Министерство оборонной и аэрокосмической промышленности Республики Казахстан

Комитет по информационной безопасности

г. Астана, пр. Мәнгілік ел 8, «Дом министерств», 1 подъезд
тел.: +7 (7172) 74-99-80, e-mail: kib@mdai.gov.kz

Авторы-составители:
Абдикаликов Р.К., Атамкулов Б.Б.,
Голобурда Д.В., Мустагулов Т.С., Шаймергенов Т.Т.

МИНИСТЕРСТВО ОБОРОННОЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН

КОМИТЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РЕКОМЕНДАЦИИ

Вопросы обеспечения кибербезопасности

Уже более 20 лет информационные технологии ежедневно изменяют нашу жизнь: Интернет и мобильная связь стали основой для новых форм коммуникации, экономической активности и развлечений.

Новые технические возможности используются государственными органами для оптимизации своих процессов и предоставления гражданам более качественных услуг.

Термин «электронное правительство» охватывает многочисленные «онлайн» мероприятия и уже сделал ненужными многие посещения государственных учреждений.

Однако нельзя игнорировать одну основную потребность человека – необходимость обеспечения безопасности.

Особенно это относится к безопасности информации, поскольку эти угрозы почти всегда остаются незамеченными с первого взгляда и часто недооценивается. Для ее обеспечения требуются знания и действия каждого, лица вовлеченного в использование ИКТ. Все пользователи призваны быть столь же осторожными «онлайн», как и «оффлайн».

Важно минимизировать риски, чтобы сохранить возможности, предоставляемые информационными технологиями и Интернетом. Безопасность возможна только тогда, когда все участники вносят свой вклад.

Надеемся, что подготовленные Министерством в качестве органа по информационной безопасности рекомендации станут вкладом в повышение уровня безопасности ИКТ в Казахстане.

Подготовлено на основании социологического исследования «Осведомленность населения об угрозах кибербезопасности», проведенного в сентябре 2018 года

Термины и определения

Что такое Интернет?

Всемирная система объединенных компьютерных сетей для хранения и передачи электронных информационных ресурсов

Персональные данные это

Сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на **электронном** и (или) ином материальном носителе

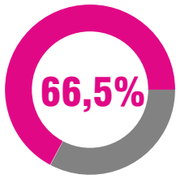
Под кибербезопасностью понимается

Состояние среды использования информационно-коммуникационных технологий, которое определяется уровнем защищенности информации в электронной форме (электронные информационные ресурсы, информационные системы и информационно-коммуникационная инфраструктура)

Почему важно поддерживать кибербезопасность?

#01

Сетевое пространство Интернета благодаря информационно-коммуникационным технологиям формирует качественно новую среду для передачи и распространения информации, удаленного оказания сервисов и услуг.



населения в Казахстане предпочитают получать интересующую информацию и услуги посредством Интернета, в том числе мобильного Интернета

#02

Взаимозависимость объектов (онлайн услуг и сервисов), нуждающихся в защите информации, может привести к «каскадному эффекту» в случае технологического сбоя или компьютерной атаки.

45,9%

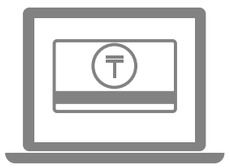
населения постоянно использует мобильные приложения для оплаты онлайн услуг

31,6%

населения регулярно пользуется порталом «Электронное правительство»

31,1%

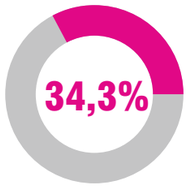
населения пользуется интернет-банкингом для получения банковских услуг



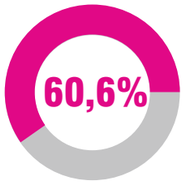
#03

Компьютерные атаки способны подорвать общественное доверие к онлайн-услугам и нанести вред экономике.

За последний год



казахстанцев подвергались кибер-атакам



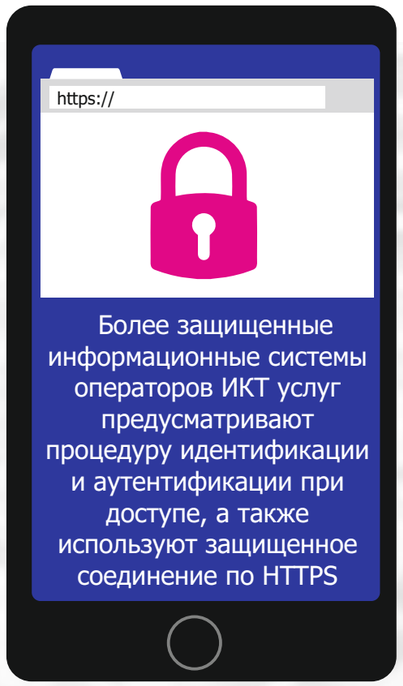
опрошенных специалистов в сфере IT сталкиваются с угрозами кибербезопасности в своей деятельности

В большинстве случаев компьютерные атаки становятся успешными из-за человеческой халатности и неосторожности.

Информационная безопасность базируется на обеспечении трех значимых для безопасности информации атрибутов:

Конфиденциальность информации	подразумевает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем.
Целостность информации	способность информации (данных) сохраняться в неискаженном виде. Неправомочные и не предусмотренные владельцем изменения информации приводят к нарушению целостности.
Доступность информации	определяется способностью информационной системы предоставлять своевременный беспрепятственный доступ к информации только идентифицированным субъектам.

Если есть возможность перейдите на двухфакторную аутентификацию, например по номеру сотового телефона через СМС-сообщение.



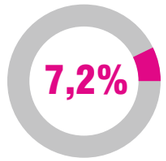
Более защищенные информационные системы операторов ИКТ услуг предусматривают процедуру идентификации и аутентификации при доступе, а также используют защищенное соединение по HTTPS

Идентификация – присвоение субъектам доступа к информационной системе или электронному ресурсу личного идентификатора, обеспечивающего установление подлинности и определение полномочий субъекта в информационной системе и регистрация действий в процессе сеанса.

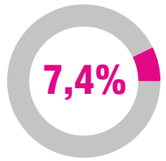
Аутентификация – это процесс проверки подлинности чего-либо. Примером аутентификации может быть сравнение пароля, введенного пользователем, с паролем, который сохранен в базе данных сервера. Подобная проверка может быть как односторонней, так и взаимной – все зависит от способа защиты и политики безопасности сервиса.

Угрозы безопасности данных

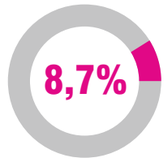
За последний год опрошенные казахстанцы подверглись следующим видам кибератак:



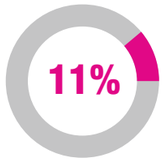
кибермошенничество с банковскими картами, другие виды кибермошенничества



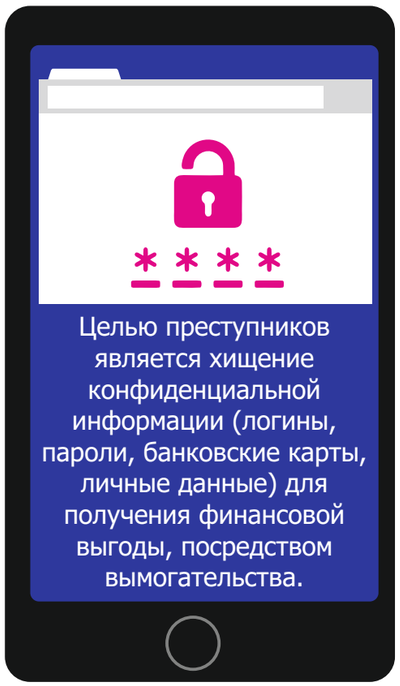
взлом аккаунтов в социальных сетях



атака вредоносных компьютерных вирусов и программ



вредоносный СПАМ



Вредоносное программное обеспечение (**malware** – сокращение от malicious software: **malicious** – злонамеренный и **software** – программное обеспечение) – представляют собой широкую категорию программного обеспечения – они устанавливаются без Вашего разрешения и влияют на работу Вашего компьютера.

По способу воздействия на информацию выделяют следующее вредоносное ПО:

- эксплоиты;
- логические бомбы;
- троянские и шпионские программы;
- компьютерные вирусы;
- сетевые черви.

Каким образом вредоносные программы проникают на компьютер пользователя?

Как это происходит?

Вредоносные программы, чаще всего, проникают на компьютер:

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

Методы распространения

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Тактика, которую используют злоумышленники, чтобы склонить пользователя к раскрытию конфиденциальной информации (направление писем с поддельными адресами с вредоносным вложением)

ФИШИНГ *(англ.phishing, от fishing – рыбная ловля, выуживание)*

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

РАСПРОСТРАНЕНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЧЕРЕЗ САЙТ

Получение злоумышленником несанкционированного доступа к файлам сайта или к разделу администрирования системы управления сайтом.

Какие последствия влечет заражение компьютера вредоносной программой?

Вредоносные программы влияют на нормальное функционирование системы, что может привести к отказу в обслуживании, блокированию, уничтожению, модификации и хищению данных, а также снижению пропускной способности сети.

Симптомами заражения вредоносной программой являются:

- снижение работоспособности системы;
- перенаправление запросов в браузере на нежелательные сайты;
- всплывающие окна.

Как защитить компьютер от вредоносных программ?

Что делать?

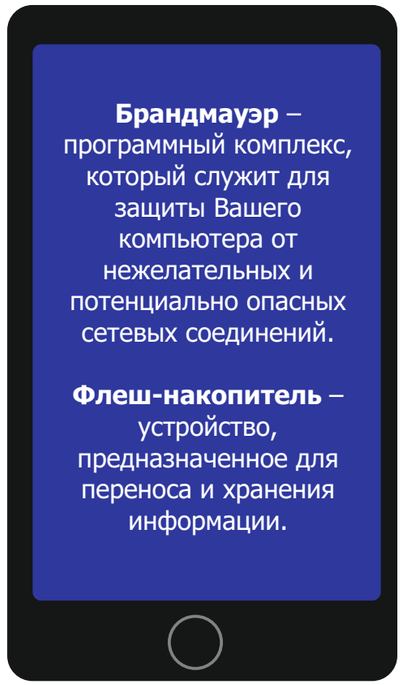
Вредоносные программы зачастую распространяются в приложении с другими файлами, так что не открывайте вложения электронной почты, отправленные с неизвестных Вам ресурсов.

#01 Никогда не отключайте встроенный брандмауэр операционной системы

Брандмауэр создает защитный заслон между вашим компьютером и Интернетом. Выключение брандмауэра даже на минуту увеличивает риск заражения ПК вредоносной программой.

55%

казахстанцев не пользуются антивирусом для своего компьютера



#02 Используйте антивирусное ПО для защиты Вашей системы от возможных онлайн-угроз. Установите антивирусные и антишпионские программы из надежных источников.

#03 Осторожно используйте флеш-накопители

Минимизируйте возможность заражения компьютера вредоносным ПО: не подключайте неизвестные флеш-накопители (или USB-накопители) в своему компьютеру.

37,6%

пользователей отметили, что при получении электронного письма от незнакомого человека с просьбой перейти по ссылке, отметили, что скорее всего перейдут по указанной ссылке

#04 Не принимайте файлы от незнакомых Вам пользователей, и особенно обращайте внимание на получаемые файлы с расширением EXE, COM, CMD.

#05 Не соглашайтесь на загрузку ПО, предлагаемую непроверенными Интернет-источниками

- Будьте очень внимательны, открывая вложенные файлы или нажимая на ссылки в электронной почте, мгновенных сообщениях или в публикациях в социальных сетях – даже если вы знаете отправителя. Позвоните ему и узнайте, он ли это сделал: если нет, удалите или закройте окно службы обмена мгновенными сообщениями.
- Загружайте программное обеспечение только на сайтах, которым Вы доверяете.
- Не переходите по ссылкам в сообщениях электронной почты и избегайте веб-сайтов, где предлагается бесплатное программное обеспечение с нарушением авторских прав. Остерегайтесь «бесплатных» загрузок музыки, игр, видео и всего прочего с малоизвестных сайтов и доменных зон (**.ws**, **.biz** и др.). Они могут содержать вредоносное программное обеспечение, как на самом сайте, так и в загружаемых файлах.

#06 Если вы столкнулись с навязчивой баннерной рекламой, всплывающими окнами

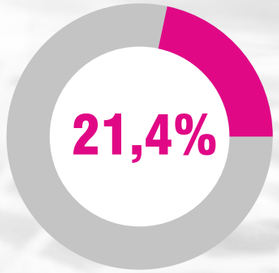
- Не нажимайте кнопки **«Согласен»**, **«ОК»**, **«Разрешить»**, **«Я принимаю»**, **«Загрузить»**, **«Продолжить»** и другие **«кнопки согласия» на дальнейшие действия** в баннерной рекламе, в неожиданных всплывающих окнах или предупреждениях, на сайтах, которые кажутся подозрительными, или в предложениях удалить шпионское ПО или вирусы.
- Нажмите **CTRL+F4** на клавиатуре, чтобы закрыть вкладку браузера.
- Если окно не закрывается, нажмите **Alt+F4** на клавиатуре, чтобы закрыть браузер.

Если вы подозреваете, что ваш компьютер заражен вредоносной программой

#07 Отключите устройство от Интернета для прекращения обработки информации, а также для того, чтобы избежать утечки информации (логинов, паролей и другой конфиденциальной информации).

69,6%

не знают или сомневаются куда могут обратиться и/или что делать в случае кибератаки, либо заражения компьютера вредоносной программой



опрошенных пользователей стараются использовать все возможные методы защиты информации

Профилактика информационной безопасности

Устаревшее или нелицензионное программное обеспечение является более уязвимым

#01

Регулярно устанавливайте обновления для всего вашего программного обеспечения – операционных систем, программ приложений, антивирусных и прочих программ

#02

Включайте функции автоматического обновления программного обеспечения, когда таковое доступно

#03

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

#04

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

#05

Регулярно создавайте копию важных для Вас данных на других устройствах

Parol123456#!&

надежные пароли должны состоять минимум из 8 символов и содержать сочетание букв, цифр и символов (!@#$%^&*)

****

никому не раскрывайте свои пароли, наиболее важные храните в зашифрованном виде

****

не используйте одинаковый пароль на всех сайтах. В случае утраты пароля, доступ к вашим данным будет облегчен

Home Wi-Fi Подключено

создавайте разные надежные пароли для модема и домашней беспроводной сети.
О том, как это сделать, прочтите в инструкции к устройству, либо узнайте в компании, представляющей модем, роутер, маршрутизатор

61,8%

пользователей не меняют своих паролей, либо меняют только когда забывают их

32,2%

пользователей использует одинаковые пароли в социальных сетях, аккаунтах, личных кабинетах

Рекомендации по безопасному «серфингу» в Интернете

#01

НАСТРОЙТЕ свои браузер для повышения степени защиты во время работы в Интернете (блокировщик рекламы и всплывающих окон, защита от отслеживания и др.)

#02

НЕ РАССКАЗЫВАЙТЕ в социальных сетях о своей жизни больше, чем нужно.

#03

НЕ ПОЛЬЗУЙТЕСЬ без особой необходимости общественными «Wi-Fi-точками» доступа в Интернет.

#04

ИЗБЕГАЙТЕ анонимных прокси-серверов (анонимайзеры). Через них Ваши данные будут доступны третьим лицам.

#05

УСТАНОВИТЕ менеджер паролей для хранения Ваших паролей в зашифрованном виде.

#06

ИСПОЛЬЗУЙТЕ сервисы оценки репутации сайтов и онлайн сканеры ссылок.

Сервисы оценки репутации сайтов и онлайн сканеры ссылок:

- **VirusTotal (https://www.virustotal.com)**
- **URLVoid (http://www.urlvoid.com/)**
- **2ip.ru (http://2ip.ru/site-virus-scaner)**
- **Web Inspector (http://siteinspector.comodo.com)**
- **Онлайн-сканер Dr.Web (http://vms.drweb.com/online)**
- **TrustOrg.com (http://trustorg.com/)**
- **Phishtank.com (http://www.phishtank.com/)**

опрошенных недооценивают значимость защиты персональных данных

казахстанцев не считают, что их персональные данные в безопасности

Важно знать!

Сбор, обработка персональных данных осуществляются собственником и (или) оператором с **СОГЛАСИЯ СУБЪЕКТА ИЛИ ЕГО ЗАКОННОГО ПРЕДСТАВИТЕЛЯ**, кроме случаев, предусмотренных законодательством.

Собственники и (или) операторы, а также третьи лица, получающие доступ к персональным данным ограниченного доступа, **ОБЕСПЕЧИВАЮТ ИХ КОНФИДЕНЦИАЛЬНОСТЬ** путем соблюдения требований не допускать их распространения без согласия субъекта или его законного представителя либо наличия иного законного основания.

Хранение персональных данных осуществляется собственником и (или) оператором, а также третьим лицом в базе, которая хранится на территории Республики Казахстан.

Собственник и (или) оператор базы, а также третье лицо обязаны принимать необходимые меры **ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**, обеспечивающие:

- предотвращение несанкционированного доступа к персональным данным;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить;
- минимизацию неблагоприятных последствий несанкционированного доступа к персональным данным.

Субъект персональных данных имеет право

#01 знать о наличии у собственника и (или) оператора базы, 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;

#02 требовать от собственника и (или) оператора базы изменения и дополнения своих персональных данных при наличии оснований;

#03 требовать от собственника и (или) оператора базы, а также третьего лица блокирования своих персональных данных в случае наличия информации о нарушении условий сбора, обработки персональных данных;

#04 требовать от собственника и (или) оператора базы, а также третьего лица уничтожения своих персональных данных, сбор и обработка которых произведены с нарушением законодательства Республики Казахстан, а также в иных случаях, установленных Законом РК «О персональных данных и их защите» и иными нормативными правовыми актами Республики Казахстан;

#05 отозвать согласие на сбор, обработку персональных данных, кроме случаев, предусмотренных пунктом 2 статьи 8 Закона РК «О персональных данных и их защите»;

#06 дать согласие (отказать) собственнику и (или) оператору базы на распространение своих персональных данных в общедоступных источниках персональных данных;

#07 на защиту своих прав и законных интересов, в том числе возмещение морального и материального вреда;

#08 на осуществление иных прав, предусмотренных Законом РК «О персональных данных и их защите» и иными законами Республики Казахстан.

Органы прокуратуры осуществляют высший надзор за соблюдением законности в сфере персональных данных и их защиты.

Использование ИКТ в профессиональной деятельности

опрошенных специалистов в сфере IT сталкиваются с угрозами кибербезопасности в своей деятельности

организаций опрошенных работников в сфере IT не имеют систему управления информационной безопасностью

#01

Работа с мобильными устройствами

Разработайте политику работы с мобильными устройствами и ознакомьте персонал для ее соблюдения. Примените базовый уровень безопасности для всех устройств. Защищайте данные как при передаче, так и во время их хранения.

#02

Обучение и осведомленность пользователей

Разработайте приемлемую политику безопасности пользователей и безопасного использования ваших систем. Включите в данную политику обучение персонала. Поддерживайте осведомленность персонала об угрозах информационной безопасности.

#03

Управление пользовательскими привилегиями

Установите эффективные процессы управления и ограничьте количество привилегированных пользователей. Ограничьте привилегии пользователей и осуществляйте мониторинг их деятельности. Контролируйте доступ к журналу событий.

#04

Правила использования съемных носителей

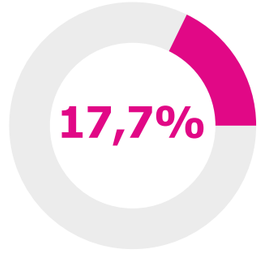
Создайте правила контроля доступа к съемным носителям. Ограничьте типы носителей и их использование. Перед подключением к корпоративной сети проверьте все носители на наличие вредоносных программ.

#05

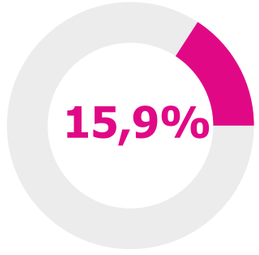
Безопасная конфигурация

Обновляйте систему безопасности и убедитесь, что поддерживается безопасная конфигурация всех систем. Контролируйте перечень устройств, подключенных и подключаемых к сети организаций.

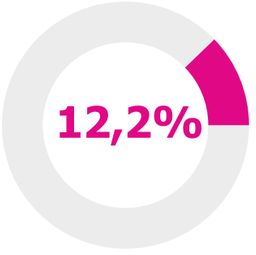
Использование ИКТ в профессиональной деятельности



используют межсетевые экраны



прибегают к шифрованию данных, каналов связи



пользуются DLP-системами

#06

Защита от вредоносных программ

Разработайте соответствующие политики и установите защиту от вредоносных программ в организации.

#07

Сетевая безопасность

Управляйте периметром сети. Защищайте сети от внешних и внутренних атак.

#08

Мониторинг

Разработайте стратегию мониторинга. Непрерывно проводите мониторинг всех систем и сетей. Анализируйте журнал событий в поисках активности, которая может указывать на события информационной безопасности. Осуществляйте мониторинг и тестирование элементов управления безопасностью.

#09

Управление инцидентами

Предусмотрите возможность резервирования и аварийного восстановления. Разработайте план реагирования на инциденты информационной безопасности.

#10

Взаимодействие

Сообщайте об инцидентах информационной безопасности в правоохранительные органы и специализированные организации.

Соблюдение стандартных мер может предупредить 80% атак, наблюдаемых сегодня.

Спросите себя

#01 Вы уверены, что Ваш брандмауэр активирован и защищает данные на Вашем компьютере?

#02 Кто имеет доступ к данным на Вашем компьютере из внутренней сети или удалено?

#03 Вы точно знаете, какие службы Вашей сети доступны через Интернет?

#04 Вам действительно известно каждое устройство Вашей сети, которое имеет внешний IP-адрес?

#05 Когда Вы в последний раз делали оценку риска или внешний тест на проникновение?

#06 Может ли злоумышленник проникнуть в Вашу сеть?

РЕКОМЕНДАЦИЯ

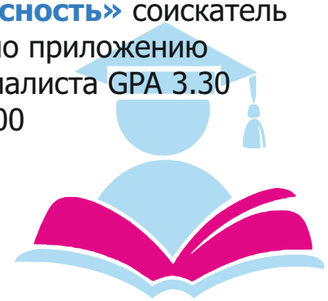
руководителям организаций, учреждений, предприятий, специалистам-профессионалам по безопасности информационной инфраструктуры и информационных технологий, а также учащимся высших учебных заведений!

Центр международных программ «Болашак»

Предоставляет приоритетные гранты для прохождения академического обучения (магистратура, докторантура), научных и производственных стажировок в ведущих компаниях и университетах мира.

Для прохождения **стажировки по специальности «информационная (кибер) безопасность»** соискатель должен иметь стаж работы не менее 3-х лет, включая последние 12 месяцев в выбранной области специализации.

Для прохождения **обучения (магистратура, докторантура) по специальности «информационная безопасность»** соискатель должен иметь средний балл по приложению диплома бакалавра или специалиста GPA 3.30 (из 4.00/4.33) либо 4.30 из 5.00



Подробная информация:

bolashak.gov.kz

KZ-CERT

При подозрении на заражение компьютера вредоносным программным обеспечением обращайтесь в Службу реагирования на компьютерные инциденты по бесплатному единому короткому номеру:
1400, +7 (7172) 55-99-97,
либо по электронной почте:
incident@kz-cert.kz

ГОРЯЧАЯ ЛИНИЯ

по противодействию противоправному контенту, пропагандирующий терроризм, экстремизм, порнографию, культ жестокости и насилия в Казахстане:

сайт: **safekaznet.kz**
телефон: **+7 (7272) 73-24-63**,
электронная почта: **report@iak.kz**

ВЫ МОЖЕТЕ ПРОВЕСТИ ОЦЕНКУ СВОЕГО ИНТЕРНЕТ-РЕСУРСА

с помощью отечественной системы **WebTotem** на интернет-ресурсе:

webtotem.kz

КОМИТЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Миссия – достижение и поддержание уровня защищенности электронных информационных ресурсов от внешних и внутренних угроз, обеспечивающие устойчивое развитие Республики Казахстан

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

Государственный контроль и профилактика соблюдения Единых требований

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

Содействие в формировании **профессиональных стандартов**

Повышение **осведомленности граждан** об угрозах информационной безопасности

Участие в реализации **образовательных программ**

Формирование Перечня и мониторинг **критически важных объектов** информационно-коммуникационной инфраструктуры

Проведение **аттестации и испытаний информационных систем** на соответствие требованиям информационной безопасности

При подготовке рекомендаций были использованы нормативные правовые акты:

- Закон РК «Об информатизации»;
- Закон РК «О связи»;
- Закон РК «О персональных данных и их защите»;
- Закон РК «Об электронном документе и электронной цифровой подписи»;
- ППРК «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».