Приложение 12
к приказу директора
ГБПОУ КК УТМиПТ
от 27.03.2024 г. № 66

ПАМЯТКА
пользователя информационных систем государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Пользователь автоматизированного рабочего места (персонального компьютера) содержит предоставленное ему автоматизированное рабочее место (далее – АРМ) и другую вычислительную и оргтехнику в хорошем техническом, гигиеническом и технологическом состоянии, следит за чистотой на компьютерном рабочем месте, не допускает наличие пыли на компьютерном оборудовании, вокруг него и под ним, уделяя особое внимание бесперебойности его работы.
2. Каждый работник, обеспеченный АРМ, получает аутентификационную информацию (персональное сетевое имя (имя пользователя), пароль), адрес электронной почты (в случае необходимости).
3. После получения доступа к информационной системе пользователь при первом входе в систему должен сменить пароль доступа (в случае наличия технической возможности) на пароль, удовлетворяющий требованиям Политики использования аутентификационной информации при доступе к информационным ресурсам и системам государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация). Также смена пароля должна осуществляться в случае его компрометации.
4. Пользователь не должен допускать многократного ввода неправильного пароля и блокировки своих учётных записей.
5. Пользователь обязан следить за сроком действия паролей и своевременно производить их смену, а в случае отсутствия технической возможности – обращаться к Администратору информационных систем.
6. Пользователь обязан хранить в секрете персональные пароли доступа к информационным активам и не передавать их другим лицам (за исключением случаев, предусмотренных Политикой использования аутентификационной информации при доступе к информационным ресурсам и системам образовательной организации).
7. Хранение пользователем аутентификационной информации (хранящейся на носителе) допускается только в личном сейфе (запираемом шкафу, ящике). При этом носитель должен быть упакован в отдельный опечатанный конверт.

8. Работа с информационными ресурсами (системами) пользователям разрешена только на закреплённых за ними АРМ, в определенное время и только с разрешённым программным обеспечением и сетевыми ресурсами.

9. Самостоятельная установка и (или) обновление пользователем программного обеспечения на АРМ запрещена. Установка и удаление любого программного обеспечения производится только ответственными сотрудниками.

10. Самостоятельное изменение пользователем аппаратной конфигурации АРМ, а также подключение к АРМ мобильных устройств передачи информации (сотовые телефоны, usb-модемы, и прочее) запрещено. Изменение (модификация) аппаратной конфигурации АРМ производится только ответственными сотрудниками.

11. Самостоятельное изменение пользователем состава локально-вычислительной сети (подключение/отключение АРМ, подключение/ отключение коммутаторов, маршрутизаторов, сетевых модемов) запрещено. Изменение состава локально-вычислительной сети осуществляется уполномоченными сотрудниками.

12. АРМ подлежат опечатыванию/опломбированию. Опечатывание осуществляется ответственными сотрудниками. Пользователь АРМ обязан следить за сохранностью данных пломб и в случае их нарушений сообщать о данном факте администратору информационной безопасности.

13. При необходимости отлучиться от АРМ, пользователь обязан, во избежание осуществления несанкционированного доступа к ресурсам АРМ, принудительно заблокировать АРМ посредством функционала операционной системы или используемого средства защиты информации от несанкционированного доступа.

14. Пользователь не должен каким-либо образом препятствовать функционированию (в том числе обновлению) средства защиты информации и принимать попытки по их деактивации.

15. Пользователь обязан обеспечить резервное копирования служебных данных, располагающихся на своих АРМ, вне сетевых файловых хранилищ. Резервное хранение таких данных осуществляется только на учтённые съёмные носители информации.

16. Пользователю АРМ запрещается:

16.1 подключать и отключать электропитание АРМ и другой вычислительной и оргтехники без ведома уполномоченных лиц;

16.2 включать в компьютерную сеть электропитания бытовые электрические приборы, а также другое электрооборудование, не относящееся к вычислительной и оргтехнике, ЛВС;

16.3 использовать носители информации, имеющие видимые повреждения, либо не проверенные на наличие вирусов;

16.4 загромождать АРМ и другую вычислительную и оргтехнику посторонними предметами;

16.5 располагать системный блок в недоступных для обслуживания местах, в местах с плохим воздухообменом, а также в местах, способствующих запылению и перегреву вентилирующих устройств;

16.6 использовать для принтеров и многофункциональных устройств помятую или не предназначенную для них бумагу;

16.7 допускать попадание влаги и посторонних предметов в монитор, системный блок АРМ, принтер, многофункциональное устройство, клавиатуру, манипулятор мышь;

16.8 выполнять чистку включённых АРМ и оргтехники, чистить АРМ и оргтехнику моющими средствами, не предназначенными для этих целей (спиртом, ацетоном, бензином и другими);

16.9 открывать системный блок АРМ или разбирать какое-либо оборудование, относящееся к вычислительной технике, оргтехнике и ЛВС;

16.10 нарушать гарантийные пломбы (наклейки) на компьютере, мониторе, принтере, многофункциональном устройстве и любом другом компьютерном или сетевом оборудовании.

17. Передача пользователем файлов как внутри образовательной организации, так и во внешние информационные системы производится с использованием учтённых съёмных носителей информации, а также посредством общих папок, средств электронной почты. Иные способы передачи запрещены.

18. Порядок использования электронной почты:

18.1. Пользователь имеет право на просмотр либо иное использование в интересах образовательной организации сообщений служебной электронной почты, которые направлены ему или получены им, соответственно с его адреса или на его адрес электронной почты.

18.2. Любые сообщения служебной электронной почты могут быть прочитаны, использованы в интересах образовательной организации, либо удалены уполномоченными на это сотрудниками.

18.3. При работе с электронной почтой пользователь должен учитывать следующие принципиальные положения:

18.3.1 электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;

18.3.2 электронная почта не является средством передачи информации, обеспечивающим конфиденциальность передаваемой информации. Передачу конфиденциальной информации вне локальной сети необходимо осуществлять только в зашифрованном виде;

18.3.3 электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

18.4. Пользователю запрещено вести частную переписку с использованием средств служебной электронной почты (к частной переписке относится переписка, не связанная с исполнением сотрудником своих должностных обязанностей). Использование служебной электронной почты для частной переписки сотрудником, является нарушением трудовой дисциплины.

18.5. Пользователю запрещается использовать сторонние сервисы электронной почты (yandex.ru, gmail.com и другие).

18.6. Пользователю запрещается использование своего адреса электронной почты для подписки на рассылки и другие сервисы, а также при

регистрации на любых сайтах, расположенных в сети интернет, если они прямо не связаны с должностными обязанностями сотрудника.

18.7. В целях повышения уровня безопасности при работе со служебной электронной почтой при получении входящей корреспонденции:

18.7.1 необходимо избегать перехода по ссылкам, содержащимся во входящих электронных сообщениях, полученных из недостоверных источников;

18.7.2 открывать вложения электронной почты, полученные из недостоверных источников;

18.7.3 проверять адреса отправителей электронной почты с целью предотвращения подделки адреса отправителя путём замены адреса на схожий, но с подменными символами (например, путём замены букв цифрами – замена «ivanov@mail.ru» на «ivanov@ma1l.ru», где вместо буквы «i» используется цифра «1»);

18.7.4 проверять ссылки на интернет-ресурсы в целях предотвращения подделки адреса Интернет-ресурса путём замены адреса на схожий, но с подменными символами (например, путём замены букв цифрами – замена «www.google.com» на «www.g00gle.com», где вместо буквы «о» используется цифра «0»);

18.7.5 проверять расширения вложенных файлов, при этом особое внимание следует обращать на так называемые «исполняемые файлы» с расширением «.exe», «.js», «.cmd», «.bat».

18.7.6 использование личных мобильных устройств (планшеты, сотовые телефоны) пользователем возможно только для доступа к сервисам служебной электронной почты. Использование мобильных устройств, для иных целей (доступа к информационным активам) запрещено.

19. Порядок работы в сети Интернет:

19.1. Доступ к сети Интернет предоставляется пользователю только в целях выполнения им своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам и (или) повышения эффективности выполнения ими своих служебных обязанностей.

19.2. Пользователю запрещается:

19.2.1 использовать предоставленный доступ в сеть Интернет в личных целях;

19.2.2 использовать специализированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет.

19.2.3 публиковать, загружать и распространять материалы, содержащие конфиденциальную информацию, за исключением случаев, когда это входит в служебные обязанности, и способ передачи является безопасным и заранее согласован с администратором информационной безопасности;

19.2.4 публиковать, загружать и распространять информацию, полностью или частично защищённую авторскими или другим правами, без разрешения владельца;

19.2.5 публиковать, загружать и распространять вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа;

19.2.6 публиковать, загружать и распространять серийные номера к коммерческому программному обеспечению и программное обеспечение для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию;

19.2.7 публиковать, загружать и распространять материалы, содержащие угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправных действий и так далее;

19.2.8 обращаться к ресурсам сети интернет, содержащим развлекательную (в том числе музыкальные, видео, графические и другие файлы, не связанные с производственной деятельностью), эротическую или порнографическую информацию;

19.2.9 использование анонимных прокси-серверов;

19.2.10 фальсификация (попытки фальсификации) своего IP-адреса, а также прочей служебной информации.

20. Порядок использования съёмных носителей информации.

20.1. Под съёмными носителями информации понимаются оптические диски, флэш-накопители, внешние накопители на жёстких дисках и иные устройства хранения информации.

20.2. Под использованием съёмных носителей информации понимается их подключение к инфраструктуре АРМ и серверам с целью приёма/передачи информации.

20.3. Допускается использование только учтённых носителей информации, которые являются собственностью образовательной организации и подвергаются регулярной ревизии и контролю.

20.4. Хранение съёмных носителей информации должно осуществляться в сейфах, запираемых металлических шкафах.

20.5. Пользователь обязан:

20.5.1 использовать носители информации исключительно для выполнения своих служебных обязанностей;

20.5.2 обеспечивать физическую безопасность носителей информации всеми разумными способами.

20.6. При использовании съёмных носителей информации запрещено:

20.6.1 использовать носители информации в личных целях;

20.6.2 передавать носители информации другим лицам;

20.6.3 оставлять съёмные носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

20.7. Любое взаимодействие (обработка, приём/передача информации) с информационными системами посредством использования неучтённых (личных) носителей информации, рассматривается как несанкционированное

(за исключением случаев, заранее оговорённых и согласованных с администратором информационной безопасности).

21. Пользователь должен обеспечивать меры, исключающие ознакомление посторонних лиц с защищаемой информацией. Такими мерами являются:

21.1 размещение мониторов, исключающее или существенно затрудняющее просмотр отображаемой информации;

21.2 размещение документации на бумажных носителях, содержащих служебную информацию, исключающее просмотр информации на них (документация убирается в папки, ящики тумбочек/столов либо переворачивается лицевой стороной вниз, либо накрывается сверху непрозрачными объектами, закрывающими область текста).

22. Пользователь должен осуществлять проверку получаемой и передаваемой информации на предмет наличия компьютерных вирусов и другого вредоносного программного обеспечения.

23. Пользователь должен обеспечивать содействие членам комиссии по обеспечению информационной безопасности в ходе проведения аудита, а также сторонним организациям, проводящим аттестацию информационных систем по требованиям безопасности информации.

24. Пользователь должен информировать администратора информационной безопасности о следующих инцидентах информационной безопасности и событиях безопасности информации (имеющих признаки инцидента):

24.1 компрометация пароля;

24.2 нарушение пломбы АРМ;

24.3 сбои в работе средств защиты информации;

24.4 вирусное заражение;

24.5 хищение/утрата носителя информации;

24.6 нарушение установленных политик безопасности и так далее.

25. Пользователь должен выполнять указания администратора информационной безопасности.

26. Пользователь должен незамедлительно предоставлять АРМ администратору информационной безопасности, администратору информационного ресурса (системы) для контроля, а также в экстренных случаях (нестабильность в работе ЛВС, угроза вирусного заражения, несанкционированного доступа к информации).

Приложение 1
к Памятке пользователя
информационных систем

ЛИСТ ОЗНАКОМЛЕНИЯ
с Памяткой пользователя информационных систем государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

Подписывая настоящий лист ознакомления с Памяткой пользователя информационных систем государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация), я подтверждаю факт ознакомления с Политиками и Правилами образовательной организации по обеспечению защиты информации (в том числе защите персональных данных), в следующем составе:

Политика использования информационных активов государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий».

Политика антивирусной защиты информации государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий».

Политика использования аутентификационной информации при доступе к информационным ресурсам и системам государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий».

Политика обеспечения отказоустойчивости информационных систем государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий».

Политика аудита информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»;

Политика управления событиями безопасности информации государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий».

Политика использования средств криптографической защиты информации государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий».

Политика сетевой безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий».

Правила обработки персональных данных в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Успенский техникум механизации и профессиональных технологий».

Правила рассмотрения запросов субъектов персональных данных или их представителей в в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Успенский техникум механизации и профессиональных технологий»..

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий».

Правила доступа в помещения государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий», в которых ведётся обработка защищаемой информации, в том числе персональных данных.

Обязуюсь исполнять требования указанных выше Политик и Правил в части, меня касающейся.

№ п/п	Ф.И.О., должность	Дата ознакомления	Подпись
1	2	3	4
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			

№ п/п	Ф.И.О., должность	Дата ознакомления	Подпись
1	2	3	4
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			
36.			
37.			
38.			

№ п/п	Ф.И.О., должность	Дата ознакомления	Подпись
1	2	3	4
39.			
40.			
41.			
42.			
43.			
44.			
45.			
46.			
47.			
48.			
49.			
50.			
51.			
52.			
53.			
54.			
55.			
56.			
57.			
58.			
59.			
60.			
61.			
62.			
63.			
64.			

№ п/п	Ф.И.О., должность	Дата ознакомления	Подпись
1	2	3	4
65.			
66.			
67.			
68.			
69.			
70.			
71.			
72.			
73.			
74.			
75.			
76.			
77.			
78.			
79.			
80.			
81.			
82.			
83.			
84.			
85.			
86.			
87.			
88.			
89.			
90.			