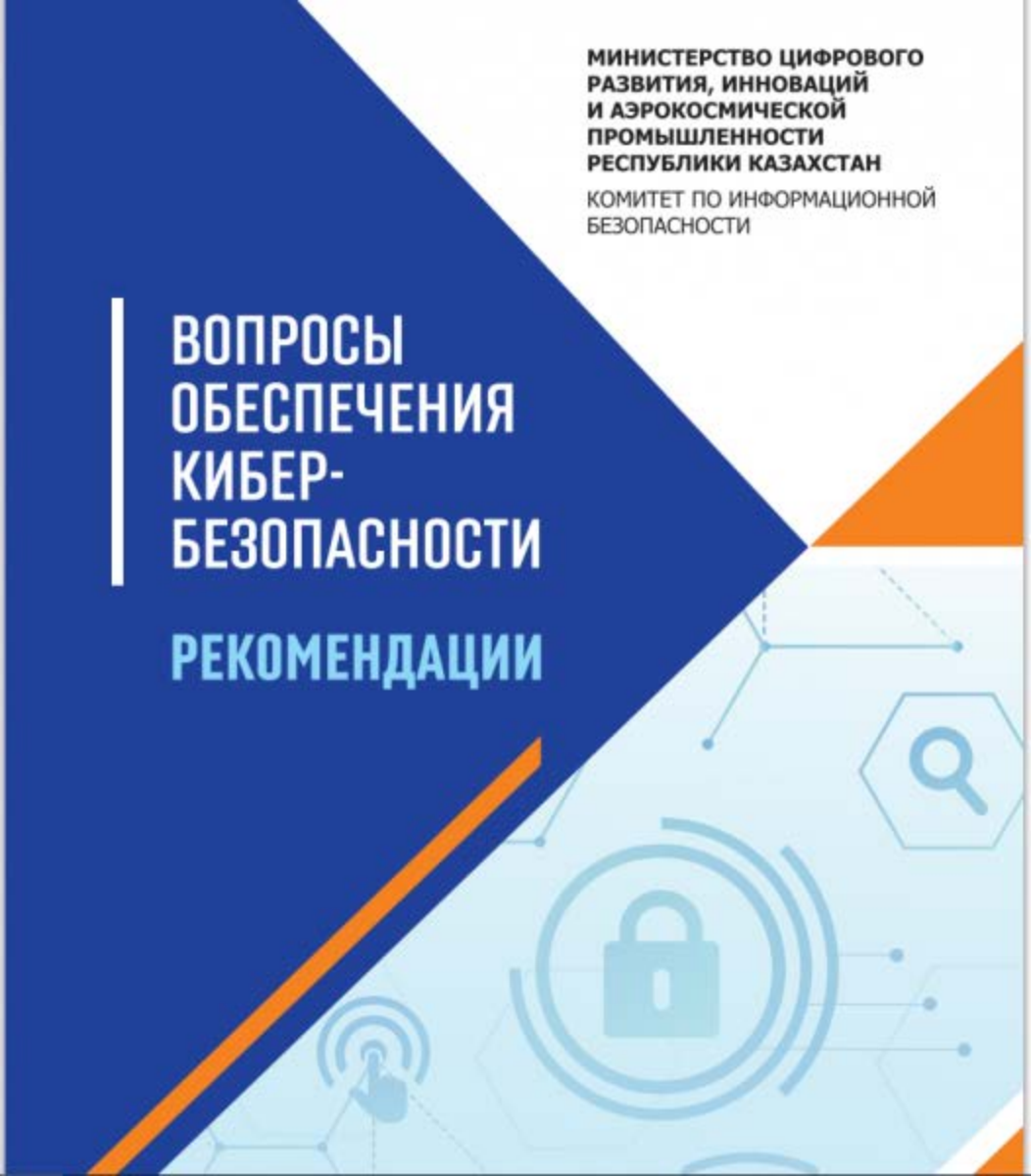
МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, ИННОВАЦИЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН

КОМИТЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕР-БЕЗОПАСНОСТИ

РЕКОМЕНДАЦИИ



ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕР-БЕЗОПАСНОСТИ

РЕКОМЕНДАЦИИ

Подготовлено на основании социологического исследования

«ОСВЕДОМЛЕННОСТЬ ОБ УГРОЗАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»,

проведенного в сентябре 2019 года

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 занимает в нём 40-е место. Отметим, что ещё в прошлом году наша страна находилась на 42 пункта ниже, занимая 82 место.

НЕМНОГО ВАЖНОЙ ИНФОРМАЦИИ

Информационная безопасность становится важной частью нашей повседневной жизни. Обычно, под информационной безопасностью 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 заполучил плохой человек.*

41,4% опрошенных граждан Республики Казахстан считают, что их персональные данные находятся в полной безопасности.

33,6% респондентов придерживаются диаметрально противоположной точки зрения.

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,

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – это соблюдение Конфиденциальности, Доступности, Целостности.

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

Опрошенные казахстанцы подвергались кибер-атакам

в 2018 году **33,9%**

в 2019 году **29,8%**

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕР-БЕЗОПАСНОСТИ

РЕКОМЕНДАЦИИ

подвергались ли вы за последний год кибер-атакам?

	2018 год	2019 год
Вредоносный СПАМ	11%	12,1%
Атака вредоносных компьютерных вирусов и программ	8,7%	8,1%
Взлом аккаунтов в социальных сетях	7,4%	6,7%
Кибермошенничество с банковскими картами	7,2%	2,5%

КАК ИЗБЕЖАТЬ НЕПРИЯТНОСТЕЙ?

15,5% пользователей не используют антивирус и не используют защиту паролем.

7 шагов к личной информационной безопасности

Киберугрозы, хакеры, вирусы, троянские кони.

Всё непонятно и запутанно?
Не пугайтесь. Защитите себя и своих близких! Мы покажем Вам путь. Путь к информационной безопасности 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.

что делать?

Самое надёжное – спрятать Ваше ЭЦП в надёжное хранилище. Таким хранилищем является электронный чип, что установлен во всех удостоверениях личности нового образца граждан Республики Казахстан. При получении ЭЦП попросите записать ЭЦП на удостоверение личности. Но есть и сложности при использовании удостоверения личности как хранилища ЭЦП. Вам будет нужно специальное устройство – кард-ридер. Это устройство часто выдают клиентам банков, оно позволяет подключать удостоверение личности или банковские карточки к компьютеру. Зато это надёжно.

Также можно воспользоваться специальным хранилищем, которое называется «токен». Он часто похож на обычную флэшку, но является самым настоящим сейфом для ЭЦП.

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

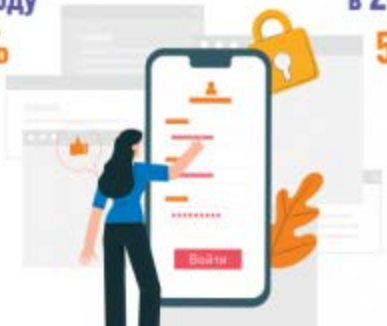
ваш щит - ваш пароль

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 Вами навсегда. Или которое легко вспомнить. Нужно воспользоваться самыми большими участками нашего мозга, отвечающими за: СЛУХ и ЗРЕНИЕ.

Пользователи не меняющие пароли, либо меняют только когда забывают их:

в 2018 году
61,8%

в 2019 году
53,5%



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: *Zelenyi_kaktus*

Пользователи составляющие сложные пароли:

в 2018 году **23,3%**

****

в 2019 году **30,6%**

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!

Никогда не передавайте свои пароли другим людям. Даже если попросят.

шаг 3

электронная почта

К сожалению, мошенники давно поняли, что мы читаем отправленные нам письма. Значит, если написать хитрое письмо, нас можно обмануть. Например, были популярны «нигерийские письма счастья». В таких письмах некий «адвокат из Нигерии» (страна могла быть любой, но впервые письма приходили из Нигерии, отсюда и название мошенничества) заявлял, что Вы стали наследником громадного наследства. Вам нужно просто выслать небольшую сумму ему на счёт «на оформление бумаг». Деньги, как правило, исчезают, а наследство никто не получает.

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.

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.

47% 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 придумать 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. Антивирусы 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 тяжелые последствия. Мы всегда задаём вопрос 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

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

Пользователи, использующие антивирус:

в 2018 году
32,9%

в 2019 году
36%

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, нестыковки, 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 пальцам 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 заимствование – 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.

что не нужно делать!

Использовать контрафактное (пиратское) программное обеспечение. 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.

Социальные сети могут быть источником излишней информации о Вас.

53,6% опрошенных граждан, имеющих страницы в социальных сетях, выкладывают информацию о своей жизни.

39,5% казахстанцев пользуются электронной почтой и личным аккаунтом для авторизации на сайтах.

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 специального 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.

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.

46,5% пользователей никогда не используют общественные «Wi-Fi точки».

47,5% анкетируемых подключаются к Интернету через доступные беспроводные каналы.

шаг 7

Резервное копирование

Информация может исчезнуть. И не обязательно Вас атаковали злые хакеры. Просто потеряли телефон или сгорел жёсткий диск компьютера.

52,3% казахстанцев не создают резервные копии важных данных

38,7% анкетируемых занимаются созданием резервных копий.

Хранят информацию:

39,7% на компьютере 

31,5% на флэш-накопителе 

20,2% в облачных сервисах 

89,7% анкетируемых не знают, кто может использовать их персональные данные и в каких целях.

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. Назвался опытным пользователем – соответствуй.

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.

МЫ И ГОСУДАРСТВО. КУДА ОБРАЩАТЬСЯ

При любых нестандартных ситуациях или при подозрении на нарушение кибербезопасности – незамедлительно обратитесь к ответственным специалистам и в

KZ-CERT

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

Закон об информатизации – Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК. **Закон регулирует общественные отношения в сфере информатизации, возникающие на территории Республики Казахстан между государственными органами, физическими и юридическими лицами при создании, развитии и эксплуатации объектов информатизации, а также при государственной поддержке развития отрасли информационно-коммуникационных технологий**. Внесены изменения и дополнения согласно Закону Республики Казахстан от 28 декабря 2017 года № 128-VI ЗРК.

Единые требования (ЕТ) – единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности. Утверждены постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832. Определяют требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности. **Положения ЕТ, относящиеся к сфере обеспечения информационной безопасности, обязательны для применения государственными органами, местными исполнительными органами, государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных**

электронных информационных ресурсов, а также собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры.

Киберщит Казахстана – концепция кибербезопасности. Концепция кибербезопасности ("Киберщит Казахстана") разработана в соответствии с Посланием Президента Республики Казахстан "Третья модернизация Казахстана: Глобальная конкурентоспособность" с учетом подходов Стратегии "Казахстан-2050" по вхождению Казахстана в число 30-ти самых развитых государств мира. **Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий**.

УПОЛНОМОЧЕННЫЙ ОРГАН В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Указом Президента Республики Казахстан от 6 октября 2016 года № 350 образован Комитет по информационной безопасности Министерства оборонной и аэрокосмической промышленности Республики Казахстан.

ПОЛНОМОЧИЯ КОМИТЕТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Разработка мер в сфере обеспечения информационной безопасности;
- Государственный контроль в сфере обеспечения информационной безопасности;
- Методологическое обеспечение и стандартизация.

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 (ET)пункт 33.

Важно! обязательно утвердите документ: «правила использования мобильных устройств и носителей информации». У 56% опрошенных специалистов в организации есть отдельный сотрудник, отвечающий за кибербезопасность.

2. **Просвещение и осведомленность пользователей.** Разработать программу подготовки персонала. Внедрить системы обучения всех сотрудников нормам информационной безопасности. Поддерживать осведомленность 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, регистрации инцидентов ИБ в Службе реагирования на компьютерные инциденты Государственной

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 пользователя и контролировать действия пользователя. Контроль доступа к 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.

42,8% **опрошенных специалистов имеют в организации систему мониторинга информационной безопасности.**

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.

43,3% **специалистов применяют единые (государственные) требования.**

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

Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан

Комитет по информационной безопасности

г. Нур-Султан, пр. Мәңгілік ел 8, «Дом министерств»
тел.: +7 (7172) 74-99-80, сайт Комитета: www.isdp.mdai.gov.kz