# 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.

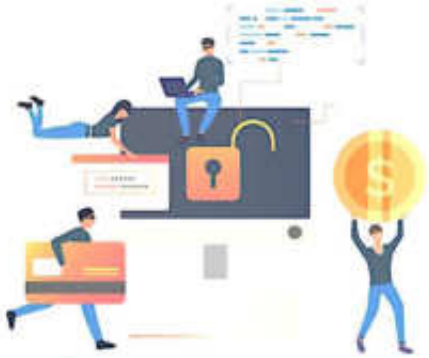
# ДОПОЛНИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ГОСУДАРСТВЕННЫХ СЛУЖАЩИХ

## 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;
- восможность 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.

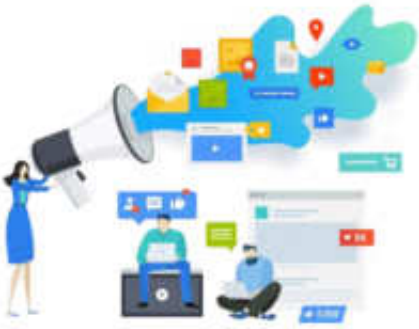
Кроме того,

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.

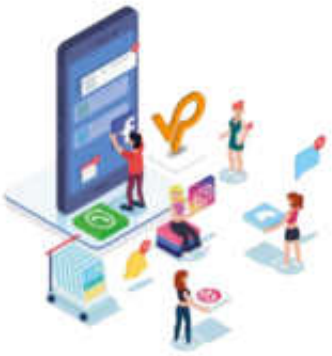
Это можно сделать, написав на электронный адрес kib@mdai.gov.kz, либо через портал «Электронного правительства» (раздел «Электронные обращения»), также можно написать на личный блог Председателя (https://dialog.egov.kz/blogs/3932160/welcome)



# 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:

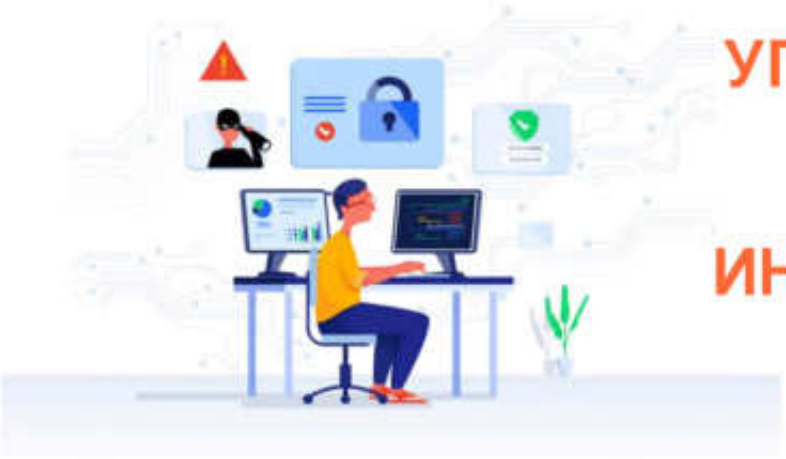
1)исключить передачу ЭЦП третьим лицам. В организациях нужно сотрудников, ответственных за подписание документов, наделить полномочиями и выдать им собственные электронные подписи. Для этого необходимо правовым актом руководителя организации передать право подписи соответствующему лицу и выпустить на 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»).



# 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