

Министерство цифрового развития, инноваций и  
аэрокосмической промышленности  
Республики Казахстан

Комитет по информационной безопасности

# ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ



РЕКОМЕНДАЦИИ



В целях определения уровня осведомленности населения об угрозах информационной безопасности (кибербезопасности) по заказу Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан в **июле-августе 2021 года** было проведено социологическое исследование среди населения.



В процессе исследования было охвачено:



среди населения в возрасте 18+.

Анализируя результаты опроса, можно отметить, что угроза информационной безопасности является актуальной проблемой в Республике Казахстан. Показатели осведомленности об угрозах информационной безопасности





Анализ данных исследований обращает внимание на снижение уровня осведомленности граждан в вопросах информационной безопасности на **3 %** в 2021г., что свидетельствует о влиянии условий макросреды (пандемия, рост использования онлайн приложений, удаленная работа и обучение) на показатель осведомленности населения.

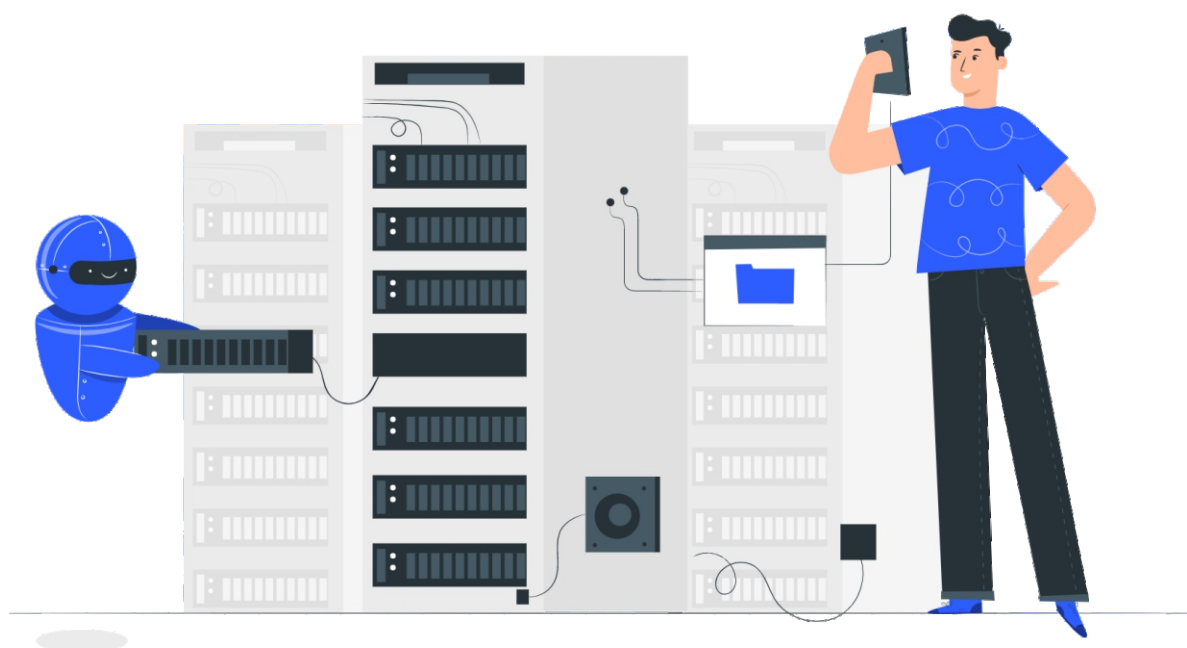


Положительным моментом является то обстоятельство, что замечен рост использования единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, так как рост составил более **17%**, что может свидетельствовать о том, что население стало больше получать государственные услуги онлайн и более осведомлено в данном вопросе.

В подтверждении к этому, нужно обратить внимание на рост числа пользователей порталом «Электронное правительство»

[www.egov.kz](http://www.egov.kz) - **23,4 %**,

что на **22,2%** выше, чем в 2020 г.



# Почему кибербезопасность важна?

Современное общество развивается в условиях неопределенности и роста влияния глобальных вызовов, в том числе и пандемии COVID-19. Это накладывает свой отпечаток на образ жизни и особенности обучения и условий труда. Так в период пандемии стали более значимыми информационные технологии, позволяющие работать и учиться удаленно. В данных условиях становится особенно актуальным и важным вопрос информационной безопасности.



Утеря данных в реальной жизни означает риски, а допустить утечку личных данных в интернет пространстве - может привести к негативным последствиям. **Государство уделяет особое внимание вопросу информационной безопасности** в связи с этим, реализуя значимые проекты и налаживая необходимые бизнес-процессы и проводя различные исследования.

## МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ

для оплаты  
онлайн услуг

**44%**

## ПОРТАЛ "ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО"

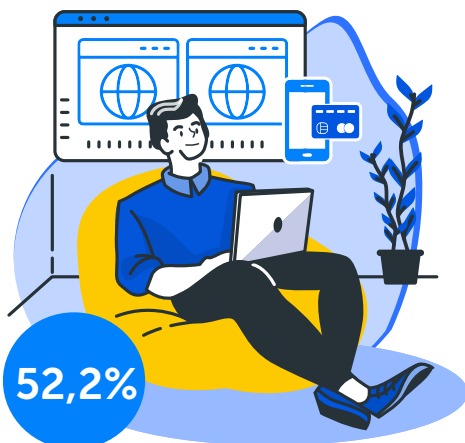
получение  
госуслуг

**23%**

## ИНТЕРНЕТ БАНКИГ

переводы, оплата,  
управление счетов

**22%**



Так, в текущем году более половины респондентов используют ежедневно интернет - **52,2%**. Интернет прежде всего необходим для оплаты онлайн услуг, использования сайта электронного правительства и др.

# Ваши права защищены законом

Использование персональных данных должно осуществляться собственником, оператором и третьим лицом только для ранее заявленных целей их сбора.

В соответствии со статьей 24 Закона Республики Казахстан «О персональных данных и их защите» Вы вправе:

- 1) знать о наличии у собственника и (или) оператора, а также третьего лица своих персональных данных, а также получать информацию, содержащую:
  - подтверждение факта, цели, источников, способов сбора и обработки персональных данных;
  - перечень персональных данных;
  - сроки обработки персональных данных, в том числе сроки их хранения;
- 2) требовать от собственника и (или) оператора изменения и дополнения, а также блокирования своих персональных данных;
- 3) отозвать согласие на сбор, обработку, распространение в общедоступных источниках, передачу третьим лицам и трансграничную передачу персональных данных;
- 4) на защиту своих прав и законных интересов, в том числе возмещение морального и материального вреда.

Если гражданин столкнулся с незаконным сбором или утечкой персональных данных, для пресечения нарушения и привлечения к ответственности виновного, он может написать обращение в уполномоченный орган по защите персональных данных – Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

## В соответствии со статьей 56 Закона Республики Казахстан "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, 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, или сбора персональных данных и до их уничтожения либо обезличивания.»



# ЗАДАЧАМИ ЕДИНЫХ ТРЕБОВАНИЙ ЯВЛЯЮТСЯ:

1



определение принципов организации и управления информатизацией государственных органов для решения текущих и стратегических задач государственного управления;

2



определение единых принципов обеспечения и управления информационной безопасностью объектов информатизации "электронного правительства";

3



установление требований по унификации компонентов объектов информационно-коммуникационной инфраструктуры;

4



установление требований по структуризации информационно-коммуникационной инфраструктуры и организации серверных помещений;

5



установление обязательности применения рекомендаций стандартов в области информационно-коммуникационных технологий и информационной безопасности на всех этапах жизненного цикла объектов информатизации;

6



повышение уровня защищенности государственных и негосударственных электронных информационных ресурсов, программного обеспечения, информационных систем и поддерживающей их информационно-коммуникационной инфраструктуры.

Согласно статье 641 Кодекс Республики Казахстан

**«Об административных правонарушениях»** за нарушения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности предусмотрена административная ответственность

Закон РК Об информатизации от 24 ноября 2015 года № 418-V ЗРК.

# 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 и Швейцария.



За прошедшие годы в стране были выработаны базовые концептуальные подходы к развитию сферы кибербезопасности страны. **Утверждена концепция кибербезопасности "Киберщит Казахстана"**.

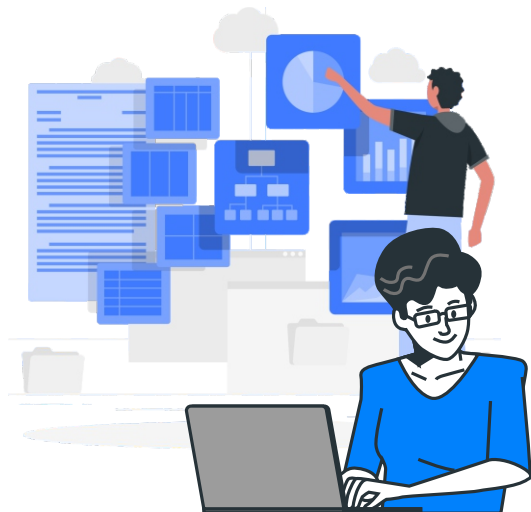


Вступил в действие целый ряд законодательных актов и отраслевых приказов. Помимо этого, созданы испытательные лаборатории в сфере информационной безопасности, запущен **Национальный координационный центр информационной безопасности**, имеются **4 Службы реагирования на компьютерные инциденты**, созданы **21 оперативных центров информационной безопасности**, увеличено количество грантов по специальности **Системы информационной безопасности** и т.д.



## Основные задачи уполномоченного органа определены:

- реализация государственной политики в области информационной безопасности в сфере информатизации, в сфере персональных данных и их защиты, а также электронного документа и электронной цифровой подписи на предмет соблюдения законодательства Республики Казахстан об электронном документе и электронной цифровой подписи;
- проведение мониторинга обеспечения информационной безопасности государственных органов, физических и юридических лиц;
- обеспечение, в пределах своей компетенции, контроля за соблюдением законодательства Республики Казахстан;



# Разъяснения по кибербезопасности

**Социальная инженерия** - это наука о том, как использовать особенности человеческой психологии для получения необходимой информации (один из основных инструментов хакеров и используется в **70%** атак).

**Распространенные варианты:**

- письмо от банка
- письмо от коллеги или руководителя
- письмо от службы технической поддержки

**Цель таких писем:** чтобы Вы поверили и перешли по предлагаемой ссылке или скачали вложенные приложения. Это может привести к утере контроля над своим компьютером или аккаунтами.

.....

**Фишинг** - это вид интернет-мошенничества, цель которого - получить идентификационные данные, номера счетов и кредитных карт.

**Как это происходит:** Отправка сообщений в виде SMS или в мессенджерах социальной сети. В этих сообщениях будут предложения перейти по ссылке или скачать фотографию.

Часто злоумышленники используют "ложные" номера телефонов или аккаунты. Именно поэтому бывает сложно проверить достоверно отправителя таких сообщений.

.....

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

**Пример:** Рассылка от банка. В первую очередь необходимо обратить внимание на почтовый адрес, это должна быть корпоративная почта. Если нет, то письмо открывать не стоит, чтобы не лишиться контроля над своим компьютером.

.....





# ЧТО НУЖНО ЗНАТЬ ПРО ЭЦП?

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;

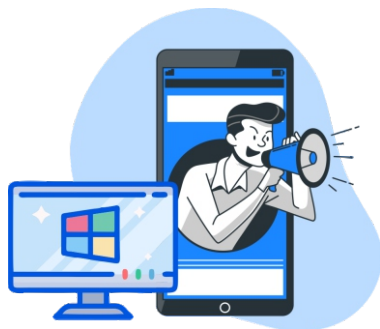


3) в случае утери перевыпустить ЭЦП, немедленно отзывая предыдущую ЭЦП, а также сменить пароль со стандартного на более сложный.

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.



# ВИДЫ УГРОЗ



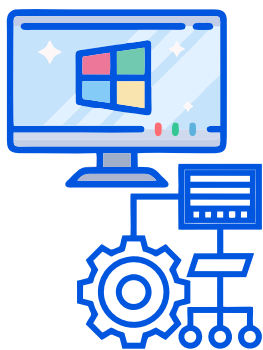
**Претестинг** - используется для получения личных данных

В результате:

- предварительной подготовки с использованием заранее, хорошо проработанного сценария;
- телефонных звонков или проведения длительной переписки с целью войти в доверие.



**Обратная социальная инженерия** - подготавливается сценарий, когда жертва сама обратится за помощью (установка приложения, вопросы технической поддержки и т.д.) Чаще всего в начале все что предоставляет хакер будет работать нормально, но через некоторое время начнет действовать вредоносная часть.



**Мальвертайзинг (вредоносная реклама)** - разновидность социальной инженерии, когда при переходе на сайт выходит сообщение, что "Мы установили, что на Вашем компьютере имеются вирусы, либо что используется устаревшее программное обеспечение. Затем обычно предлагается скачать и установить программное обеспечение с сайта. Важно помнить: что ни у браузера, ни у сайта нет информации по вашему компьютеру или используемому программному обеспечению, а скачанный файл может оказаться вирусом.

## Что угрожает Вашему компьютеру



1. Вирусы-шифровальщики и вымогатели

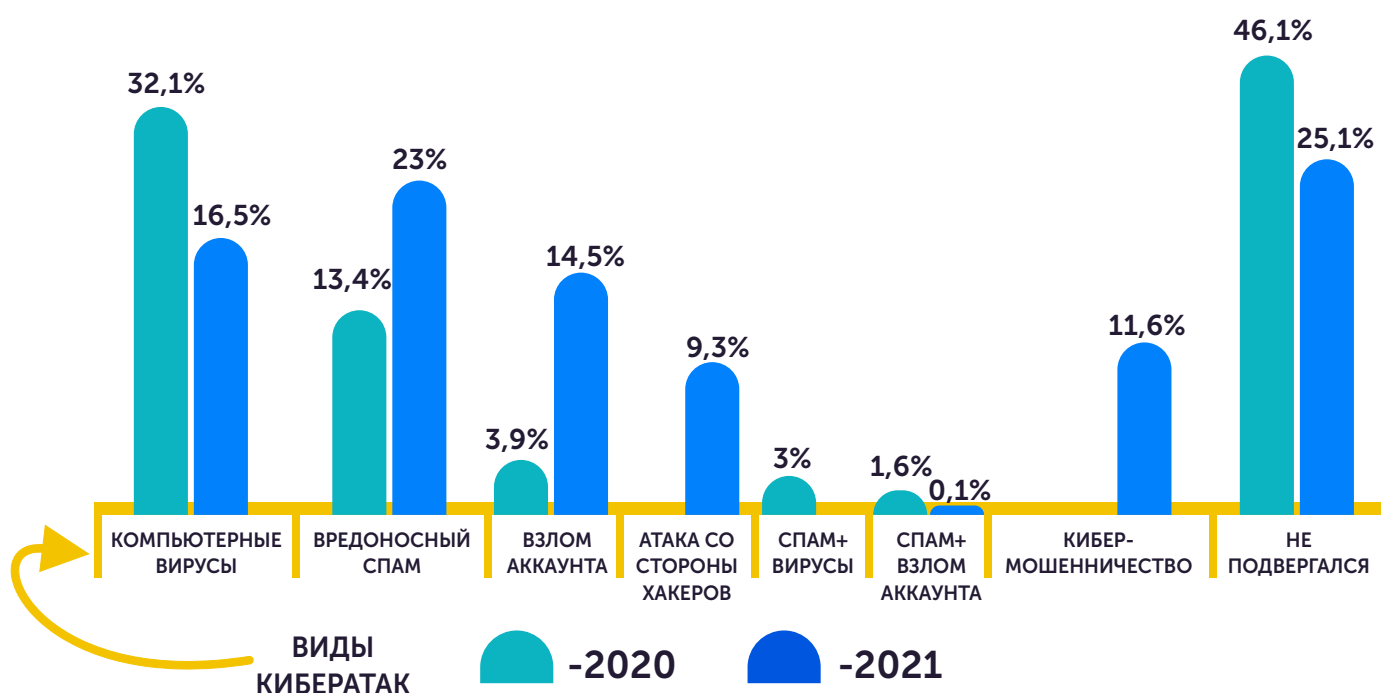


2. Кража или потеря данных

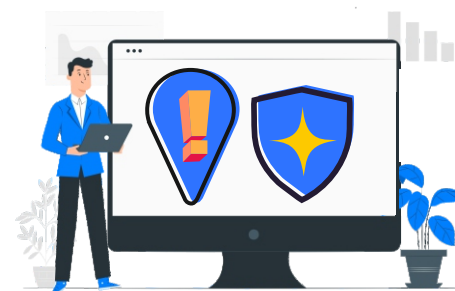


3. Кража личной информации

# Каким видам кибератак Вы подвергались?



## Почему важно обеспечить кибербезопасность?



Население в первую очередь беспокоит вопрос защиты от кибермошенничества, а также защита персональных данных от утечки, что в свою очередь может привести к мошенническим действиям и росту преступности в информационном пространстве.

Защита от  
мошенников  
каждый третий

**30%**

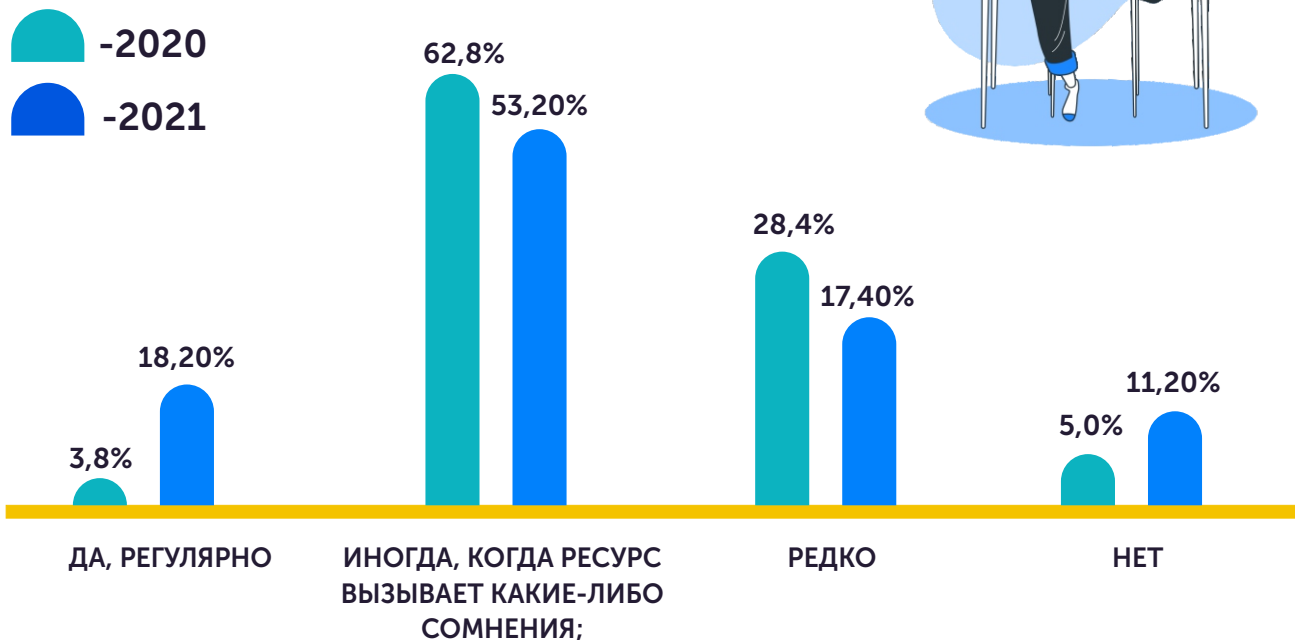
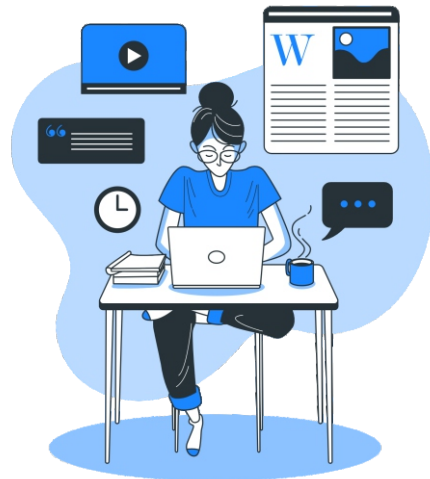
Защита  
персональных  
данных  
каждый третий

**28%**

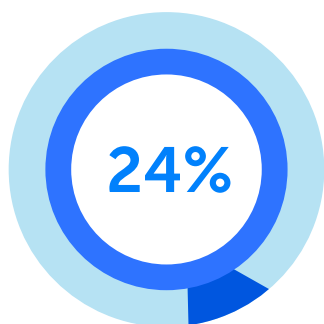
Безопасность в  
Интернет  
пространстве  
каждый четвертый

**23%**

# Проверяете ли Вы информацию о сайтах, на которых авторизуетесь?



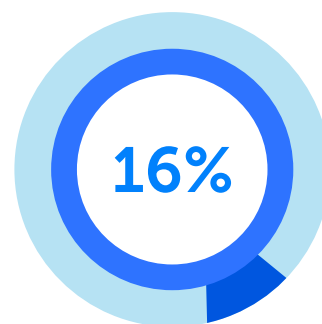
## При подозрении нарушения кибербезопасности какие меры Вы предпримете?



IT специалист  
обратится за помощью






Уполномоченный орган  
официальное обращение






Правоохранительные органы  
официальное обращение

# РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ





## ПАРОЛЬНАЯ ПОЛИТИКА

-  - Запрещается хранение паролей в открытом доступе.
- Не рекомендуется составления пароля из общеизвестных данных, таких как ФИО, дата вашего рождения и т.д.
-  - Пароли должны иметь в составе специальные символы «\*», «?», «!», а также использование заглавных букв. Количество символов не менее 8.
- 




## АНТИВИРУСНОЕ ОБЕСПЕЧЕНИЕ

-  - Запрещается использовать «пиратские» версии антивируса.
-  - Не рекомендуется пользоваться ПК без антивируса.
- Обязательно необходимо проверять все внешние источники данных на наличие вирусов.
- 




## ИНТЕРНЕТ И СОЦИАЛЬНЫЕ СЕТИ

-  - Запрещается переходить по ссылкам содержащих материалы террористической, экстремисткой, деструктивной направленности.
-  - Переходить по «фишинговым» ссылкам.
- Не рекомендуется производить вход с посторонних устройств в личные аккаунты, так как ваши данные подвержены угрозе быть использованными злоумышленниками.
- 
- Рекомендуется соблюдать «информационную гигиену». Периодический анализ сохраненных данных и доступов.
- 







## ПОЧТА

-  - Запрещается проходить по ссылкам и сообщениям от незнакомых лиц.
-  - Не рекомендуется передача и хранение «ценных» данных по электронной почте такие как ЭЦП, пароли, электронные документы.
-  - Нужно всегда проверять данные адресата.

## СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

-  - Запрещается передача третьим лицам данных содержащих IP-адреса, коды доступа, аккаунты.
-  - Не рекомендуется установка «сомнительных» ПО.
- Рекомендуется обращение к специалистам для установки новых ПО.
- 

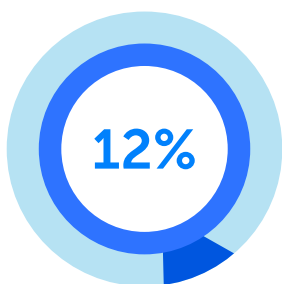
## ДОПОЛНИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ГОССЛУЖАЩИХ

-  - 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.
-  - 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.

# Считаете ли Вы, что ваши персональные данные в безопасности?



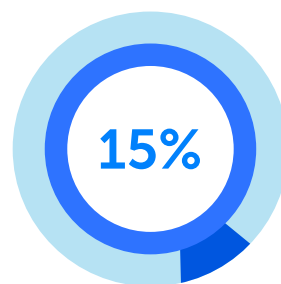
Почти каждый **четвертый** респондент отметил, что подвергался атакам очень часто, при этом только треть участников опроса отметили, что никогда не подвергались подобным атакам. Это свидетельствует о значительной частоте данного явления в онлайн пространстве и необходимо информировать население о правильных действиях в подобных случаях.



Повседневно  
каждый восьмой



Довольно часто  
каждый седьмой

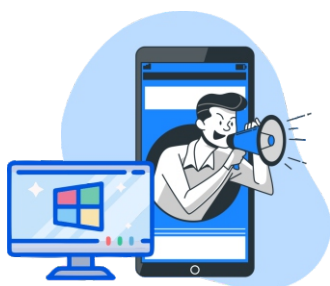


Редко  
каждый шестой

## ЧТО ДЕЛАТЬ?

Обратится в Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

Написав на электронный адрес [kib@mdai.gov.kz](mailto:kib@mdai.gov.kz), либо через портал «Электронного правительства» (раздел «Электронные обращения»), также можно написать на личный блог Председателя (<http://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;



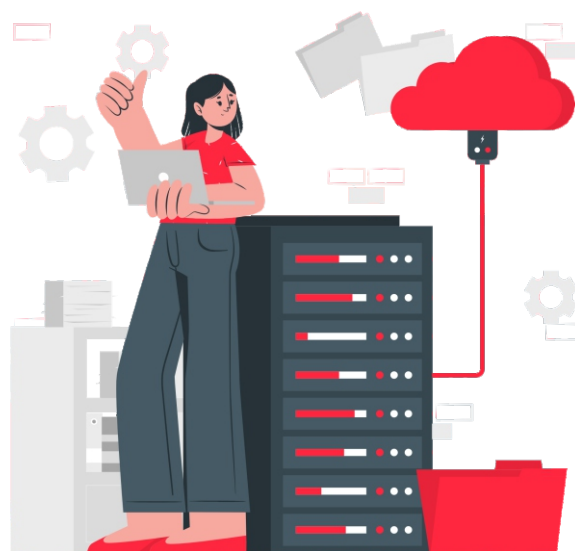
**5**  
Наименование  
организации, допустившей  
правонарушение.

# Рекомендации для рабочего места

Эксперты советуют:

## Как защитить Ваши данные?

**Кибербезопасность** не ограничивается несколькими действиями, это целая система последовательных и согласованных действий, направленных на защиту данных.



### Приложения Антивирус

Антивирусное программное обеспечение обнаруживает и удаляет вирусы на вашем компьютере. Учитывая что каждый день появляется огромное количество новых вирусов, программное обеспечение должно быть надежными.



### Брандмауэры

Брандмауэр - это цифровой барьер, защищающий ваш компьютер от опасных пользователей и вредоносных программ.



### SSO

SSO (единый вход) - это централизованное решение для аутентификации, которое позволяет пользователям получать доступ ко всей платформе учетных записей и приложений всего за один вход.



### 2FA

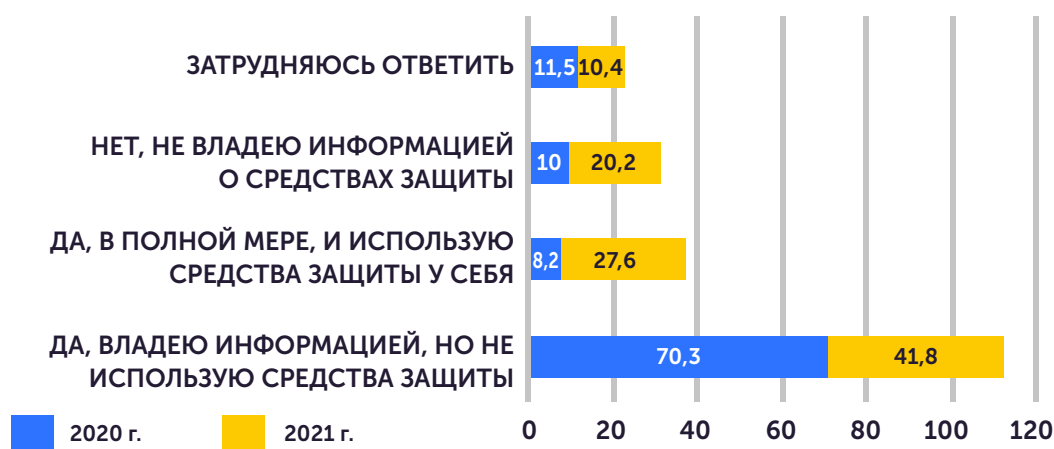
Двухфакторная аутентификация (2FA) - это метод входа в систему, который требует использования имени пользователя или пин-кода, а также доступа к внешнему устройству или учетной записи, например адресу электронной почты, номеру телефона или программному обеспечению безопасности.

# Владеете ли Вы информацией о методах защиты детей в Интернете (родительский контроль)?

К сожалению, в нашем обществе все еще актуален вопрос защиты детей в информационном пространстве. **Кибербуллинг** - это всего лишь один вид негативного воздействия, которому могут подвергнуться дети, именно поэтому важно, чтобы родители больше знали о средствах защиты.



МЕТОДЫ ЗАЩИТЫ, В %



## РОДИТЕЛЬСКИЙ КОНТРОЛЬ\*

это набор инструментов, позволяющих родителям контролировать процесс использования Интернета их детьми.



ВКЛЮЧАЮТ ФУНКЦИИ:

УПРАВЛЕНИЕ ЭКРАННЫМ  
ВРЕМЕНЕМ

ФИЛЬТРАЦИЯ ВЕБ-САЙТОВ

ИСТОРИЯ ПОСЕЩЕНИЯ  
САЙТОВ

ИСТОРИИ ИСПОЛЬЗОВАНИЯ  
ПРОГРАММ





## ✓ Рекомендации для родителей

### Как установить родительский контроль на телефоне?

1. Откройте приложение "Настройки" на устройстве ребенка.
2. Нажмите Google. Родительский контроль.
3. Нажмите Начать.
4. Выберите Ребенок или подросток.
5. Нажмите Далее.
6. Выберите аккаунт ребенка или создайте новый.
7. Нажмите Далее ...
8. Следуйте инструкциям по настройке родительского контроля.



### Как установить родительский контроль на телефоне?

1. Перейдите в меню «Настройки» и выберите функцию «Экранное время».
2. Нажмите «Продолжить» и выберите вариант «Это мой [устройство]» или «Это [устройство] моего ребенка».
3. Нажмите «Контент и конфиденциальность».
4. При необходимости введите код-пароль и выберите вариант «Контент и конфиденциальность».



## ✓ Как установить на телефоне ограничение по времени? Как ограничить время в приложениях

1. Скажите "Окей, Google" или "Siri" или нажмите и удерживайте кнопку главного экрана на телефоне.
  2. Скажите или введите команду для таймера приложений.
- Например:**  
Установи таймер для приложения на 15 минут.  
Установи таймер на 30 минут для приложения.



## ✓ Как ограничить доступ детей к интернету?(Windows)

1. Выберите раздел «Учетные записи» — «Семья и другие люди»
2. Выберите «Добавить члена семьи».
3. Таким образом можно создать отдельную учетную запись для ребенка (опция «Добавить учетную запись ребенка») и в настройках указать необходимые ограничения.

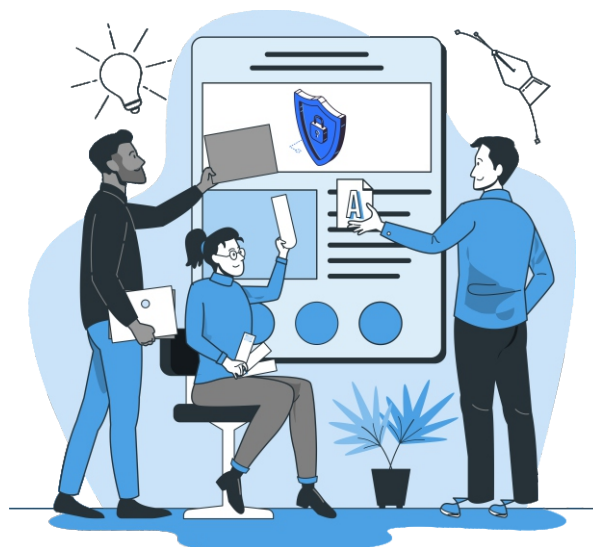
# Куда обращаться при компьютерных инцидентах?

Служба реагирования



1400

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



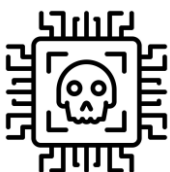
распространение вредоносного программного обеспечения, незатребованной корреспонденции (спам);



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 Служба реагирования на компьютерные инциденты

## АНАЛИЗ И ИТОГИ ИССЛЕДОВАНИЯ

1. По результатам исследования был сделан вывод, что население республики стало уделять больше внимания вопросам информационной безопасности.
2. Наблюдается рост активности использования информационных технологий и как результат рост угроз по вопросам информационной безопасности.
3. Население стало больше обращать внимание на вопросы защиты детей в интернет-пространстве.



---

В этом году при разработке буклета особое внимание было уделено вопросам защиты детей в информационном пространстве, так как именно они могут подвергаться различному негативному влиянию и требуют дополнительной защиты и внимания со стороны родителей.



**Министерство цифрового развития, инноваций и  
аэрокосмической промышленности  
Республики Казахстан**

**Комитет по информационной  
безопасности**

**РЕКОМЕНДАЦИИ**

**г.Нур-Султан  
2021**