МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, ИННОВАЦИЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН

КОМИТЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕР-БЕЗОПАСНОСТИ

РЕКОМЕНДАЦИИ

ПОЧЕМУ ВАЖНО ПОДДЕРЖИВАТЬ КИБЕРБЕЗОПАСНОСТЬ?

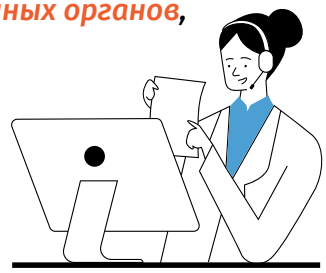
Подготовлено на основании социологического исследования

«ОСВЕДОМЛЕННОСТЬ НАСЕЛЕНИЯ ОБ УГРОЗАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КИБЕРБЕЗОПАСНОСТИ)»

проведенного в сентябре 2020 года

Обеспечение информационной безопасности и защита персональных данных является важной составляющей частью работы уполномоченного органа в лице Комитета по информационной безопасности.

“В Глобальном индексе кибербезопасности (GCI) Казахстан стремительно улучшает свою позицию. Например, в последнем отчете Казахстан поднялся сразу на *42 пункта — до 40-го места.* Это *результат совместной работы государственных органов*, неправительственных организаций и бизнеса.”



НЕМНОГО ВАЖНОЙ ИНФОРМАЦИИ

Информационная безопасность является неотъемлемой частью нашей жизни. Под информационной безопасностью подразумевают, как правило, соблюдение трех важных принципов:

Конфиденциальность

Доступность

Целостность

Что это такое?

- *Доступ к информации должен быть только у того, кто имеет на это право.*
- *Информация должна быть доступна в любой момент, когда она нужна.*
- *Информация должна быть достоверной.*

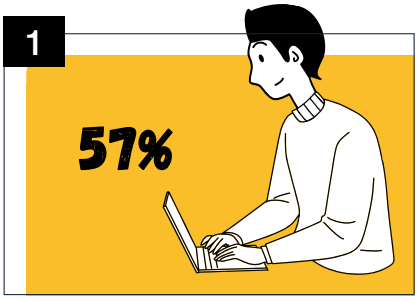
Нарушение одного из принципов может привести к нарушению других.

УГРОЗЫ БЕЗОПАСНОСТИ ДАННЫХ

Информационная безопасность в сфере информатизации (Кибербезопасность) **– состояние защищенности электронных информационных ресурсов, информационных систем и информационно – коммуникационной инфраструктуры от внешних и внутренних угроз.**

РЕЗУЛЬТАТЫ СОЦИОЛОГИЧЕСКОГО ОПРОСА ПОКАЗЫВАЮТ:

1

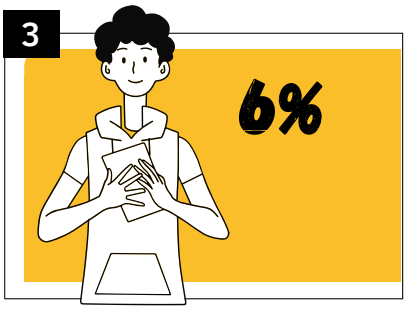


Большинство респондентов получают информацию посредством интернета

2

Посредством телевизора и интернета

3



Посредством мобильных приложений

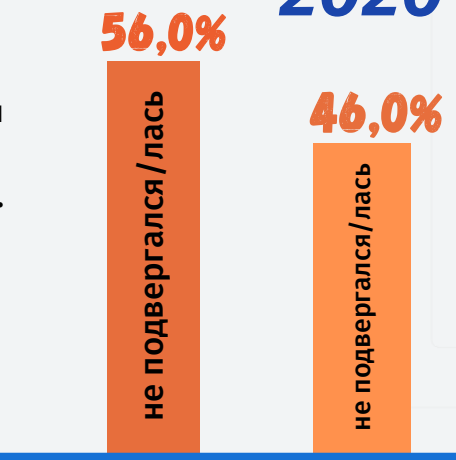
КАКИМ ВИДАМ КИБЕРАТАК ВЫ ПОДВЕРГАЛИСЬ ЗА ПОСЛЕДНИЙ ГОД ?

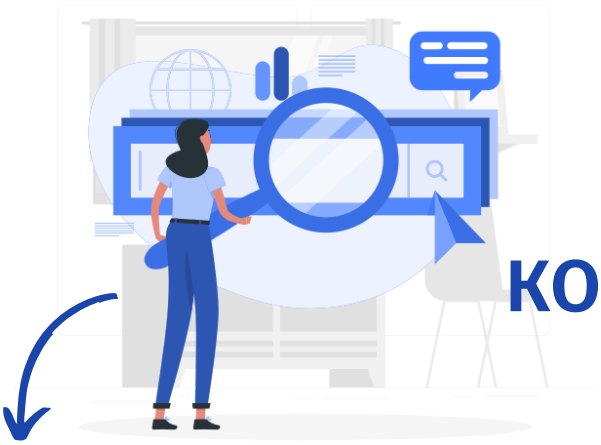
Согласно опросу, за последний год население страны подвергалось следующим видам кибератак:

	2020	2019	2018
Атака компьютерных вирусов	32.1%	8.1%	8.7%
Вредоносный спам	13.4%	12.1%	11%
Взлом аккаунтов в социальных сетях	3.9%	6.7%	7.4%

ПОДВЕРГАЛИСЬ ЛИ ВЫ КИБЕРАТАКАМ?

По итогам опроса 2020 года 46% респондентов ответили, что они не подвергались кибератакам. В сравнении с прошлым годом данный показатель немного ниже. Так, в 2019 году 56% опрошенных отметили, что случаев кибератак у них не было.





ИСПОЛЬЗУЕТЕ ЛИ ВЫ СРЕДСТВА ОТ КОМПЬЮТЕРНЫХ АТАК?

ПО ДАННЫМ 2019 ГОДА ВСЕГО 36% ИСПОЛЬЗОВАЛИ ЛИЦЕНЗИОННЫЕ ПРОДУКТЫ

Информационная безопасность является одним из основных задач в обеспечении защиты данных, в том числе персональных, и её повышение требует, по мнению респондентов, принятия мер.

ПРОФИЛАКТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«ПЕРЕХОДИТЕ ЛИ ВЫ ПО ПРИСЛАННЫМ ССЫЛКАМ ОТ НЕЗНАКОМЫХ В СОЦИАЛЬНЫХ СЕТЯХ?»

Результаты социального опроса показывают:

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

63,3% – Проверка сайта осуществляется иногда, когда ресурс вызывает какие-либо сомнения.

Процентов респондентов проверяют информацию о сайтах редко. – **27,3%**

5,3% – Процентов респондентов не проверяют вообще.

РЕКОМЕНДАЦИИ

Профилактика информационной безопасности (рекомендации)

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

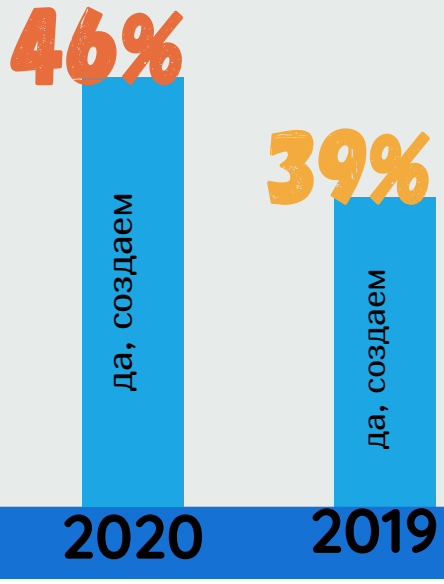
Включайте функцию автоматического обновления программного обеспечения, когда таковое доступно.

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

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

Регулярно создавайте копию важных для Вас данных на других устройствах.

В 2019-2020 годах резервные копии на устройствах хранения информации создавали 39% и 46% респондентов, соответственно.



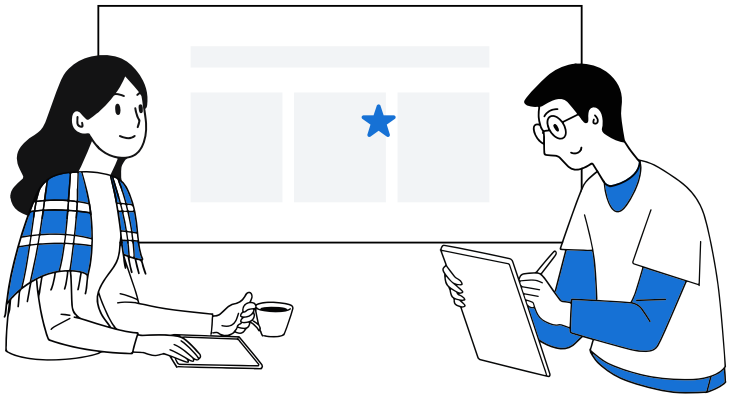
СОЗДАЕТЕ ЛИ ВЫ РЕЗЕРВНЫЕ КОПИИ ВАЖНЫХ ДЛЯ ВАС ДАННЫХ?

Резервное копирование- это надежный способ хранения данных, подразумевающий процедуру создания копии данных на устройствах хранения информации.

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

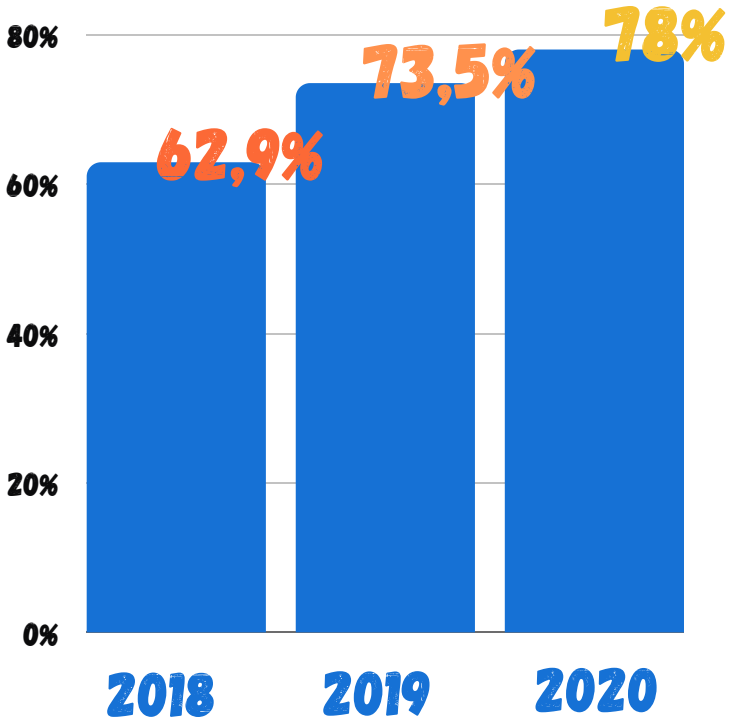
- -обращение к IT-специалисту — **73,5%**
- -обращение в уполномоченный орган в сфере обеспечения информационной безопасности — **4,8%**
- -самостоятельное устранение последствия кибератаки — **1,6%**
- -не обращение никуда — **1,5%**

При любых нестандартных или при подозрении на нарушения информационной безопасности:
-незамедлительно обратитесь к ответственным специалистам;
-также можно обратиться в службу реагирования на компьютерные инциденты по номеру телефона:
1400 или
+7 (7172) 55-99-97,
эл.почта:
info@kz-cert.kz



ОПРОС:

ОСВЕДОМЛЕННОСТИ НАСЕЛЕНИЯ ОБ УГРОЗАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Данный показатель осведомленности за 2018 и 2019 годы составил 62,9% и 73,5%, соответственно. Это говорит о том, что осведомленность населения в 2020 году увеличилась на 15% и 4,5% по сравнению с 2018 и 2019 годами.

КИБЕРБЕЗОПАСНОСТЬ

Методические рекомендации разработаны с целью обеспечения реализации образовательными организациями системы мероприятий, направленных на обучение учащихся правилам безопасного поведения в интернет пространстве

26,3% **01**

Использование лицензионного антивирусного программного обеспечения

22,7% **02**

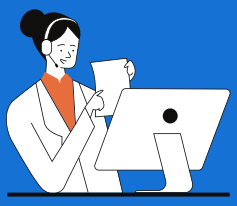
Неиспользование одинакового пароля на всех сайтах

12,8% **03**

Периодическое изменение пароля

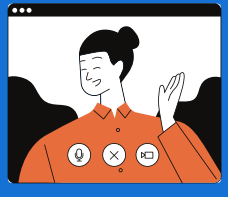
9,8% **04**

Не раскрытие паролей



9,7% **05**

Неиспользование нелицензионного программного обеспечения



РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ

01 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.

02 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.

03 АНТИВИРУСНОЕ ПРОГРАММНОЕ 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.

04 СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- ✗ Запрещается сообщать третьим лицам IP-адреса и сочетание логина и пароля.
- ✗ Запрещается устанавливать самостоятельно программное обеспечение.

ДОПОЛНИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ГОССЛУЖАЩИХ

05 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 и сроки сбора персональных данных;
- возможность передачи третьим лицам собранных персональных данных;
- трансграничная передача данных.

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

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. Обращения можно подавать любым удобным и доступным способом.

НОВЫЕ РЕКОМЕНДАЦИИ В СВЯЗИ С ПАНДЕМИЕЙ

Удаленный доступ

Использовать удаленный доступ в сеть организации строго с двухфакторной аутентификацией.

Права

Сегментировать сети и разделить права доступа. Желательно, чтобы даже удаленная активность пользователей покрывалась периметровыми средствами защиты организации.

Проверка

Проверить все сервисы и оборудование, которые используются для удаленного доступа, на наличие обновленных микропрограмм и патчей безопасности. Другим вариантом является доступ к данным сервисам только через VPN, защищенный двухфакторной аутентификацией.

Терминальный доступ

При работе с домашних компьютеров рекомендуется использовать терминальный доступ к корпоративным информационным системам или виртуальные рабочие места со всеми установленными средствами защиты информации.

Почта

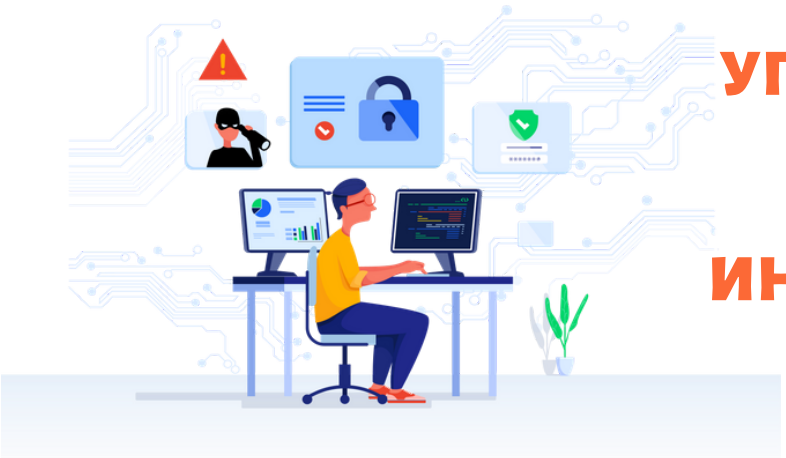
Проверить, что электронная почта защищена двухфакторной аутентификацией. Кроме того, необходимо внедрить решение по работе с электронной почтой для отправки «сомнительных» писем в изолированную среду для детонации вредоносного кода (песочница).

Удаленные действия

Проверить наличие и срок ведения журналов удаленных действий пользователей, а также наличие таймаута неактивного удаленного подключения с требованием повторной аутентификации.

Сторонние сервисы

Не использовать для доступа в корпоративную сеть сторонние сервисы, которые подключаются через промежуточные сервера и самостоятельно проводят авторизацию и аутентификацию.



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.

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 2020 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 граждан об угрозах информационной безопасности.

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.

РАЗДЕЛ ДЛЯ ПРОФЕССИОНАЛОВ

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

10 ШАГОВ ПО СНИЖЕНИЮ РИСКОВ КИБЕР-УГРОЗ

1 Разработка политики информационной безопасности

Это первичный документ организации - Ваша конституция в сфере информационной безопасности. Но кроме конституции нужны законы. Такие законы называются "Документы второго уровня" и детализируют требования политики. 86,1% респондентов не используют стандарты безопасности данных.

ВАЖНО!

Организации должны иметь подразделение по информационной безопасности или ответственного сотрудника за информационную безопасность, обособленного от подразделения, занимающегося вопросами создания, сопровождения и развития объектов информатизации.

2 Просвещение и осведомленность пользователей

Разработать программу подготовки персонала. Внедрить систему обучения всех сотрудников нормам информационной безопасности. Поддерживать осведомленность пользователей о кибер-рисках. 31,4% респондентов считают, что осведомлены об угрозах информационной безопасности.

3 Управление инцидентами

Необходимы меры: регистрация событий информационной безопасности , управления инцидентами ИБ, уведомление ответственных об инцидентах ИБ, регистрация инцидентов ИБ в Службе реагирования на компьютерные инциденты АО «Государственная техническая служба» КНБ РК. 73,5% респондентов намерены обращаться к IT-специалистам.

4 Управление рисками

Нужно разработать Руководство или Методику оценки рисков информационной безопасности. Вы должны знать, что угрожает Вашей организации. 62,8% респондентов иногда, когда ресурс вызывает какие-либо сомнения проверяют информацию о сайтах, на которых они авторизуются.

5 Управление привилегиями пользователей

Установить процессы управления учетными записями и ограничить количество привилегированных учетных записей. Ограничить привилегии пользователя и контролировать действия пользователя. Контроль доступа к деятельности и журналам регистрации событий.

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 маркетинга, вспомогательную политику. Постоянный мониторинг всех систем и сетей информационно-коммуникационных технологий. 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

Установка актуальной защиты (лицензионный антивирус) от вредоносных программ и их постоянное обновление. 32,1% респондентов подвергались атакам компьютерных вирусов, 13,4% - вредоносного спама.

10 Сетевая безопасность

Защита сети от внутренних и внешних угроз. Управление периметром сети. Ограничить несанкционированный доступ и вредоносное содержимое. Мониторинг и тестирование элементов управления безопасности. 61,1% респондентов считают, что их персональные данные в полной безопасности.

КУДА ОБРАЩАТЬСЯ ПРИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТАХ?

Служба реагирования на компьютерные инциденты по короткому номеру телефона: 1400 или +7 (7172) 55-99-97,
электронная почта: info@kz-cert.kz

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

ОБРАБОТКА СЛЕДУЮЩИХ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

В компетенцию службы реагирования на компьютерные инциденты входит обработка следующих компьютерных инцидентов с целью их выявления и нейтрализации:

- **Захват паролей и другой аутентификационной информации**
- **Несанкционированный доступ к информационным ресурсам**
- **Взлом систем защиты информационных сетей**
- **Распространение вредоносного ПО, незатребованной корреспонденции (спама)**
- **Сканирование информационных сетей и хостов**
- **Атаки на узлы сетевой инфраструктуры и серверные ресурсы**

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, ИННОВАЦИЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН

КОМИТЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РЕКОМЕНДАЦИИ

г.Нур-Султан-2020 г.