Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан

Комитет по информационной безопасности

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Рекомендации

ЗАЩИТА ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Одним из важнейших вопросов глобальной цифровизации становится обеспечение информационной безопасности.

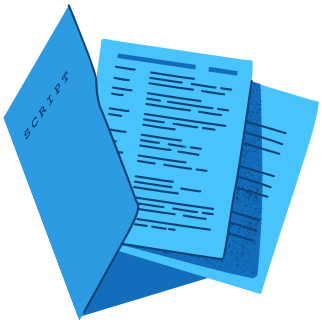
В Глобальном индексе кибербезопасности (ГИК) в Международном союзе электросвязи Организации Объединенных Нации (МСЭ ООН), Казахстан стремительно улучшил свою позицию. Повышение уровня достижения индикаторов в ГИК-е позволило Казахстану достичь определенных результатов по проведенному анализу экспертами МСЭ ООН, где Республика Казахстан поднялась на 9 позиций и в настоящее время занимает 31 место (ранее 40-е) в ГИК-е.

По поручению Главы государства принята Концепция цифровой трансформации, развития отрасли ИКТ и кибербезопасности на 2023-2029 годы, утвержденная постановлением Правительства Республики Казахстан от 28 марта 2023 года №269 с отдельными целями и задачами, а также отдельным направлением по развитию кибербезопасности.

В данной Концепции регламентированы дополнительные меры, направленные на укрепление кибербезопасности страны, в частности предусмотрены мероприятия по технической защите, совершенствования радиоконтроля, защиты персональных данных и повышения осведомленности населения.

11 декабря 2023 года Главой государства подписан Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам информационной безопасности, информатизации и цифровых активов».

Данный Закон направлен на усиление защиты персональных данных и определение новых механизмов взаимодействия при обеспечении информационной безопаности объектов информатизации, в том числе государственных органов.



ЭКОСИСТЕМА КИБЕРБЕЗОПАСНОСТИ

Основными элементами экосистемы кибербезопасности являются: человеческий капитал, развитие рынка кибербезопасности, техническая защита.

В целях развития человеческого капитала в стране имеются 8 высших учебных заведений и 25 среднеспециальных учебных заведений, выпускающих специалистов информационной безопасности.

На 2022-2023 учебные годы увеличено до 3009 образовательных грантов по специальности информационная безопасность (по сравнению с 2021-2022 годами было выделено до 2600).

В 2023-2024 годы выделено 3723 образовательных грантов по специальности информационная безопасность.

85 специалистов получили образование по специальностям «Информационная (кибер) безопасность и криптография», «Информационная безопасность» в ведущих зарубежных высших учебных заведениях по программе «Болашак».

ЭКОСИСТЕМА КИБЕРБЕЗОПАСНОСТИ

В целях развития рынка качественных профессиональных услуг в области информационной безопасности имеются 3 профильных общественных организаций, задействованы в порядке 50 компаний в сфере информационной безопасности. Определены 514 стратегических объектов, обладающих критической инфраструктурой. Созданы 41 частных оперативных центров информационной безопасности, имеются 3 службы реагирования на компьютерные инциденты (FIRST) и 9 частных испытательных лабораторий.

В целях технической защиты в 2018 году создан и начал свою работу Национальный координационный центр информационной безопасности. Дополнительно, в будущем будет проработан вопрос в части защищенной резервной инфраструктуры для случаев дезорганизации его работ в период чрезвычайных ситуаций в мирное время, в период военного положения и военного времени.

В 2022 году создан Государственный оперативный центр информационной безопасности (GSOC), также был создан отраслевой оперативный центр информационной безопасности (SOC).

В 2022 году запущен Сервис контроля доступа к персональным данным (сервис КДП). Данный сервис предназначен для получения отзыва согласия гражданина на доступ к его персональным данным. Также сервис защищает персональные данные от несанкционированного доступа или распространения.

В 2023 году к сервису КДП уже подключены 113 информационных систем.

Уровень осведомленности населения

Так, в целях определения уровня осведомленности населения об угрозах информационной безопасности (кибербезопасности) и защиты персональных данных по заказу Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан в сентябре-ноябре 2023 года было проведено социологическое исследование по осведомленности населения об угрозах информационной безопасности (кибербезопасности) и защиты персональных данных (кибербезопасности).

В процессе социологического исследования было охвачено:

3 города республиканского значения (Астана, Алматы, Шымкент)

17 районов и сел областей по Республике

11371 участвовавших респондентов

Участники: граждане РК от 18 лет и старше;

Количество вопросов анкетных блоков:

- социально - демографический блок - 10;
- основной блок - 30;
- дополнительный блок - 20;

Уровень осведомленности населения

Всего в опросе социологического исследования, проведенного по Республике в течение 3 месяцев, приняли участие 11371 респондентов. Анализируя результаты опроса, можно отметить, что на сегодняшний день существует рост уровня осведомленности населения Казахстана по информационной безопасности.

Показатели осведомленности населения об угрозах информационной безопасности (кибербезопасности) и защиты персональных данных:

Результаты социологического исследования проведенного в 2023 году, показывают что большинство респондентов:

- **получают знания о защите личной информации при использовании социальных сетей – 90,52 %;**

- **осведомлены при использовании своей «электронной цифровой подписи» – 85,06 %;**

- **знают о потенциальных рисках детей при использовании интернета – 76,65 %;**

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.

ВАЖНО ЗНАТЬ:

Информационная безопасность является неоторванный частью нашей жизни. Под информационной безопасностью подразумевают, как правило, три важных принципа:

- **Конфиденциальность** — доступ к информации должен быть только, у того, кто имеет на это право.
- **Доступность** — информация должна быть доступна в любой момент, когда она нужна.
- **Целостность** — информация должна быть достоверной.

Нарушение одного из принципов может привести к нарушению других.

Каким образом вредоносные программы проникают в компьютер пользователя?

Типы угроз кибербезопасности:

- **Фишинг** - это распространенная форма онлайн-мошенничества, основанная на невнимательности онлайн-пользователей.
- **Взлом сайта** - получение доступа к внутренним данным или к админ-панели веб-ресурса незаконным путем.
- **Социальная инженерия** - психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации.
- **DDos-атака** - это перегрузка информационной системы избыточным числом запросов, блокирующих обработку обращений.
- **Троянский конь** - вредоносное программное обеспечение, которое маскирует свое истинное назначение. При этом, в отличие от вируса, троян не способен самостоятельно дублировать или заражать файлы.
- **Программа-вымогатель** - блокирует компьютер, а затем требует выкуп за то, чтобы разблокировать его.

Методы распространения:

ссылки на вредоносные сайты в электронной почте

сообщения в социальных сетях

убеждают загрузить зараженный файл

посещение зараженного сайта

использование зараженного USB-накопителя на компьютере

собирают пароли с веб-сайтов и других компьютеров, которые они взломали

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ (РЕКОМЕНДАЦИИ)

РЕКОМЕНДАЦИИ:

Внимательно посмотрите на посещаемые сайты и ресурсы, проверьте доменные имена и внимательно прочитайте, с чем вы соглашаетесь, прежде чем нажимать «да, я согласен».

Прежде чем открывать письмо, которое вы получили, напишите на нем несколько слов в ответ, потому что, если отправитель верен, сторона, отправившая письмо, обязательно ответит.

Настройте сложные пароли и/или двухфакторную аутентификацию для доступа к личным данным.

Откройте отдельную виртуальную карту для покупок в интернете и вставьте только сумму, рассчитанную на покупку внутри.

За последний год подвергались ли вы кибератакам?

Согласно опросу, за последний год население Казахстана подверглось нижеуказанным видам кибератак:

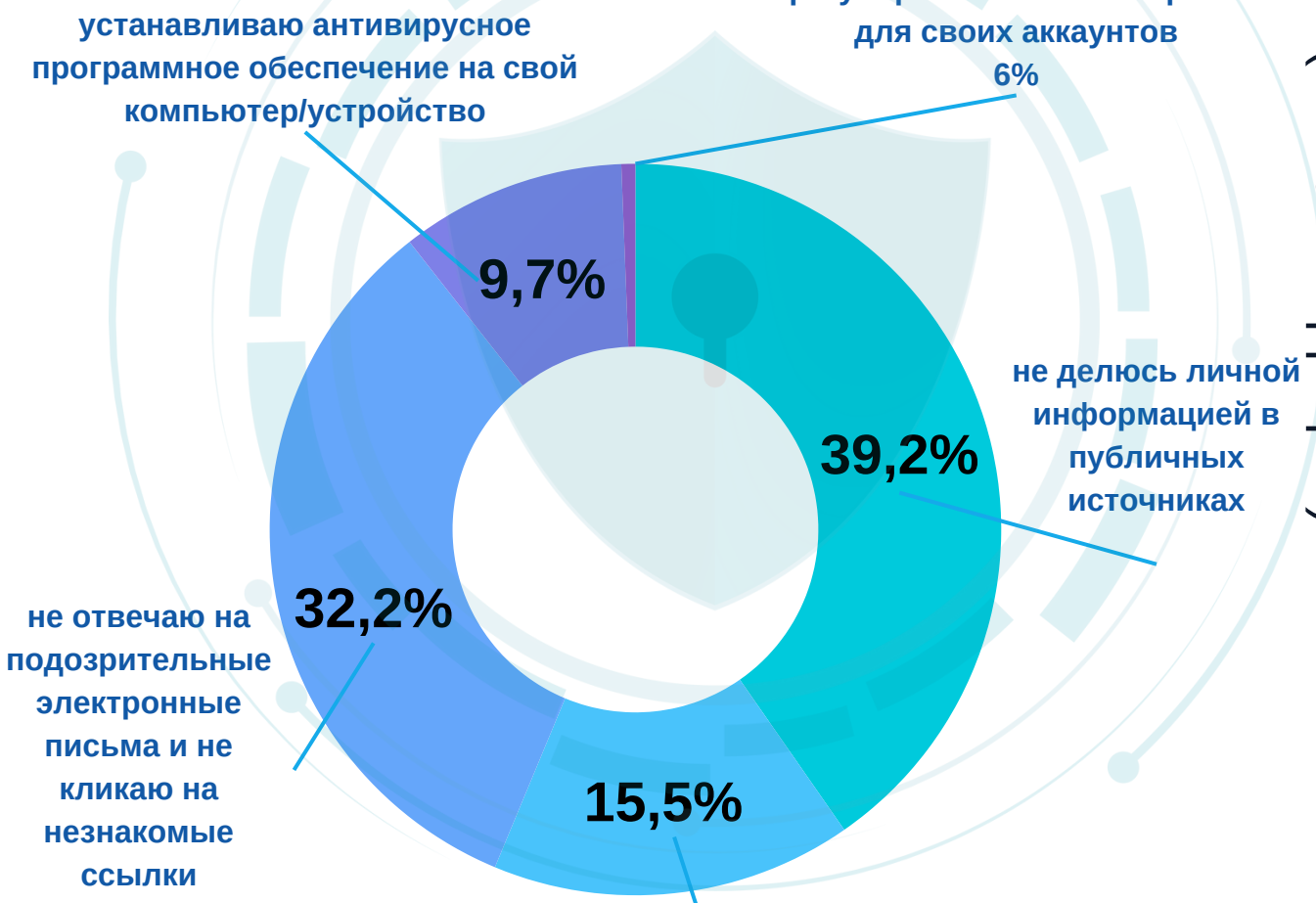
- компьютерные вирусы – 22,8%;
- вредоносные спам – 16,9%;
- взлом аккаунта – 8,1%;
- атака со стороны хакера – 3,6%;
- кибер мошенничество – 6,9%;

	2023	2022	2021	2020
Атака компьютерных вирусов	22,8%	51,7%	16,5%	32,1%
Вредоносный спам	16,9%	34,5%	23,0%	13,4%
Взлом аккаунтов в социальных сетях	8,1%	28,4%	14,5%	3,9%

РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ:

- Регулярно обновляйте пароли.
- Используйте двухфакторную аутентификацию.
- Оформляйте отдельные банковские карты для детей.
- Ограничивайте доступ приложениям и убирайте геолокацию.
- Настраивайте приватность в соцсетях.
- Используйте почту для пересылки документов.
- Скачивайте программное обеспечение только с официальных сайтов.
- Отдавайте предпочтение мобильной версии ресурса, а не сайту.

КАКИЕ МЕРЫ БЕЗОПАСНОСТИ ВЫ ИСПОЛЬЗУЕТЕ ПРИ РАБОТЕ В ИНТЕРНЕТЕ?



ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ (РЕКОМЕНДАЦИИ)

ПРОФИЛАКТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРОВЕРЯЮТ ЛИ РЕСПОНДЕНТЫ ИНФОРМАЦИЮ О САЙТАХ, НА КОТОРЫХ ОНИ РЕГИСТРИРУЮТСЯ?

Результаты социального опроса показывают:

40,4% процентов респондентов проверяют информацию о сайтах регулярно;

42,5% процентов респондентов проверяют информацию о сайтах иногда, когда ресурс вызывают какие-либо сомнения;

16,9% процентов респондентов не проверяют информацию о сайтах никогда;

Что следует предпринять, если Вы заметили подозрительную активность на своем банковском счете в интернет-банкинге, онлайн магазине и т.д.?

5,96% респондентов поделятся информацией о подозрительной активности в социальных сетях;

68,91% респондентов сразу же сообщат в банк о подозрительной активности;

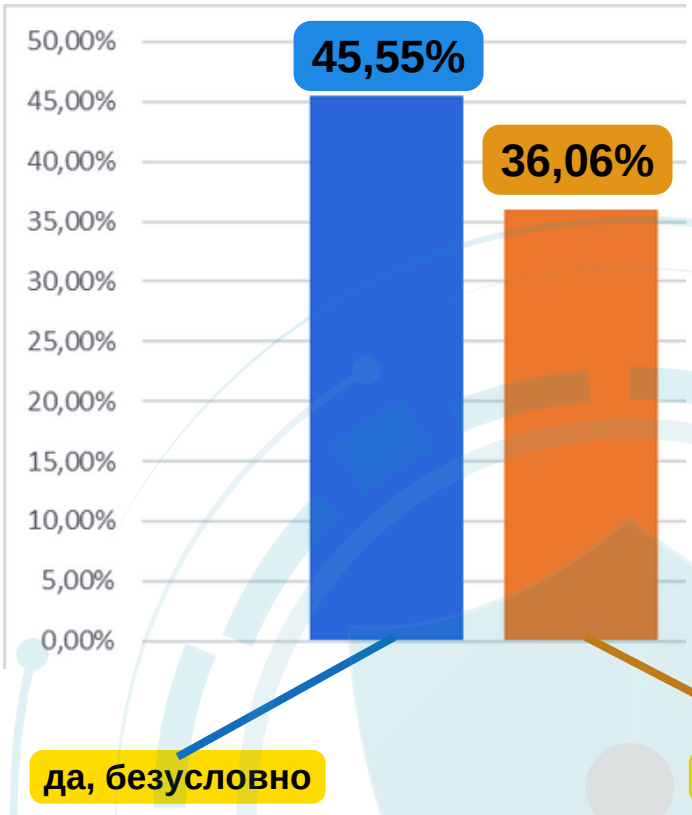
12,35% респондентов оставят все как есть, возможно это системная ошибка;

РЕКОМЕНДАЦИИ
(профилактика по информационной безопасности)

- **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 или программного обеспечения из непроверенных источников.**
- **Регулярно создавайте копию важных для вас данных на других устройствах.**

ПРОФИЛАКТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ответ респондентов на проведенный опрос:



«Знаете ли Вы о деятельности уполномоченного органа по вопросам обеспечения информационной безопасности и способах обращения к нему?»

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

- **Обращение в правоохранительные органы** — **10,79%**
- **Обращение к IT-специалисту** — **55,36%**
- **Обращение в уполномоченный орган в сфере обеспечения информационной безопасности** — **15,37%**
- **Не считают нужным что-либо делать** — **3,70%**

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ (РЕКОМЕНДАЦИИ)

При любых нестандартных подозрениях на нарушение информационной безопасности:
-незамедлительно обратитесь к ответственным специалистам;
-также можно обратиться в службу реагирования на компьютер/ телефон:
1400 или
+7 (7172) 55-99-97,
эл.почта:
info@ kz-cert.kz

РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПАРОЛЬНАЯ ПОЛИТИКА

Запрещается хранить 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.

ПОЧТА

Запрещается открывать электронные письма и подозрительные вложения от незнакомых лиц.

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.

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.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Запрещается сообщать третьим лицам IP-адреса и сочетание логина и пароля.

Запрещается устанавливать самостоятельно программное обеспечение.

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.

ДОПОЛНИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ГОСУДАРСТВЕННЫХ СЛУЖАЩИХ

- Запрещается подключение внутренних сетей государственного органа (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, местных исполнительных органов (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 Единой транспортной среде (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;**
- **восможность трансграничной передачи данных;**
- **возможность распространения персональных данных в общественных источниках.**

При предоставлении персональных данных куда либо, обязательным требованием является наличие согласия физического лица или 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.

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 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,

11 декабря 2023 года появилась новая система защиты по закону «О внесений изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов»:

Закон предусматривает следующие нововведения в части:

наделения уполномоченного органа в сфере защиты персональных данных (Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан) функцией государственного контроля за соблюдением законодательства Республики Казахстан о персональных данных и их защите;

установление запрета на сбор, обработку копий документов, удостоверяющих личность, содержащих персональные данные;

информирование граждан о фактах утечки персональных данных;

установления добровольного отказа от получения банковских займов;

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 Республики Казахстан для принятия мер по пресечению нарушений.

Это можно сделать, написав через портал “Электронного правительства” (раздел “Электронные обращения”), также можно написать на личный блог председателя (*https://dialog.egov.kz/blogs/3932160/welcome*)

ОБРАЩЕНИЯ ДОЛЖНЫ СОДЕРЖАТЬ:

1. ФИО,контакты заявителя;
2. Описание ситуации, при которой допущено нарушение;
3. Период и сроки совершения нарушения;
4. Достоверныематериалы, подтверждающие нарушение;
5. 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 в сфере защиты персональных данных – КОМИТЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МИНИСТЕРСТВА ЦИФРОВОГО РАЗВИТИЯ, ИННОВАЦИЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН. Обращения можно подавать любым удобным и доступным способом.

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Что такое электронная цифровая подпись (ЭЦП)?

Проще говоря, электронная цифровая подпись (ЭЦП) – это собственная подпись гражданина в электронном виде, на которой можно подписывать документы.

Что может произойти в случае попадания ЭЦП в руки мошенников или кого-либо еще:

Если ЭЦП не защищен паролем, через него могут быть подписаны документы или финансовые операции.

Для субъектов предпринимательства получение ЭЦП может привести к трудоустройству “фиктивных работников”.

Регистрация нескольких лиц без уведомления в квартире по имени владельца ЭЦП.

По защите собственной ЭЦП необходимо принять следующие меры:

Когда вы впервые получаете ЭЦП из ЦОНа, может стоять простой пароль, поэтому его следует заменить сложным паролем.

Не передавайте ЭЦП посторонним лицам. Они могут подписывать документы от вашего имени, когда ответственность лежит на вас.

Не отправляйте ЭЦП в специальных чатах, мессенджерах.

Обеспечьте компьютер или ноутбук, на котором хранится ЭЦП, программами защиты от вирусов.

При сохранении ЭЦП в файлах не сохраняйте ее пароль с именем файла.

Не берите ЭЦП на кого-то другого. Получить ЭЦП можно несколькими способами: через Центры обслуживания населения (ЦОН) или через eGov.

Избегайте установки непроверенных или ненадежных программ на гаджеты-смартфоны с вашим компьютером.

Немедленно обновите свой ключ, если вы потеряли ЭЦП или если он попал в руки других лиц.

Защита безопасности детей в сети Интернет

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ (РЕКОМЕНДАЦИИ)

На сегодняшний день на интернет ресурсе появляется все больше источников, представляющих опасность для детей. Если упомянуть некоторых из них: **запрещенные заговоры, ресурсы и группы, которые побуждают детей к суициду или к негативным действиям буллинга, которые наносят вред детям.**

Кибербуллинг на сегодняшний день является очень актуальной проблемой для безопасности детей. В таких ситуациях родители должны обратить внимание:

- Плохое настроение после проведенного времени в Интернете.
- Становится необычайно скрытным, особенно когда дело доходит до использования нежелательных информаций в сети интернет.
- Агрессия или вспышка гнева.
- Тревога и/или волнения у ребенка.
- Часто просят деньги.

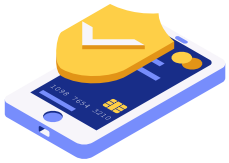
Какие меры следует предпринять родителям для защиты детей от киберугроз:

* Ограничьте время использования интернета.

* Возьмите под свой контроль контент, просматриваемый детьми в интернете и различных сетях.

* Обсудите с детьми потенциальные угрозы в интернете.

* Объясните детям, что на негативный контент можно жаловаться модератору ресурса.

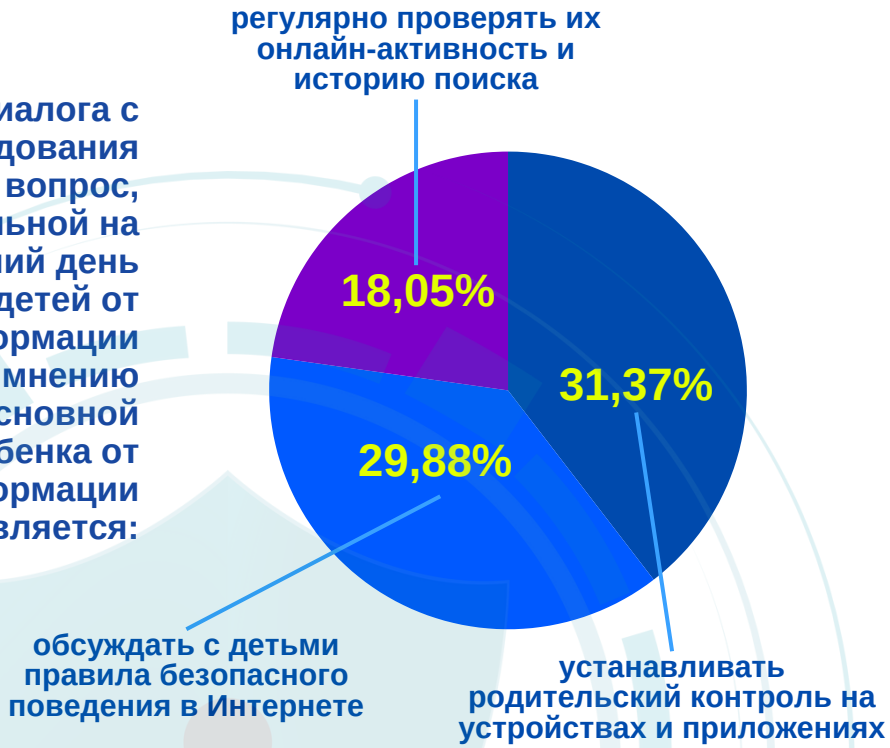


* Если дети сталкиваются с неприятной ситуацией в интернете, помогите им преодолеть эту ситуацию, не повышая голоса.

Правила информационной безопасности ДЕТЕЙ И ПОДРОСТКОВ В СЕТИ ИНТЕРНЕТ

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ (РЕКОМЕНДАЦИИ)

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?

1. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилейи при регистрации на конкурсы в Интернете.

2. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

3. 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.

4. 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.

5. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

6. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

РАЗДЕЛ ДЛЯ ПРОФЕССИОНАЛОВ

Рекомендации, которые следует помнить владельцам бизнеса, работникам соответствующей отрасли, IT-специалисту, офицеру информационной безопасности:

1 РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Руководство предприятия или организации должно разработать и внедрить концепцию по обеспечению информационной безопасности. Этот документ является основополагающим для разработки внутренних регламентов и системы защитных мер.

2 СОЗДАНИЕ ЗАЩИТЫ НА НЕСКОЛЬКИХ УРОВНЯХ.

Многоуровневый подход к кибербезопасности снизит риск атаки шифровальщиков. Он предполагает комбинирование нескольких защитных инструментов. Если угроза обойдет один уровень защиты, то на следующем уровне она столкнется с новым препятствием.

3 ПЕРЕСМОТР ПОЛИТИКИ ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ УСТРОЙСТВ В РАБОЧИХ ЦЕЛЯХ.

Удаленные сотрудники иногда пользуются собственными ноутбуками или мобильными устройствами для работы и подключения к корпоративной сети. Однако на личных устройствах не всегда установлен надежный антивирус или другое средство безопасности.

4 ИСПОЛЬЗОВАНИЕ ФИЛЬТРОВ ЭЛЕКТРОННОЙ ПОЧТЫ.

Конечно, почтовые фильтры не могут гарантировать, что организация не получит фишинговое письмо, но они повышают уровень безопасности. 46,1% респондентов указали, что открывают только известные и надежные электронные письма.

5 ИСПОЛЬЗОВАНИЕ МЕНЕДЖЕРА ПАРОЛЕЙ.

Организация использования сотрудниками менеджера паролей- он создает и хранит длинные и сложные пароли и переносит их в поля ввода в приложениях.

РАЗДЕЛ ДЛЯ ПРОФЕССИОНАЛОВ

6 РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ.

Регулярно создавайте резервную копию не только тех данных, которые хранятся на компьютере, но и тех, что вы храните на мобильных устройствах. Так вы сможете быстро восстановить нужную информацию, если устройство будет потеряно или украдено.

7 ОБУЧЕНИЕ СОТРУДНИКОВ.

В большинстве случаев сотрудники не знают, что их действия могут быть опасными. Вы можете снизить риск человеческой ошибки, повысив осведомленность сотрудников организации о киберугрозах, включая угрозы, связанные с социальной инженерией.

В случае угрозы информационной безопасности исследование показало, что 55,4% респондентов обращаются к специалистам it - сферы.

8 СОСТАВЛЕНИЕ ПЛАНА ДЕЙСТВИЙ В СЛУЧАЕ КИБЕРАТАКИ.

Нужно быть готовым к чрезвычайной ситуации.Для надежной защиты бизнеса, сотрудников и клиентов важно иметь подробный план действий в случае нападения.

9 ВКЛЮЧИТЬ ЗАЩИТУ ПАРОЛЕМ.

Чтобы уберечь среднестатистического злоумышленника от мобильного устройства, необходимо использовать сложный пароль или PIN-код. 33,6% респондентов указали, что они используют индивидуальный сложный пароль для каждой учетной записи.

ПОЛНОМОЧИЯ КОМИТЕТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

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

2. **КОНТРОЛЬ**
   Государственный контроль в области обеспечения информационной безопасности в сфере информатизации, защиты персональных данных, электронного документа и электронной цифровой подписи и обеспеченных цифровых активов.

3. **ПРОФИЛАКТИКА**
   Профилактика соблюдения Единых требований в области информационно – коммуникационных технологий и обеспечения информационной безопасности.

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

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

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

7. **ОРГАНИЗАЦИЯ**
   Организация исполнения Национального плана реагирования на инциденты информационной безопасности.

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

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

14. **РАЗРЕШЕНИЕ**
    Выдача разрешения на выпуск и обращение обеспеченных цифровых активов

15. **ПОДДЕРЖКА**
    Поддержка научных исследований в сфере информационной безопасности.

КУДА ОБРАЩАТЬСЯ ПРИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТАХ?

Во время компьютерного инцидента необходимо связаться!

Служба реагирования
1400
(8 (7172) 55-99-97

info@kz-cert.kz

Национальная Служба реагирования на компьютерные инциденты – это единый центр для пользователей национальных информационных систем и сегмента сети Интернет, обеспечивающий сбор и анализ информации по компьютерным инцидентам, консультативную и техническую поддержку пользователям в предотвращении угроз компьютерной безопасности.

В КОМПЕТЕНЦИЮ СЛУЖБЫ ВХОДИТ ОБРАБОТКА СЛЕДУЮЩИХ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ С ЦЕЛЬЮ ИХ ВЫЯВЛЕНИЯ И НЕЙТРАЛИЗАЦИИ:

атаки на узлы сетевой инфраструктуры и серверные ресурсы;

несанкционированный доступ к информационным ресурсам;

сканирование национальных информационных сетей и хостов;

подбор и захват паролей и другой аутентификационной информации;

распространение вредоносного программного обеспечения, незатребованной корреспонденции (спам);

взлом систем защиты информационных сетей;

КРАТКИЙ АНАЛИЗ

результатов социологического исследования по вопросам информационной безопасности (кибербезопасности) и защиты персональных данных

По заказу Республиканского государственного учреждения «Комитет 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 80,4%.

В целом полученные результаты социологического исследования по вопросам информационной безопасности (кибербезопасности) и защиты персональных данных свидетельствуют о растущей значимости вопросов информационной безопасности в повседневной жизни граждан:

- уровень способности распознавать попытки фишинга составил – 74,64%;
- 90,52% знаний населения владеют о защите личной информации при использовании социальных сетей.

Результаты исследования показывают о положительном динамизме в формировании осведомленности населения в области информационной безопасности (кибербезопасности) и защиты персональных данных. Однако вызовы этой сферы требуют постоянного совершентсвования мер и механизмов, чтобы обеспечить стойкую защиту интересов граждан в цифровой эпохе.

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

РЕКОМЕНДАЦИИ

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: **moap@mdai.gov.kz**
https://www.gov.kz/memleket/entities/infsecurity?lang=ru

г. Астана, 2023 ж.