Подписано цифровой подписью: Пальчук М.И.
DN: cn=Пальчук М.И., o=ГБПОУ РК "Романовский колледж индустрии гостеприимства", ou=Директор, email=043@crimeaedu.ru, c=RU
Дата: 2023.05.16 10:02:32 +03'00'

УТВЕРЖДАЮ
Директор
ГБПОУ РК «РКИГ»
_____ Пальчук М. И.
Приказ № 38 от 09.03.2023 г.

Анкета тестирования пользователей СКЗИ

Заполняется персонально пользователем СКЗИ

Фамилия, Имя, Отчество	Структурное подразделение

Для корректного заполнения просьба отметить один или несколько вариантов ответа

1. Сколько процентов из общего объема нарушений и преступлений составляют ошибки персонала?
    a) 4%;
    b) 19%;
    c) 20%;
    d) >50%.

2. Кто входит в состав системы обеспечения информационной безопасности?
    a) сотрудники подразделения информационной безопасности;
    b) сотрудники Казначейства;
    c) все сотрудники ГБПОУ РК «РКИГ», имеющие прямое или косвенное отношение к системе.

3. Имеет ли право пользователь использовать предоставленные ему ресурсы ГБПОУ РК «РКИГ» в личных целях?
    a) да;
    b) нет;
    c) иногда.

4. Что должен сделать пользователь, если он оказался свидетелем порчи имущества ГБПОУ РК «РКИГ»?
    a) попытаться исправить испорченное имущество;
    b) попытаться предотвратить порчу имущества;
    c) незамедлительно сообщить непосредственному руководителю о произошедшем;
    d) не придавать этому значения.

5. Какие операции не имеет право производить пользователь с аппаратно-программными средствами, выданными ему ГБПОУ РК «РКИГ» для исполнения своих служебных обязанностей?

a) вскрытие системного блока ЭВМ (для протирания пыли), мыши, клавиатуры;
b) добавление в аппаратную часть ЭВМ дополнительных плат для увеличения производительности ЭВМ;
c) исполнение своих служебных обязанностей;
d) инсталляция сторонних программ на ЭВМ;
e) внесение изменений в настройки аппаратной части ЭВМ, программных продуктов, установленных на ЭВМ.

6. Что должен сделать пользователь при обнаружении вирусного заражения ЭВМ?
   a) обновить базы антивируса, произвести проверку компьютера и удалить вирус;
   b) прекратить обработку информации на компьютере;
   c) сообщить в подразделение информационной безопасности, эксплуатирующей систему;
   d) перезагрузить компьютер;
   e) выключить компьютер и отсоединить от сети.

7. Что должен сделать пользователь при временном уходе с рабочего места?
   a) убрать в недоступное место записанные на бумаге пароли;
   b) завершить работу всех открытых приложений;
   c) заблокировать экран нажатием клавиш Ctrl-Alt-Del + Enter;
   d) выключить компьютер;
   e) ключевой носитель убрать в запираемое и опечатываемое хранилище.

8. Какие пользователи допускаются к самостоятельной работе с СКЗИ?
   a) все пользователи ГБПОУ РК «РКИГ»;
   b) нуждающиеся в СКЗИ для исполнения своих служебных обязанностей;
   c) прошедшие обучение правилам работы с СКЗИ;
   d) сдавшие зачеты по программе обучения правилам работы с СКЗИ.

9. Какие обстоятельства относятся к компрометации ключей?
   a) утеря ключевого носителя с последующим обнаружением;
   b) утеря ключевого носителя;
   c) временное оставление ключевого носителя без присмотра;
   d) нарушение печатей на сейфе с ключевыми носителями;
   e) утеря ключей от сейфа, в котором хранятся ключевые носители.

10. Как должен действовать пользователь СКЗИ при утере ключевого носителя с последующим обнаружением в случае, когда нельзя достоверно установить, что произошло с ключевым носителем?
    a) незамедлительно поставить в известность о факте компрометации ключей администратора безопасности;
    b) самостоятельно произвести генерацию новых ключей ЭП, поставив в известность банк о факте компрометации;
    c) продолжить работу с найденными ключами.

11. Как обеспечить стойкий и легко запоминающийся пароль?

a) использовать парольные фразы;
b) придумать длинный пароль, но не менее 8-и символов;
c) выборочно заменить буквы спецсимволами;
d) добавить спецсимволы в начале (в середине, в конце);
e) использовать ассоциации;
f) использовать личные данные (ФИО, кличка собаки, марку машины, название улицы и пр.).

12. Какая ответственность предусмотрена законодательством РФ за нарушения правил работы с конфиденциальной информацией?
a) уголовная;
b) административная;
c) ответственность не предусмотрена.

13. Какая ответственность предусмотрена Уголовным кодексом РФ пользователю за разглашение коммерческой тайны?
a) штраф в размере до 1 млн. руб.;
b) штраф в размере до 80 000 руб.;
c) лишение свободы до двух лет;
d) лишение свободы до трех лет.

14. Ключевые носители ("флешки", "таблетки" и т.п.), содержащие действующие ключи ЭП, используемые для подписания платежных документов, разрешается:
a) передавать работникам других департаментов;
b) передавать сотрудникам службы технической поддержки;
c) временно (в процессе генерации новых ключей ЭП) передавать сотрудникам службы технической поддержки;
d) временно (в процессе генерации новых ключей ЭП) передавать сотрудникам службы информационной безопасности;
e) Ничего из вышеперечисленного. Ключевые носители, содержащие действующие ключи ЭП, запрещается передавать другим лицам.

15. Допускается сообщать пароль для доступа к ключевым носителям, содержащим действующие ключи ЭП, и используемым для подписания документов:
a) работникам других департаментов;
b) сотрудникам службы технической поддержки;
c) временно (в процессе генерации новых ключей ЭП) сотрудникам службы технической поддержки;
d) временно (в процессе генерации новых ключей ЭП) сотрудникам службы информационной безопасности;
e) Ничего из вышеперечисленного. Пароль запрещается разглашать другим лицам.

16. В случае потери ключевого носителя, содержащего действующие ключи ЭП:
a) сообщить сотрудникам ГБПОУ РК «РКИГ» для генерации новых ключей ЭП;
b) сообщить сотрудникам службы технической поддержки для генерации новых ключей ЭП;

c) направить администратору безопасности сообщение о компрометации ключей ЭП.

17. В случае обнаружения после потери своего ключевого носителя, содержащего действующие ключи ЭП:
    a) сообщить сотрудникам ГБПОУ РК «РКИГ» для генерации новых ключей ЭП;
    b) сообщить сотрудникам службы технической поддержки для генерации новых ключей ЭП;
    c) продолжить использование данного ключевого носителя без генерации новых ключей ЭП;
    d) направить администратору безопасности сообщение о компрометации ключей ЭП.

18. Свой ключевой носитель, содержащий действующие ключи ЭП, и используемый для подписания документов разрешается временно передавать для работы:
    a) сотрудникам ГБПОУ РК «РКИГ»;
    b) сотрудникам службы технической поддержки;
    c) администратору безопасности;
    d) только своему коллеге по подразделению;
    e) ничего из вышеперечисленного. Ключевой носитель, содержащий действующие ключи ЭП, нельзя передавать другим лицам к ним не допущенным.

19. На ключевой носитель, содержащий действующие ключи ЭП, и используемый для подписания документов разрешается записывать файлы:
    a) если они содержат служебные документы по профилю работы;
    b) если есть свободное место на ключевом носителе, и они содержат служебные документы по профилю работы;
    c) нельзя записывать, даже если они содержат служебные документы по профилю работы.

20. Каким образом осуществляется пересылка конфиденциальных сведений ГБПОУ РК «РКИГ»?
    a) в открытом виде с использованием личных почтовых ящиков, зарегистрированных на внешних (сторонних) серверах;
    b) с помощью защищенных с использованием шифровальных (криптографических) средств систем;
    c) возможны оба варианта.

21. Какие требования предъявляются к хранению ключевых носителей, содержащих электронную подпись?
    a) ключевые носители хранятся в спецпомещениях, убранными в опечатанные хранилища;
    b) ключевые носители хранятся в спецпомещении, в ящике рабочего стола, закрытыми на ключ;

c) ключевые носители хранятся в спецпомещении на рабочем столе пользователя;
d) ключевые носители хранятся на связке обычных ключей.

22. Какие виды ответственности предусмотрены законодательством РФ для лиц, виновных в нарушении требований по защите конфиденциальной информации?
    a) ответственность не предусмотрена;
    b) дисциплинарная: расторжение трудового договора по инициативе работодателя;
    c) уголовная: 7 лет лишения свободы, штраф до 1 млн. руб.;
    d) уголовная: штраф 500 000 руб.;
    e) административная: штраф 30 000 руб., приостановление деятельности организации на срок до 90 суток.

Подпись _____

Дата _____

Результаты проверки

Всего ответов _____(кол-во)

Правильных ответов _____(кол-во)

Зачтено/не зачтено

Проверил

Ведущий специалист по защите информации А. О. Грибенников