других.

УГРОЗЫ БЕЗОПАСНОСТИ ДАННЫХ

Информационная безопасность в сфере информатизации (Кибербезопасность) **- состояние защищенности электронных информационных ресурсов, информационных систем и информационно - коммуникационной инфраструктуры от внешних и внутренних угроз.**

РЕЗУЛЬТАТЫ СОЦИОЛОГИЧЕСКОГО ОПРОСА ПОКАЗЫВАЮТ:

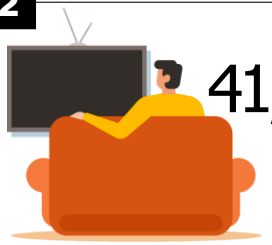
1

51,5%

Получают информацию посредством интернета

2

41,6%



Посредством телевизора

3

65,4%

Посредством мобильных приложений

Большинство респондентов:

КАКИМ ВИДАМ КИБЕРАТАК ВЫ ПОДВЕРГАЛИСЬ ЗА ПОСЛЕДНИЙ ГОД ?

Согласно опросу, за последний год население страны подвергалось следующим видам кибератак:

	2020	2021	2022
Атака компьютерных вирусов	32.1%	16.5%	51.7%
Вредоносный спам	13.4%	23.0%	34,5%
Взлом аккаунтов в социальных сетях	3.9%	14.5%	28.4%

По мнению респондентов основной мерой при подозрении на нарушение кибербезопасности является:

-обращение к IT-специалисту — 27,4%

-обращение в уполномоченный орган в сфере обеспечения информационной безопасности — 19,2%

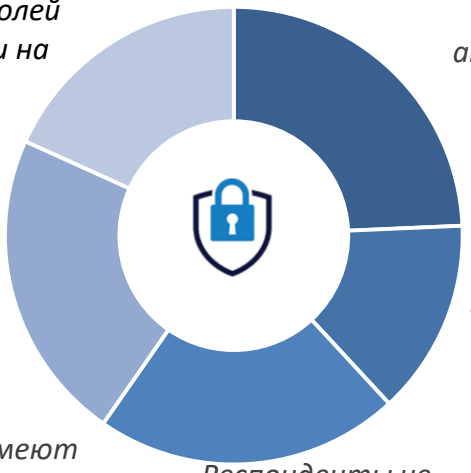
-обращение правоохранительные органы — 32,1%

-не обращение никуда — 10,1%

При любых нестандартных или при подозрении на нарушения информационной безопасности:
-незамедлительно обратитесь к ответственным специалистам;
-также можно обратиться в службу реагирования на компьютерные инциденты по номеру телефона:
1400 или
+7 (7172) 55-99-97,
эл.почта:
info@ kz-cert.kz

КАКИЕ МЕРЫ БЕЗОПАСНОСТИ ВЫ ИСПОЛЬЗУЕТЕ ПРИ РАБОТЕ В ИНТЕРНЕТЕ?

Результаты социологического опроса показывают:



Респонденты не сохраняют паролей при регисрации на сайтах 18%

Респонденты используют антивирусные программы 24%

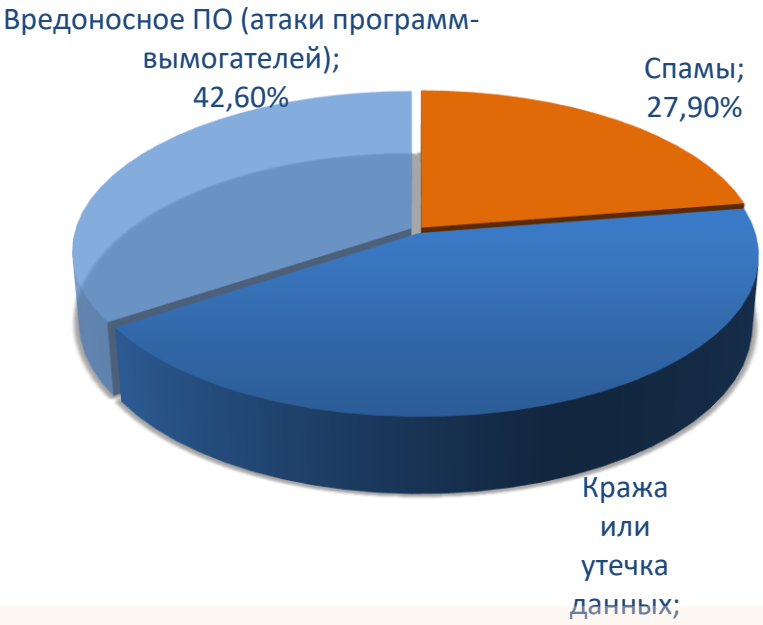
Респонденты не оставляют информацию о личных данных 14%

Респонденты не посещают незнакомые сайты 22%

Респонденты имеют сложные комбинации паролей 22%

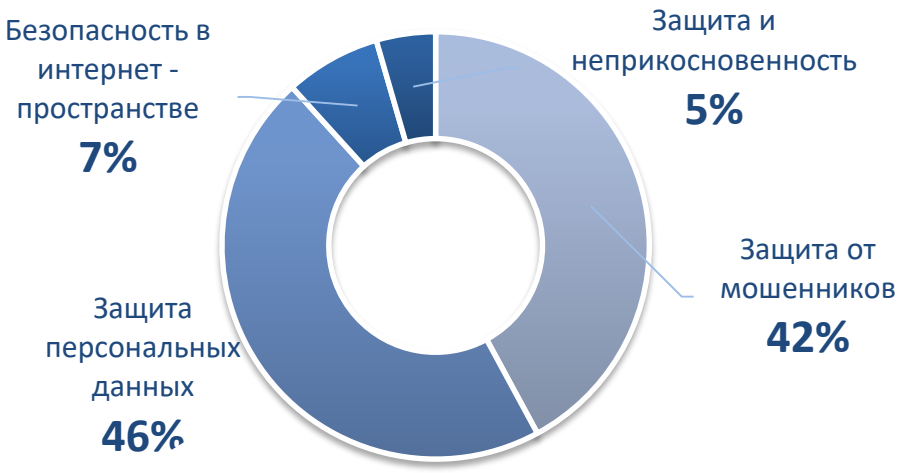
ЗНАЕТЕ ЛИ ВЫ ОБ ИМЕЮЩИХСЯ ВИДАХ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ?

ВИДЫ КИБЕРУГРОЗ:



Результаты социологического опроса показывают:

КАК ВЫ СЧИТАЕТЕ, ОТ ЧЕГО НУЖНО ОБЕСПЕЧИВАТЬ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ:

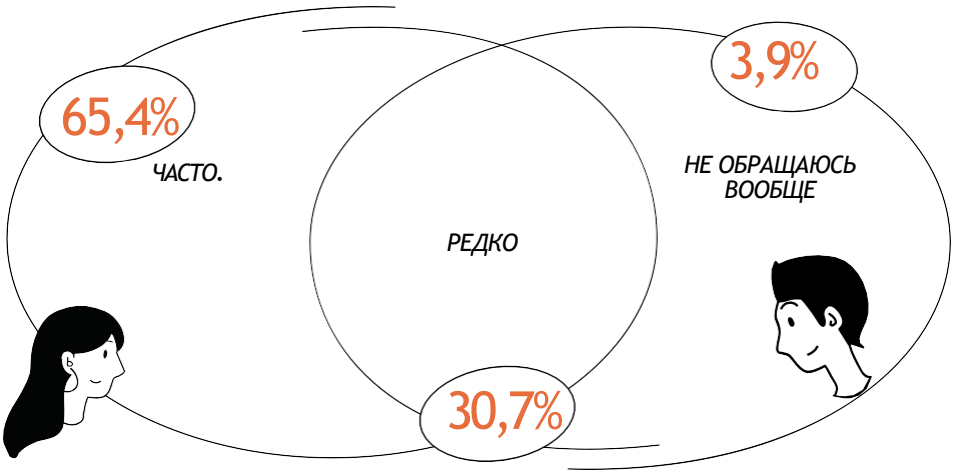


Информационная безопасность является одним из основных задач в обеспечении защиты данных, в том числе персональных, и её повышение требует, по мнению респондентов, принятия мер.

ПРОФИЛАКТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«КАК ЧАСТО ВЫ ИСПОЛЬЗУЕТЕ СОЦИАЛЬНЫЕ СЕТИ И МЕССЕНДЖЕРЫ?»

Результаты социального опроса показывают:



ПРОВЕРЯЮТ ЛИ РЕСПОНДЕНТЫ ИНФОРМАЦИЮ О САЙТАХ, НА КОТОРЫХ РЕГИСТРИРУЕТЕСЬ?

63,1% - Да, регулярно

Иногда, когда ресурс вызывает сомнения - 22,9%

14,0% - Нет

РЕКОМЕНДАЦИИ

Профилактика информационной безопасности (рекомендации)

Регулярно устанавливайте обновления для вашего программного обеспечения - операционных систем, программ приложений, антивирусных и прочих программ.

Включайте функцию автоматического обновления программного обеспечения, когда таковое доступно.

Удаляйте программное обеспечение, которое вы не используете или когда, не получаете обновления разработчика.

Избегайте установки нелицензионного программного обеспечения, либо программного обеспечения из непроверенных источников.

Регулярно создавайте копию важных для Вас данных на других устройствах.

Каким образом вредоносные программы проникают на компьютер пользователя?

Методы распространения:

Фишинг

Один из видов интернет – мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логины, пароли, данные банковских карт и т.п.) через поддельные интернет-ресурсы, внешне неотличимые от настоящих.

Социальная инженерия

это способ получения конфиденциальной информации с помощью психологического воздействия на человека. Основной целью социальной инженерии является получение выгоды через доступ к паролям, банковским данным и другим защищенным системам.

Троянский конь

разновидность социальной инженерии, когда в письме присутствует опасное вложение, из-за которого Ваш компьютер будет заражен.

Рекомендации

Вредоносные программы, чаще всего, проникают на компьютер:

- ✓ по электронной почте;
- ✓ через носители информации (флеш-накопители);
- ✓ при скачивании файлов с неизвестных сайтов.

Что делать?

Вредоносные программы зачастую распространяются в приложении с другими файлами, так что не открывайте вложения электронной почты, отправленные с неизвестных Вам ресурсов.

- ✓ Никогда не отключайте встроенный брандмауэр операционной системы.
- ✓ Используйте антивирусное ПО для защиты Вашей системы от возможных онлайн- угроз. Установите антивирусные и антишпионские программы из надежных источников.
- ✓ Осторожно используйте флеш-накопители. Минимизируйте возможность заражения компьютера вредоносным ПО: не подключайте неизвестные флеш-накопители (или USB- накопители) в своему компьютеру.
- ✓ Не принимайте файлы от незнакомых Вам пользователей, и особенно обращайте внимание на получаемые файлы с расширением EXE, COM, CMD.

Правила информационной безопасности в интернете (Рекомендации)

1. Используй безопасные и разные пароли везде. Отдавай предпочтение двухфакторной аутентификации и сверке по отпечатку пальца там, где наибольшие риски.

2. Не давай незнакомым людям позвонить. Они могут сделать что угодно, а не только сбежать с телефоном.

3. Меньше рассказывай о себе любимом в интернете. Эту информацию могут использовать совсем не в хороших и корыстных целях злоумышленники.

4. Не покупайся на слова «бесплатно», «free», «скидка», «скачать бесплатно и без регистрации».

5. Когда заходишь в социальные сети или на почту с чужого компьютера, то не забудь выйти.
Но лучше избегай это делать. Это повышенный риск.

6. Не пересылай конфиденциальную информацию через почту или социальные сети.
Сразу удаляй сканы паспорта и документов

7. Всегда читай правила при оплате в интернете. Самое важное могут написать самыми маленькими буквами.

8. Выключай Wi -Fi и блютуз, когда им не пользуешься. Это повысит информационную безопасность.

9. Анализируй какие мобильные приложения получают доступ к твоей информации. Зачем им знать контакты, получать фото, определять местоположение, давать доступ к камере или микрофону? Думай прежде.

10. Все безопасные сайты сейчас начинаются с «https://», а не «http://».
Особенно при оплате смотри на это. Также такие сайты помечены закрытым замочком в адресной строке.

РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ

1 ПАРОЛЬНАЯ ПОЛИТИКА

- Запрещается сохранять пароли в электронном виде на рабочем столе.
- Допускается раскрытие значений пароля в случае производственной необходимости.
- Пароли должны быть не меньше 8 символов и должны обновляться ежеквартально.

2 ПОЧТА

- Запрещается открывать от незнакомых лиц электронные письма и подозрительные вложения.
- На любой подозрительный запрос по электронной почте необходимо использовать альтернативный канал связи (к примеру, телефон), чтобы подтвердить запрос у адресата.
- Необходимо всегда проверять правильность написания адреса отправителя и получателя.

3 АНТИВИРУСНОЕ ПРОГРАМНОЕ ОБЕСПЕЧЕНИЕ

- Необходимо использовать ЛИЦЕНЗИОННОЕ антивирусное программное обеспечение.
- Обязательно проверять на вирусы любой носитель при подключении к Вашему компьютеру.
- Проверять все файлы из входящей электронной почты на вирусы путем настройки автоматической проверки.

4 СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- Запрещается сообщать третьим лицам IP-адреса и сочетание логина и пароля.
- Запрещается устанавливать самостоятельно программное обеспечение.

ДОПОЛНИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ГОСУДАРСТВЕННЫХ СЛУЖАЩИХ

5 ИНТЕРНЕТ И СОЦИАЛЬНЫЕ СЕТИ

- Не допускается переходить по ссылкам от неизвестного отправителя.
- Запрещается посещать вебсайты, содержащие материалы террористической, экстремисткой, антиконституционной и иной деструктивной направленности.
- Запрещается принимать соглашения при посещении сайтов, смысла которых Вы не понимаете.
- Запрещается использовать пароли доступа в локальную сеть в других программах и на сайтах.
- Во избежание угроз, связанных с использованием cookies (файлы небольшого объема) рекомендуется периодически проводить анализ сохраненных cookies.

- Запрещается подключение внутренних сетей ГО к интернету.
- Подключение к сети Интернет необходимо проводить только через Единый шлюз доступа к Интернету.
- При работе с ресурсами сети Интернет и электронной почтой запрещается разглашение государственной, служебной и коммерческой информации, ставшей известной сотруднику по служебной необходимости либо иным путем.
- Служащие ГО, МИО при осуществлении служебной переписки в электронной форме при исполнении ими служебных обязанностей используют только ведомственную электронную почту.
- Запрещается оставлять включенными без присмотра компьютеры и Интернет-сети в открытом виде. В случае оставления рабочего места в обязательном порядке необходимо блокировать компьютер (- комбинация клавиш Windows+L).
- Запрещается подключение к ЕТС ГО, локальной сети ГО посредством беспроводных сетей, беспроводного доступа, модемов, радиомодемов, модемов сетей операторов сотовой связи и других беспроводных сетевых устройств.

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ:

При подписании согласия обратите внимание на:

- перечень персональных данных, которые собирает оператор;
- цели сбора и обработки персональных данных;
- срок или период, в течении которого действует согласие;
- возможность передачи третьим лицам;
- возможность трансграничной передачи данных;
- возможность распространения персональных данных в общественных источниках.

При предоставлении персональных данных куда либо, обязательным требованием является наличие согласия физического лица либо основание, предусмотренное Законом

Без Вашего согласия, персональные данные не могут быть переданы оператором другим лицам и организациям.

Также в целях защиты личных данных от незаконного распространения, настоятельно рекомендуется ***ознакомиться с политикой соблюдения конфиденциальности персональных данных организации***, а также обращать пристальное внимание на условия их обработки.

ВАШИ ПРАВА ЗАЩИЩЕНЫ ЗАКОНОМ

Согласно *пункту 2 статьи 20 Закона Республики Казахстан "О персональных данных и их защите":*

сбор и обработка персональных данных осуществляются только в случаях обеспечения их защиты.

персональные данные, собственник и (или) оператор базы, содержащей персональные данные, а также третьи лица,

обязаны принимать меры по их защите в соответствии с настоящим Законом,

законодательством Республики Казахстан о персональных данных и их защите и действующими на территории Республики Казахстан стандартами. Данная обязанность возникает с момента получения электронных информационных ресурсов, содержащих персональные данные, и до их уничтожения либо обезличивания.

Кроме того,

В соответствии со статьей 56 Закона РК "Об информатизации", собственники и владельцы информационных систем, получившие электронные информационные ресурсы, содержащие

ЧТО ДЕЛАТЬ?

При обнаружении фактов незаконного сбора и утечки личных данных граждане могут обратиться в *Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности РК* для принятия мер по пресечению нарушений.

Это можно сделать, написав на электронный адрес kib@mdai.gov.kz, либо через портал «Электронного правительства» (раздел «Электронные обращения»), также можно написать на личный блог Председателя (https://dialog.egov.kz/blogs/3932160/welcome)

ОБРАЩЕНИЯ ДОЛЖНЫ СОДЕРЖАТЬ:

01 ФИО, контакты заявителя;

02 Описание ситуации, при которой допущено нарушение;

03 Период и сроки совершения нарушения;

04 Достоверные материалы, подтверждающие нарушение;

05 Наименование организации, допустившей правонарушение.

Если Вы обнаружили, что кто-либо осуществляет сбор и обработку ваших персональных данных без вашего согласия, Вы вправе обратиться к данному лицу/ организации с требованием *уничтожить незаконно собранные данные*. Кроме того, Вы также вправе отозвать данное ранее согласие на сбор и обработку ваших персональных данных. В случае бездействия или отказа оператора *уничтожить данные*, Вы можете пожаловаться в уполномоченный орган по защите персональных данных - КОМИТЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МИНИСТЕРСТВА ЦИФРОВОГО РАЗВИТИЯ, ИННОВАЦИЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН.

Обращения можно подавать любым удобным и доступным способом.

ЧТО НЕОБХОДИМО ЗНАТЬ ПРО ЭЛЕКТРОННУЮ ЦИФРОВУЮ ПОДПИСЬ ?

Электронная цифровая подпись (далее - ЭЦП) равнозначна собственноручной подписи подписывающего лица и влечет одинаковые юридические последствия

В целях предотвращения нарушений в сфере ЭЦП необходимо придерживаться следующих рекомендаций:

1)исключить передачу ЭЦП третьим лицам. В организациях нужно сотрудников, ответственных за подписание документов, наделить полномочиями и выдать им собственные электронные подписи. Для этого необходимо правовым актом руководителя организации передать право подписи соответствующему лицу и выпустить на его имя ЭЦП (передача ЭЦП руководителя, выпущенного на его имя, по доверенности сотруднику является незаконной);

2)отслеживать факты увольнения сотрудников, имевших ЭЦП от организации, и отзывать их ЭЦП;

3) в случае утери перевыпустить ЭЦП, немедленно отозвав предыдущую ЭЦП, а также сменить пароль со стандартного на более сложный.

При обнаружении фактов незаконной передачи или неправомерного пользования ЭЦП необходимо в кратчайшие сроки информировать Комитет по информационной безопасности в соответствии с действующим законодательством Республики Казахстан.

*пункт 1 статьи 10 Закона Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи»).

Правила информационной безопасности ДЕТЕЙ И ПОДРОСТКОВ В СЕТИ ИНТЕРНЕТ

В продолжении диалога с участниками исследования также был обсужден вопрос, связанный с актуальной на сегодняшний день проблемой защиты детей от нежелательной информации в интернете. ***По мнению респондентов основной мерой защиты ребенка от нежелательной информации в Интернете является:***

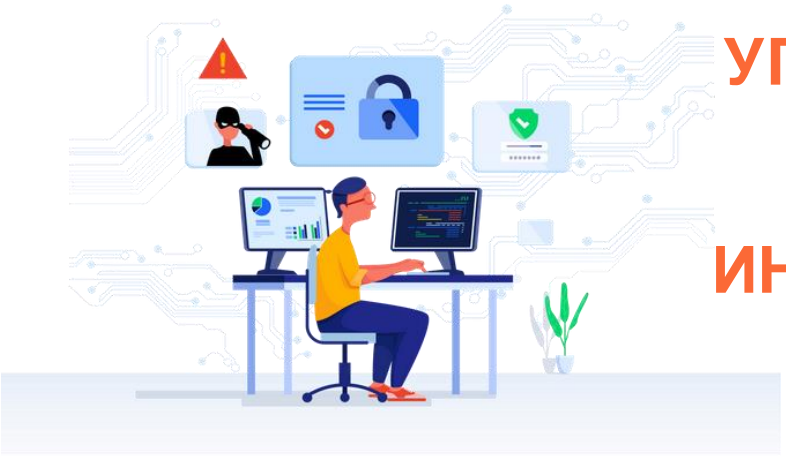
Рекомендации для родителей:

- ✓ Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
- ✓ Компьютер с подключением к сети Интернет должен находиться в общей комнате.
- ✓ Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
- ✓ Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- ✓ Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

Постоянно контролируйте использование Интернета Вашим ребенком!
Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

КАК ОГРАНИЧИТЬ ДОСТУП ДЕТЕЙ И ПОДРОСТКОВ К ИНТЕРНЕТУ?

- ✓ Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
- ✓ Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
- ✓ Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах.
- ✓ Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
- ✓
- ✓ Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
- ✓ Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.



УПОЛНОМОЧЕННЫЙ ОРГАН В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПОЛНОМОЧИЯ КОМИТЕТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В рамках Указа Президента Республики Казахстан от 6 октября 2016 года №350 создан Комитет по информационной безопасности.

01 **Разработка**
Разработка мер в сфере обеспечения информационной безопасности (за исключением госсекретов).

02 **Контроль**
Государственный контроль и профилактика соблюдения Единых требований в области информационно - коммуникационных технологий и обеспечения информационной безопасности

03 **Формирование**
Формирование перечня и мониторинг критически важных информационно-коммуникационной инфраструктуры.

04 **Управление**
Управление и распределение доменных имен в пространстве казахстанского сегмента Интернета.

05 **Выдача**
Выдача акта по результатам испытаний на соответствие требованиям информационной безопасности.

06 **Координация**
Межведомственная координация Концепции кибербезопасности «Киберщит Казахстана» до 2022 года.

07 **Организация**
Организация исполнения Национального плана реагирования на инциденты информационной безопасности.

08 **Рассмотрение**
Рассмотрение и привлечение к ответственности за нарушения в сфере персональных данных.

09 **Осуществление**
Осуществление аккредитации удостоверяющих центров.

10 **Осведомление**
Повышение осведомленности населения об угрозах информационной безопасности (кибербезопасности)

11 **Участие**
Участие в реализации образовательных программ.

12 **Содействие**
Содействие в формировании профессиональных стандартов.

13 **Поддержка**
Поддержка научных исследований в сфере информационной безопасности.

14 **Взаимодействие**
Взаимодействие с международными организациями, национальными регуляторами и центрами кибербезопасности.

Куда обращаться при компьютерных инцидентах?

Служба реагирования

1400

или 8 (7172) 55-99-97
Бесплатная Горячая Линия
эл.почта: info@kz-cert.kz

В компетенцию службы входит обработка следующих компьютерных инцидентов с целью их выявления и нейтрализации:

- атаки на узлы сетевой инфраструктуры и серверные ресурсы, с целью нарушения их работоспособности (DoS (Denial of Service) и DDoS) и конфиденциальности информации;
- несанкционированный доступ к информационным ресурсам;
- распространение вредоносного программного обеспечения, незатребованной корреспонденции (спам);
- сканирование национальных информационных сетей и хостов;
- подбор и захват паролей и другой аутентификационной информации;
- взлом систем защиты информационных сетей, в том числе с внедрением вредоносных программ (сниффер, rootkit, keylogger и т.д.).

KZ CERT

KZ-CERT Служба реагирования на компьютерные инциденты

Краткий анализ исследования

по результатам социологического исследования по вопросам информационной безопасности и защиты персональных данных

По заказу Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан проведено социологическое исследование по вопросам информационной безопасности (кибербезопасности) и защиты персональных данных. Результат проведенного опроса определил общий показатель осведомленности населения об имеющихся угрозах информационной безопасности (кибербезопасности) и защиты персональных данных на уровне **77,4%.**

В целом, полученные результаты социологического исследования свидетельствуют о следующем состоянии информационной безопасности (кибербезопасности):

- уровень владения населения компьютером и другими цифровыми устройствами составил (73,8%);

- для 51,5% населения основным источником получения информации является интернет. При этом, для непосредственного выхода в интернет использования мобильных устройств, смартфонов и планшетов составило (70,2%);

- 45,1 % населения не владеют основными методами защиты детей от нежелательной информации в интернете и т.д.

В этой связи, с учетом проведенного социологического опроса, исследовательской группой выработаны соответствующие рекомендации и предложения для дальнейшего обеспечения информационной безопасности граждан и защиты их персональных данных в информационном пространстве.

По заказу РГУ "Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан"

Республика Казахстан 010000, г. Астана, пр. Мәңгілік ел 55/14, блок С 2.4

тел.: +7 (7172) 64-93-96, +7 (7172) 64-93-99

e-mail: **kib@mdai.gov.kz**

https://www.gov.kz/memleket/entities/infsecurity?lang=ru

РЕКОМЕНДАЦИИ

г. Астана 2022