Министерство искусственного интеллекта и цифрового развития Республики Казахстан

Комитет по информационной безопасности

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Рекомендации

Подготовлено на основании социологического исследования “Осведомленность населения об угрозах кибербезопасности” проведенного в марте-сентябре 2025 года

Термины и определения

Что такое кибербуллинг?	Травля, оскорбления, запугивание или унижение человека с использованием цифровых технологий
Персональные данные это:	Сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном и (или) ином материальном носителе
Под кибербезопасностью понимется:	Состояние защищенности цифровых объектов от нарушения их конфиденциальности, целостности и доступности

Уровень осведомленности населения

В соответствии с Концепцией цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы одной из основной задачей является повышение уровня осведомленности населения по вопросам кибергигиены. В этом ключе в целях определения уровня осведомленности населения об угрозах кибербезопасности и защиты персональных данных проведено социологическое исследование среди населения Казахстана.

Показатели осведомленности населения об угрозах кибербезопасности и защиты персональных данных:

- 62,9% — в 2018 году
- 73,5% — в 2019 году
- 78% — в 2020 году
- 75% — в 2021 году
- 77,4% — в 2022 году
- 80,4% — в 2023 году
- 86% — в 2025 году

В процессе социологического исследования было охвачено:

- **3** города республиканского значения (Астана, Алматы, Шымкент)
- **17** районов и сел областей по Республике
- **6000** участвовавших респондентов

Участники: граждане РК от 18 лет и старше;

Количество вопросов анкетных блоков:

- **социально - демографический блок - 5;**
- **основной блок - 15;**
- **дополнительный блок - 10;**

Вопросам развития сферы кибербезопасности в Казахстане уделяется пристальное внимание. И результат работы, проводимой совместно государственными органами, НПО и бизнесом – это тенденция последних лет, когда наша страна стремительно улучшает свои позиции в Глобальном индексе кибербезопасности. Сейчас Казахстан находится в группе Tier2 - Advancing и занял 3-е место во второй группе из 29 стран, набрав 94,4 балла из 100 возможных.

НЕМНОГО ВАЖНОЙ ИНФОРМАЦИИ

Кибербезопасность становится важной частью нашей повседневной жизни. Обычно, под кибербезопасностью подразумевают соблюдение трёх важных принципов:

КОНФИДЕНЦИАЛЬНОСТЬ

Что это такое? Доступ к информации должен быть только у того, кто имеет на это право. А у кого нет такого права, тому доступ к информации закрыт.

Плохой пример: *Доступ к номеру Вашей карточки и CVV коду получил плохой человек.*

ПО МНЕНИЮ:

28% **респондентов, одним из наиболее эффективных действий для защиты конфиденциальных данных является использование шифрования при передаче информации.**

29% **респондентов, одним из наиболее эффективных способов защиты конфиденциальных данных является ограничение публичного доступа к личной информации.**

ДОСТУПНОСТЬ

Что это такое? Информация должна быть доступна в любой момент, когда она нужна. Сразу и быстро.

Плохой пример: *Вы должны подать заявку на устройство ребёнка в детский сад через «Портал Акимата». По-другому не принимают. Но сайт этого портала не открывается 5 минут, 15 минут, час, день, неделю…*

ЦЕЛОСТНОСТЬ

Что это такое? Информация должна быть достоверной. Она не должна меняться сама и тем более её не должны искажать намеренно.

Плохой пример: *Вы делаете перевод денежных средств со своей карточки на карточку друга. Вредоносное ПО может изменить номер карточки получателя и отправить деньги на карточку злоумышленника.*

Итак,

КИБЕРБЕЗОПАСНОСТЬ — это соблюдение Конфиденциальности, Доступности, Целостности.

Нарушение одного принципа, как правило, приводит к нарушению других.

	2025	2023	2022	2021	2020
Атака компьютерных вирусов	18%	22,8%	51,7%	16,5%	32,1%
Вредоносный спам	12%	16,9%	34,5%	23,0%	13,4%
Взлом аккаунтов в социальных сетях	5%	8,1%	28,4%	14,5%	3,9%

КАК ИЗБЕЖАТЬ НЕПРИЯТНОСТЕЙ?

11% **пользователей не используют антивирус и не используют защиту паролем.**

7 шагов к личной КИБЕРБЕЗОПАСНОСТИ

Киберугрозы, хакеры, вирусы, троянские кони.

Всё непонятно и запутанно?

Не пугайтесь. Защитите себя и своих близких! Мы покажем Вам путь. Путь к кибербезопасности состоит из 7 простых шагов.

Идите с нами и злые хакеры с их вирусами Вам не страшны.

шаг 1

ХРАНИТЕ ЭЦП КАК ЗЕНИЦУ ОКА

- **Все мы знаем, что такое ЭЦП. Это – Электронно-цифровая подпись. Тут на Вашу защиту встаёт точнейшая из наук – математика. Каждый гражданин Казахстана может легко получить ЭЦП. ЭЦП — это удобно и надёжно.**
- **Но есть серьёзная опасность, и Вы должны её знать. Если ЭЦП у Вас украли, то документы за Вас может подписывать кто-то другой. Иногда это очень важные документы! Да, да, ЭЦП можно украсть, как и всё, что лежит без присмотра.**

По защите собственной ЭЦП необходимо принять следующие меры:

- **При первом получении ЭЦП сразу установите сложный пароль.**
- **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.**

шаг 1

ВАЖНО!

Как правило, при выдаче ЭЦП сотрудник ЦОНа устанавливает типовой пароль. Обязательно смените пароль от своего ЭЦП. Это можно сделать на сайте www.pki.gov.kz

Или просто попросите при выпуске ЭЦП установить Ваш собственный, а не типовой пароль. Но его придётся запомнить.

ЧТО НЕ НУЖНО ДЕЛАТЬ!

НИКОГДА НЕ ОТПРАВЛЯЙТЕ ЭЦП В ОТКРЫТОМ ВИДЕ ПО ЭЛЕКТРОННОЙ ПОЧТЕ.

Почту могут взломать, тогда ЭЦП точно украдут. Нужно всё-таки отправить? На Ваш страх и риск, но обязательно зашифруйте ЭЦП любым надёжным способом. Например, с помощью техники «заархивировать с паролем». Не умеете «архивировать с паролем»? Спросите у специалистов, родственников и друзей. Вам обязательно помогут.

Никогда не копируйте своё ЭЦП на незнакомые компьютеры.

Если всё-таки пришлось подписывать что-либо с незнакомого компьютера, обязательно убедитесь, что Ваше ЭЦП не осталось на чужом компьютере.

Не храните своё ЭЦП на компьютере.

Если хакеры всё-таки Вас взломали или вирус проник в Ваш компьютер, то они не должны найти там ЭЦП, так как его там не должно быть. Если Вы получили ЭЦП на флэшку, а не на удостоверение личности или токен, то пусть ЭЦП и остаётся на флэшке. Храните флэшку в надёжном месте и не используйте для других нужд, кроме хранения ЭЦП.

шаг 2

ВАШ ЩИТ — ВАШ ПАРОЛЬ

Наш мозг устроен интересным образом. Мы мыслим ассоциациями. Наша мысль обязательно построена на предыдущей мысли. Наше мышление представляет собой поток мыслей, воспоминаний и идей, все они обязательно взаимосвязаны.

У нас два вида памяти: краткосрочная и долгосрочная.

В краткосрочной памяти хранятся все события или информация на несколько минут или часов. Возможно — дней.

Если информация для нас важная и мы переживаем в процессе запоминания какие-либо ассоциации, то информация переходит в долгосрочную память.

Как уверяют исследователи мозга, это построено на образовании синапсов нейронов головного мозга. Самый простой способ записать информацию в долгосрочную память — сделать ассоциативную связь между информацией и чем-то, что уже запомнилось Вам навсегда. Или которое легко вспомнить.

Нужно воспользоваться самыми большими участками нашего мозга, отвечающими за: СЛУХ и ЗРЕНИЕ.

шаг 2

ЧТО ДЕЛАТЬ?

У нас сильно развиты отделы мозга, отвечающие за зрительную память. Этим и нужно воспользоваться.

Садясь за рабочий компьютер, оглядитесь вокруг. Вокруг Вас будут сотни предметов, которые постоянно находятся на Вашем столе, на стенах, в шкафах или даже за окном.

Просто загадайте как пароль предмет, который Вы видите каждый день, сидя за своим рабочим местом. Это и будет Ваш пароль.

Пример: Kachestvennyy_organayzer

Пользователи составлящие сложные пароли:

В 2023 году — **22%**

В 2025 году — **47%**

ВАЖНО!

Загадывая предмет в качестве пароля, загадайте два слова, например, название предмета и его цвет.

Можно загадывать слова любимых песен, города и места, где Вы были. Главное, чтобы в пароле было минимум 8 знаков.

ЧТО НЕ НУЖНО ДЕЛАТЬ?

1) Никогда не передавайте свои пароли другим людям. **Даже если просят.**

2) Не записывайте свои пароли на стикеры, бумажки. **Не храните пароли в электронной почте.**

шаг 3

ЭЛЕКТРОННАЯ ПОЧТА

К сожалению, мошенники давно поняли, что мы читаем отправленные нам письма. Значит, если написать хитрое письмо, нас можно обмануть.

Пример мошеннической схемы: «Письмо от иностранного адвоката о наследстве». Суть схемы:

На электронную почту приходит письмо от человека, который представляется иностранным адвокатом или нотариусом. Он сообщает, что его «клиент с вашей фамилией» недавно умер и оставил крупное состояние — обычно от 1 до 10 млн долларов.

Как развивается мошенничество:

1. Адвокат утверждает, что наследников нет и вы можете стать законным получателем. 2. Просит предоставить: копию удостоверения личности, контактные данные, иногда — доверенность. 3. Далее сообщает, что для оформления нужно оплатить «небольшие расходы»: нотариальные услуги, пошлины, оплату перевода документов, «разморозку счёта» в банке.

После отправки денег — мошенники прекращают общение.

Самым распространённым способом заражения персональных компьютеров является отправка электронного письма с вредоносным содержимым.

ЧТО ДЕЛАТЬ?

Никогда не открывайте самозапускаемые файлы.

Такие файлы легко распознать по буквам, которые идут после последней точки в названии. Эти буквы называются расширением файла.

Примеры расширений самозапускающихся файлов:

.exe **.com** **.cmd** **.msi** **.bat**

Файлы вложений с такими расширениями открывать нельзя.

Даже если они помещены в архив. Например, упакованы в архив WinZip.

шаг 3

Хакеры могут модифицировать и обычные файлы документов офисных приложений.

Макросы — набор команд, которые позволяют записывать и воспроизводить стандартный пакет офисных приложений. Вы не знаете, какие команды записаны в макрос. Набор команд может быть довольно большим и представлять собой вредоносный код.

ВАЖНО!

Ни в коем случае нельзя включать «макросы», пришедшие с файлами по электронной почте.

ЧТО НЕ НУЖНО ДЕЛАТЬ?

Не открывайте подозрительные письма.

Если письмо Вам не интересно, значит оно не достойно Вашего внимания. Внимательно изучите вложенные файлы (вложения).

Не отвечайте на подозрительные письма.

Не переходите по ссылкам в подозрительных письмах.

Помните, мошенники играют на человеческих чувствах – жадности, гордыне, страхе, гневе. Думайте головой и не попадайте на мошеннические схемы.

45% **пользователей не переходят по присланным ссылкам в социальных сетях и мессенджерах**

шаг 4

АНТИВИРУСНАЯ ЗАЩИТА

Как понятно из названия, **Антивирус – это такое средство для защиты от «вирусов».**

Мы называем всё вредоносное программное обеспечение «вирусами». Это не совсем корректно, так как «вирус» — это только один из признаков вредоносного программного обеспечения (сокращённо ПО).

Но что нужно точно знать – вредоносное ПО не миф, оно реально вредоносно и его реально много. Мошенники пытаются придумывать всё более хитроумные схемы нарушения доступности, конфиденциальности и целостности.

Компьютерные «вирусы» очень похожи на реальные заразные болезни, только поражают они не людей, а компьютерные системы.

Антивирус нужно воспринимать как вакцины и прививки, только для компьютерных «вирусов».

ЧТО ГЛАВНОЕ В ПРИВИВКЕ?

1. Прививка должна быть качественно изготовлена,
иначе могут возникнуть побочные эффекты и возможны тяжёлые последствия. Мы всегда задаём вопросы при вакцинации: что это за прививка, кто её изготовил, прошла ли она клинические испытания?

2. Прививка должна быть эффективна,
иначе нет смысла её вообще ставить. В этом случае вакцинация может принести немало вреда. Мы получаем иллюзию защиты, которой на самом деле нет.

3. Прививку нужно ставить вовремя!
Нельзя пропускать срок вакцинации и тем более ставить прививку на ослабленный или даже больной организм.

шаг 4

Относитесь к антивирусам, как к прививкам от реальных человеческих вирусов.

Количество респондентов, считающих использование антивирусного ПО самым важным в обеспечении информационной безопасности в интернете:

В 2023 году

23%

В 2025 году

23%

Поставьте себе на смартфон и компьютер любой надёжный антивирус и не выключайте его обновления!

шаг 5

ОБНОВЛЕНИЯ И ЕЩЁ РАЗ ОБНОВЛЕНИЯ

Обновления системы, как они нас нервируют! Но современные ПО – это продукт труда тысяч профессионалов.

Современные программы содержат тысячи строк кода. Конечно, в этом коде могут обнаруживаться какие-нибудь ошибки, нестиковки, пробелы. Такие ошибки принято называть **«уязвимости»**.

Это похоже на некачественно построенную стену с дырами, которую оклеили обоями. Если знать, где в этой стене дыра, можно пальцем пробить обои.

Хорошо, что программное обеспечение – это не стены. Это набор компьютерного кода.

И хорошо, что Ваш смартфон и компьютер подключены к Интернету. Через Интернет производители программного обеспечения высылают **«заплатки»** на свои же **«уязвимости»**.

Кстати, заплатка по-английски называется patch, отсюда слово **заплатка — патч.**

Пожалуйста, заделывайте дыры в стенах вовремя! Пусть патчи устанавливаются на Ваше программное обеспечение вовремя. Промедление даже на несколько часов опасно.

ЧТО ДЕЛАТЬ?

Устанавливать обновления программного обеспечения. Всегда.
Антивирус и операционная система должны обновляться автоматически.

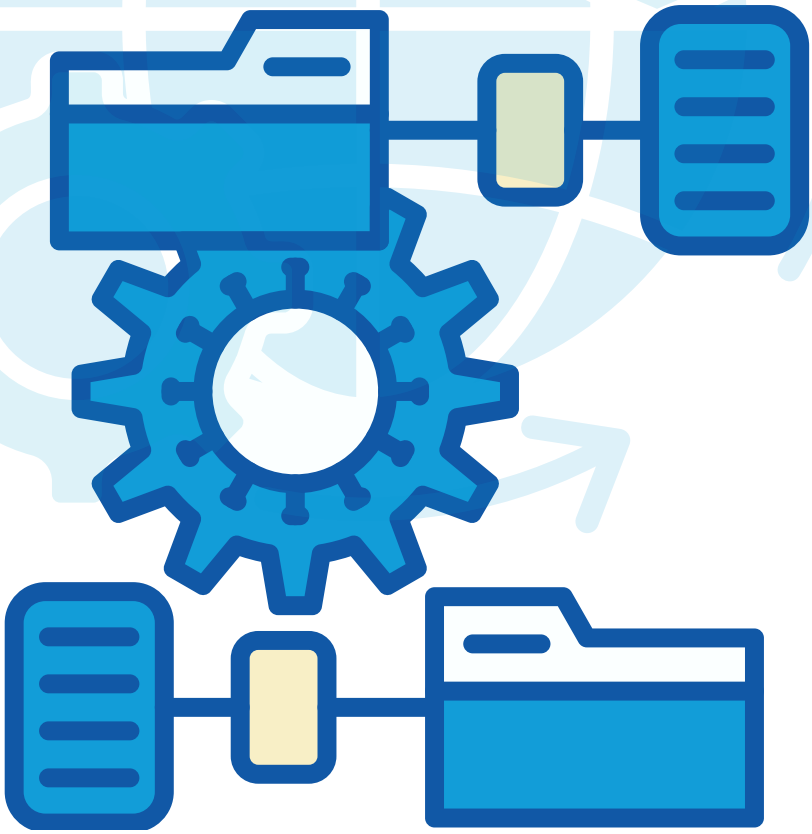
Проверять, установлены ли последние обновления.

шаг 5

ЧТО НЕ НУЖНО ДЕЛАТЬ?

Использовать контрафактное (пиратское) ПО.
Как правило, пиратское ПО уже взломано умельцами и отключено от системы обновлений. Ведь при обращении на сервер производителя ПО сразу становится понятно, что товар контрафактный. Значит, Вы не получите обновлений и будете пользоваться «дырявым» ПО.
Вам это нужно?

И, пожалуйста, не отключайте обновления.



шаг 6

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. СОЦИАЛЬНЫЕ СЕТИ. СКИММИНГ

Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей.
Никогда никому не говорите свои пароли от компьютерных систем. Никогда не оставляйте записанные на бумаге пароли на видных или доступных для посторонних местах.

Знайте, злоумышленники пытаются манипулировать нашими эмоциями.
Не говорите незнакомым людям: номера мобильных телефонов своих родственников и коллег, IP адреса, время отсутствия на рабочем месте или дома.

Экран Вашего монитора или смартфона могут подсмотреть через плечо.
Не работайте за компьютером или ноутбуком, когда за Вашей спиной есть посторонние.
В людных местах старайтесь работать спиной к непрозрачной стене.

Скимминг – кража данных банковской карты или паролей при помощи специально считывающего устройства, скиммера.

В публичных местах много видеокамер. Старайтесь вводить пароли как можно более скрытно. Например, прикрыв экран мобильного телефона ладонью или одеждой. Экран ноутбука желательно максимально прикрыть при вводе пароля, чтобы скрыть движения Ваших пальцев.

Банкоматы и терминалы оплаты:
Внимательно осмотрите банкомат, перед тем как им воспользоваться. Необычно высокая клавиатура ввода, необычное окошко ввода карточки должны Вас насторожить.

шаг 6

Сомневаетесь – воспользуйтесь другим банкоматом. Ведите себя так, как будто прямо за Вами стоят несколько подозрительных людей.
Прикрывайте ладонью клавиатуру, когда вводите пин-код или пароль.

ЧТО ДЕЛАТЬ?

Будьте внимательны, собраны и осторожны.

ЧТО НЕ НУЖНО ДЕЛАТЬ?

- **Разговаривать с незнакомыми людьми по телефону насчёт своих банковских счетов или карт.**

Конечно, разговаривать иногда нужно, но только если Вы сами позвонили в банк по официальному номеру телефона.

- **Не отвечать на подозрительные письма, но об этом мы уже говорили в разделе Почта.**
- **Пользоваться подозрительными банкоматами и терминалами оплаты.**
- **Отдавать свою карточку официанту или бармену надолго в руки. Платите картой только сами.**

Если Вы подключились к сети Интернет через публичный WiFi (например, в аэропорту или в кафе), то желательно воспользоваться сервисами VPN.

шаг 7

РЕЗЕРВНОЕ КОПИРОВАНИЕ

ИНФОРМАЦИЯ МОЖЕТ ИСЧЕЗНУТЬ. И НЕ ОБЯЗАТЕЛЬНО ВАС АТАКОВАЛИ ЗЛЫЕ ХАКЕРЫ. ПРОСТО ПОТЕРЯЛИ ТЕЛЕФОН ИЛИ СГОРЕЛ ЖЁСТКИЙ ДИСК КОМПЬЮТЕРА.

ЧТО ДЕЛАТЬ?

Регулярно копировать важную информацию на внешний носитель.

Самое простое — воспользоваться множеством сервисов резервного копирования.

Некоторые из них бесплатны, например облако Google, Apple iCloud, Mail.ru, Yandex.

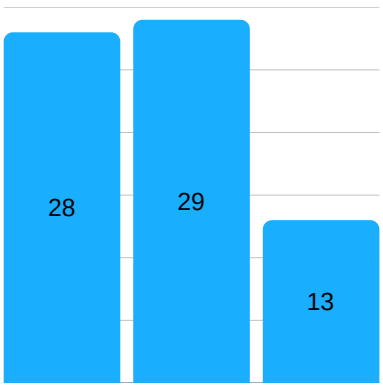
А также можно воспользоваться сервисами казахстанских облачных хранилищ Oblako.kz и Ps.kz.

ВАЖНО!

Если Вы пользуетесь облачными сервисами для хранения информации – значит Вы опытный пользователь. Ведите себя как опытный пользователь. Назвались опытным пользователем – соответственно.

Какие из следующих действий вы считаете наиболее эффективными для защиты конфиденциальных данных?

Ответ респондентов на проведенный опрос:



- **Использование шифрования при передаче данных – 28%**
- **Ограничение публичного доступа к личной информации – 29%**
- **Установка антивирусного программного обеспечения – 13%**

шаг 7

Пароли! Внимательно изучите нашу памятку в разделе «Пароли». Без надёжного пароля никаких прогулок в облака.

Двухфакторная аутентификация. Не отключайте на смартфоне разблокировку по отпечатку пальца или распознавание лица.

ЧТО НЕ НУЖНО ДЕЛАТЬ?

Хранить в «облаке» очень конфиденциальную информацию всё же не стоит. **Не храните свою ЭЦП в открытом виде, семейные или личные тайны в «облаке».**

Самое надёжное — заведите себе внешний жёсткий диск или большую карту памяти.

Просто регулярно копируйте на этот жёсткий диск важную информацию со своего компьютера или смартфона. Хотя это требует самодисциплины и организованности.

Пройдите все семь шагов – и Вы станете великим мастером личной информационной безопасности.

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

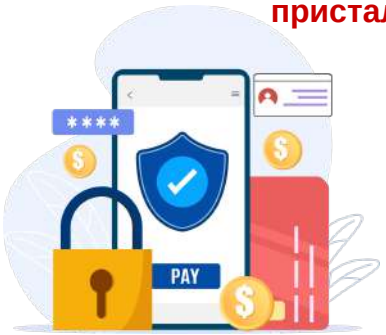
ПРИ ПОДПИСАНИИ СОГЛАСИЯ ОБРАТИТЕ ВНИМАНИЕ НА:

- **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.



ЧТО ДЕЛАТЬ?

При обнаружении фактов незаконного сбора и утечки личных данных

граждане могут обратиться в Комитет по информационной безопасности Министерства искусственного интеллекта и цифрового развития 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. Достоверные материалы, 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 ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ЦИФРОВОГО РАЗВИТИЯ РЕСПУБЛИКИ КАЗАХСТАН.

Обращения можно подавать любым удобным и доступным способом.

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.

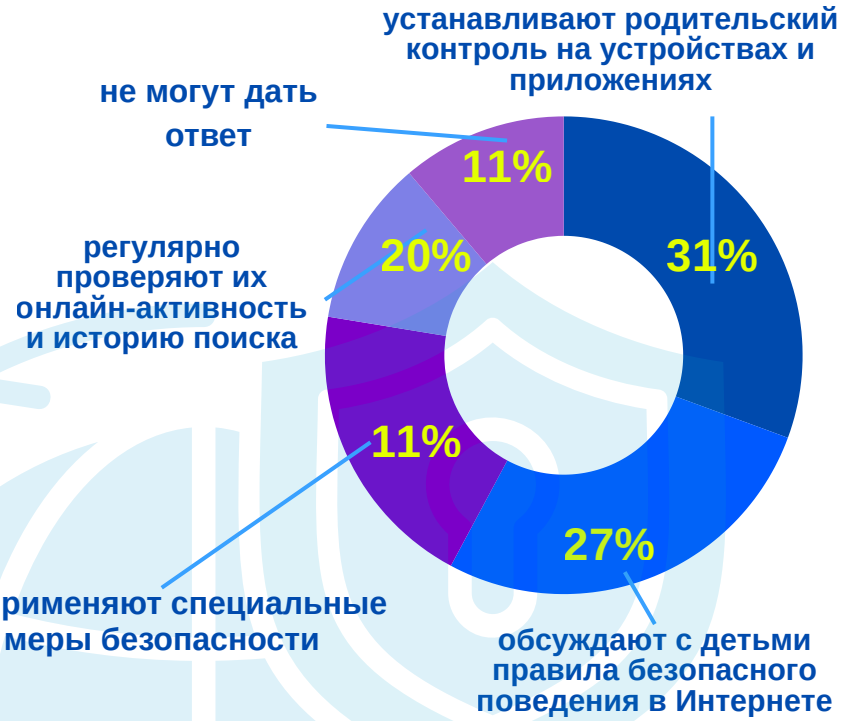
13. **ВЗАИМОДЕЙСТВИЕ**
Взаимодействие с международными организациями, национальными регуляторами и центрами кибербезопасности.

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

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

Защита безопасности детей 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.

Основные принципы при онлайн мошенничестве

1 Правило сомнения

Любое **«срочно», «немедленно», «ваш счёт заблокирован»** — повод насторожиться.

Кибермошенники всегда **давят на страх или жадность**: «потеряете деньги», «вы выиграли приз», «вам одобрен кредит»

2 Никогда не сообщайте конфиденциальные данные

ПИН-коды, пароли, CVV-код карты, коды из SMS и PUSH-уведомлений **нельзя говорить никому** — даже «сотруднику банка» или «полицейскому» по телефону.

Настоящие банки и госорганы этого **не спрашивают**.

3 Спокойствие важнее скорости

Если вам звонят и пугают блокировкой счёта, штрафами или уголовным делом, **немедленно положите трубку** и перезвоните сами в банк или в соответствующий государственный орган.

Никогда не принимайте решений «за минуту».

ИНТЕРНЕТ-ПОКУПКИ И ОНЛАЙН-СЕРВИСЫ

ПРОВЕРЯЙТЕ САЙТЫ ПЕРЕД ОПЛАТОЙ

- Адрес сайта должен начинаться с https:// и содержать правильное название магазина/банка.
- Оплачивайте только на официальных сайтах и через проверенные платёжные системы.

ОСТОРОЖНО С ОБЪЯВЛЕНИЯМИ И МАРКЕТПЛЕЙСАМИ

- Слишком низкая цена, предоплата «прямо сейчас», отказ от безопасной сделки на платформе — признаки мошенничества.
- Не переводите деньги «незнакомцу на карту» до получения товара или услуги, если нет надёжных гарантий.

ПОДДЕЛЬНЫЕ СЕРВИСЫ И ПРИЛОЖЕНИЯ

- Скачивайте приложения только из официальных магазинов (Google Play, App Store).
- Не вводите логины и пароли на сайтах, куда вас «перекинула» ссылка из SMS или письма — сами откройте сайт в браузере, набрав адрес вручную.

РАЗДЕЛ ДЛЯ ПРОФЕССИОНАЛОВ

Если Вы владелец бизнеса, ответственный сотрудник, ИТ-специалист, офицер информационной безопасности – соблюдайте эти рекомендации:

10 ШАГОВ ПО СНИЖЕНИЮ РИСКОВ КИБЕР-УГРОЗ

1 **Разработать политику информационной безопасности.** Это документ первого уровня – Ваша конституция в сфере информационной безопасности. Но кроме конституции нужны законы. Такие законы называются «Документы второго уровня» и детализируют требования политики. Подробнее смотрите постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 (ЕТ) пункт 33.

ВАЖНО!

Обязательно утвердите документ: «Правила использования мобильных устройств и носителей информации».

2 **Просвещение и осведомлённость пользователей.**
Разработать программу подготовки персонала. Внедрить системы обучения всех сотрудников нормам информационной безопасности. Поддерживать осведомлённость пользователей о кибер-рисках.

3 **Управление инцидентами.**
Необходимы (и для некоторых организаций обязательны) меры: регистрация событий ИБ, управление инцидентами ИБ, уведомления ответственных об инцидентах ИБ, регистрация инцидентов ИБ в Службе реагирования на компьютерные инциденты Государственной технической службы.
Вы должны точно знать, что происходило и происходит.
Подробнее смотрите постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 Параграф 2.

РАЗДЕЛ ДЛЯ ПРОФЕССИОНАЛОВ

4 **Управляйте рисками.**
Желательно разработать «методику оценки рисков информационной безопасности». Вы должны знать, что угрожает Вашей организации.

5 **Управление привилегиями пользователей.**
Установить процессы управления учетными записями, и ограничить количество привилегированных учетных записей. Ограничить привилегии пользователей и контролировать действия пользователя. Контроль доступа и деятельности и журналам аудита.

6 **Элементы управления съемными носителями.**
Создать политику для управления доступом к съемным носителям. Ограничение типов и использования носителей. Перед импортом в корпоративную систему просканировать все носители на наличие вредоносных программ.

7 **Мониторинг.**
Разработать стратегию мониторинга, вспомогательную политику. Постоянный мониторинг всех систем и сетей ИКТ. Проанализировать журналы на предмет необычной активности, которая может указывать на атаку.

8 **Безопасная конфигурация.**
Применяйте заплатки (патчи) безопасности и убедитесь, что безопасная конфигурация всех систем ИКТ сохраняется. Создание системы инвентаризации и определения базовой сборки для всех устройств ИКТ.

9 **Защита от вредоносных программ.**
Производить соответствующую политику и установить защиту от вредоносных программ, которые применимы и актуальны для Вашего направления деятельности. Сканирование на наличие вредоносных программ в организации.

10 **Сетевая безопасность.**
Защитить сеть от внешних и внутренних атак. Управление периметром сети. Отфильтровать несанкционированный доступ и вредоносное содержание. Мониторинг и тестирование элементов управления безопасностью.

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 кибербезопасности и защиты персональных данных

По заказу Республиканского государственного учреждения «Комитет по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан» проведено социологическое исследование по вопросам кибербезопасности и защиты персональных данных.

Результат проведенного опроса определил общий показатель осведомленности населения об имеющихся угрозах кибербезопасности и защиты персональных данных на уровне 86%.

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

- уровень способности распозновать попытки фишинга составил – 84,8%;
- 80,5% выбирают безопасную стратегию при регистрации в -онлайн-сервисах (разные сложные пароли).
- 85,9% респондентов применяют меры безопасности при покупке товаров в интернет-магазинах.
- не менее 86% родителей проверяют контент, который их дети смотрят в интернете, один или более раз в месяц.

Результаты исследования показывают о положительном динамизме в формировании осведомленности населения в области 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 кибербезопасности граждан и защиты их персональных данных в цифровом пространстве.

РЕКОМЕНДАЦИИ

По заказу РГУ "Комитет по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан"

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

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

г. Астана, 2025 г.