РГП на ПХВ «РЦЭЗ» МЦРИАП РК и РГП на ПХВ «ННЦРЗ им.Салидат Каирбековой» МЗ РК

ОСНОВЫ КИБЕРГИГИЕНЫ

Астана, 2024 год

СОДЕРЖАНИЕ

ЧТО ТАКОЕ КИБЕРГИГИЕНА?

представляет собой набор действий, выполняемых пользователями компьютеров и других устройств для повышения сетевой безопасности и обеспечения работоспособности системы

это образ мышления и привычки с акцентом на безопасность, помогающие пользователям и организациям снизить количество нарушений при работе в интернете, повысить сетевую безопасность и обеспечить работоспособность системы

КИБЕРГИГИЕНА

Защита личных данных

Пользователи сети должны быть внимательны к тому, какую информацию о себе они раскрывают в интернете, чтобы избежать ее попадания в неправильные руки. Это включает в себя не только избегание предоставления конфиденциальной информации

Предотвращение кибератак

предотвращение кибератак, таких как вирусы, хакерские атаки, фишинг и другие формы онлайн-угроз. Это включает в себя использование антивирусного программного обеспечения, установку обновлений безопасности для программного обеспечения и операционных систем, а также обучение пользователям о методах защиты от различных видов киберугроз

Обеспечение безопасности онлайн-транзакций

использование безопасных методов онлайн-платежей, защиту банковских данных и мониторинг финансовых активов для выявления подозрительной активности

Под информационной безопасностью подразумевают соблюдение трех важных принципов:

КОНФИДЕНЦИАЛЬНОСТЬ

Доступ к информации должен быть только у того, кто имеет на это право. А у кого нет права, тому доступ к информации закрыт.

ДОСТУПНОСТЬ

Информация должна быть доступна в любой момент, когда она нужна. Сразу и быстро

ЦЕЛОСТНОСТЬ

способность информации (данных) сохраняться в неискаженном виде. Неправомочные и не предусмотренные владельцем изменения информации (в результате ошибки оператора или преднамеренного действия неуполномоченного лица) приводят к нарушению целостности.

РИСКИ ИБ ДЛЯ ПОДРЫВА РЕПУТАЦИИ

- НЕДОСТУПНОСТЬ РЕСУРСА
  Социальная напряженность общественности
- ПАРОЛЬНАЯ ПОЛИТИКА
  Утечка информации
- ДОСТУП К АДМИНИСТРАТИВНОЙ ПАНЕЛИ
  Распространение ложной информации
- УТЕЧКА ПОСРЕДСТВОМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ
  Доступ к конфиденциальным данным ГО
- ВЗЛОМ АККАУНТОВ СОЦСЕТЕЙ
  Невозможность восстановления

РИСКИ ИБ ДЛЯ ПОДРЫВА РЕПУТАЦИИ

ПАРОЛЬНАЯ ПОЛИТИКА

- Простые пароли
- Не используется двухфакторная аутентификация
- Повтор пароля (gmail, mail)
- Привязка корпоративной почты к персональным соцсетям и подобным сервисам
- Не закрытие сессии на постороннем компьютере
- Брутфорс (подбор паролей)

ФИШИНГ

- Переход по нелегитимным ссылкам
- Открытие непроверенных файлов
- Отсутствие СЗИ (Средство защиты информации)

УТЕЧКА ДАННЫХ

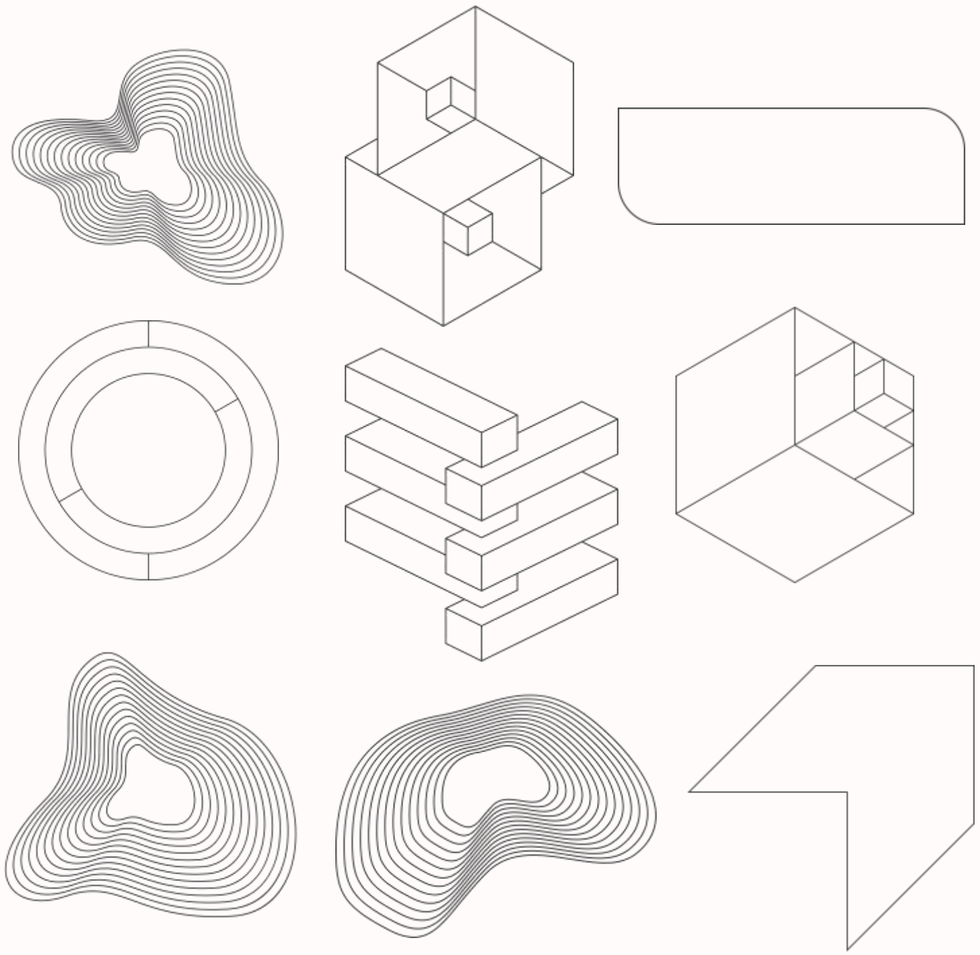
- Незащищённый публичный Wi-Fi
- Загрузка ВПО
- USB
- Фото документов, отправляющихся через мессенджер
- Скачивание на посторонний компьютер баз данных
- Личный Wi-Fi со слабым паролем

Правила использования Интернет и электронной почты

При использовании сети Интернет сотруднику запрещено:

- использовать предоставленный МЗ РК доступ Интернет в личных целях;
- разглашать присвоенное им имя пользователя и пароль;
- предоставлять доступ в Интернет с выделенного для этих целей СВТ другим сотрудникам или посторонним лицам;
- использовать специализированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- передавать конфиденциальную информацию, за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным с применением средств криптографического преобразования;
- передавать информацию, защищенную авторскими или другим правами, без разрешения владельца.

Правила использования Интернет и электронной почты



При использовании сети Интернет сотруднику запрещено:

- передавать вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому ПО и ПО для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию;
- просматривать видео (кинофильмы и т.п.) через личные страницы социальных сетей и Интернет каналов, а также совершать/посещать следующие сайты:
  - онлайн-игры;
  - торренты;
  - онлайн-радио и телевидение.

Правила использования Интернет и электронной почты

При использовании электронной почты сотрудникам МЗ РК запрещается:

- открытие и прочтение писем, сохранение и запуск вложений в электронные письма, поступивших с неизвестных или сомнительных адресов (при необходимости такие вложения выгружаются на внешний носитель и проверяются на наличие вирусов на компьютере, не подключенном к локальной сети);
- использование бесплатных почтовых служб, а также использование электронной почты в личных, не связанных с выполнением служебных обязанностей, целях;
- использование личных почтовых ящиков для рабочих коммуникаций и/или использование одного общего ящика на множество сотрудников;

Правила использования Интернет и электронной почты

При использовании электронной почты сотрудникам МЗ РК запрещается:

- использование публичных Wi-Fi сетей без применения средств VPN для доступа к корпоративной почте МЗ РК;
- передавать электронные сообщения:
- содержащие конфиденциальную информацию, если способ передачи не является безопасным;
- информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца;
- информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также осуществить несанкционированный доступ, а также ссылки на вышеуказанную информацию;
- переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей;

Правила использования Интернет и электронной почты

При использовании электронной почты сотрудникам МЗ РК запрещается:

по собственной инициативе (без указания руководителя) осуществлять рассылку (в том числе и массовую) электронных сообщений (если рассылка не связана с выполнением служебных обязанностей);

использовать адрес электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением служебных обязанностей;

предоставлять другим сотрудникам МЗ РК сотрудникам и третьим лицам доступ к своему электронному почтовому ящику;

перенаправлять электронные сообщения с личных почтовых ящиков на корпоративный без служебной необходимости;

разглашать данные учетной записи электронной почты.

РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ

Используйте лицензионное программное обеспечение.
Обновляйте программные продукты своевременно

Никогда не открывайте самозапускаемые файлы.
Пример: .exe , .com , .cmd , .msi , .bat
Файлы вложений с такими расширениями открывать нельзя!

Никогда не отправляйте ЭЦП в открытом виде по электронной почте.
Никогда не копируйте свое ЭЦП на незнакомые компьютеры.
Не храните свое ЭЦП на компьютере.

РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ

4

Не скачивайте и не открывайте подозрительные файлы и не переходите по ссылкам от непроверенных источников

5

Не отправляйте копии своих документов, содержащие личные данные, удостоверение личности, данные банковских карт и т.п

6

Проводите регулярное резервное копирование данных

7

Не доверяйте общественным WI-FI точкам и не вводите свои аутентификационные данные через незащищенные беспроводные сети

8

Регулярно проверяйте ПК на наличие вредоносных файлов

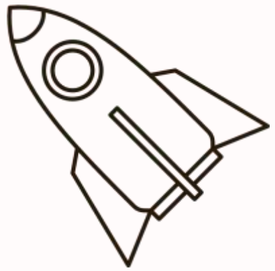
9

Используйте двухфакторную аутентификацию

ХРАНЕНИЕ ПАРОЛЕЙ В БЕЗОПАСНОСТИ

Не использовать один и тот же пароль для нескольких учетных записей

Использовать пароли длиной не менее 12 символов



Регулярно менять пароль.

Менять установленные по умолчанию пароли на устройствах интернета вещей

Использовать пароли, в состав которых входят заглавные и строчные буквы, символы и цифры

Не записывать пароли и не сообщать их другим людям.

Защита от атак социальной инженерии

- Не переходить по подозрительным ссылкам, в которых вы не уверены.
- Не открывать письма, выглядящие подозрительно.
- Не загружать подозрительные вложения в сообщения электронной почты и текстовые сообщения, которых вы не ждете.
- Не переходить по объявлениям, обещающим бесплатные деньги, призы и скидки.

Спасибо за внимание!