МИНИСТЕРСТВО ОБРАЗОВАНИЯ И
НАУКИ ХАБАРОВСКОГО КРАЯ

КРАЕВОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
**«КОМСОМОЛЬСКИЙ-НА-АМУРЕ
КОЛЛЕДЖ ТЕХНОЛОГИЙ И СЕРВИСА»**

ПРИКАЗ

25.10.2024 № 255 -ОД

Об обеспечение информационной безопасности персональных данных

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» в целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приложение №1)
2. Руководителю отдела сопровождения дистанционного образования и информатизации учебного процесса обеспечить выполнение Мер по обеспечению безопасности персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных (далее - «Меры по обеспечению безопасности персональных данных»).
3. Заместителю директора по АХР осуществлять общий контроль за организацией выполнения Мер по обеспечению безопасности персональных данных в Колледже.
4. Признать утратившим силу приказ директора Колледжа от 09.01.2019 года № 02-ОД.
5. Контроль за исполнением приказа оставляю за собой

Приложение:

1. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Директор колледжа Г.А. Горбунова

Приложение №1
к приказу директора КГБ ПОУ ККТиС
от 25.10.2024 . № 255 -ОД

СОСТАВ И СОДЕРЖАНИЕ
организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

№ п/п	Меры по обеспечению безопасности персональных данных	Организационно-технические мероприятия	Примечание
1.	Идентификация и аутентификация субъектов доступа и объектов доступа	Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).	
2.	Управление доступом субъектов доступа к объектам доступа	Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.	
3.	Ограничение программной среды	Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.	
4.	Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных)	Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.	
5.	Регистрация событий безопасности	Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.	

6.	Антивирусная защита	Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.	
7.	Обнаружение (предотвращение) вторжений	Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.	
8.	Контроль (анализ) защищенности персональных данных	Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.	
9.	Обеспечение целостности информационной системы и персональных данных	Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.	
10.	Обеспечение доступности персональных данных	Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.	
11.	Защита среды виртуализации	Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры),	

		сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.	
12.	Защита технических средств	Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.	
13.	Защита информационной системы, ее средств, систем связи и передачи данных	Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.	
14.	Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них	Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.	
15.	Управление конфигурацией информационной системы и системы защиты персональных данных.	Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.	

И.о. Руководителя отдела СДО и ИУП И.И. Задоя