

СОГЛАСОВАНО
Советом трудового коллектива
ГБПОУ МО «Колледж «Подмосковье»
Протокол заседания
совета
от «_05_» __06__ 2024__г. №_10_

УТВЕРЖДАЮ
Директор ГБПОУ МО
«Колледж «Подмосковье»
_____ А.В. Юдина
«_05_» __06__ 2024г.

ПОЛОЖЕНИЕ

О службе компьютерного обеспечения
Государственного бюджетного профессионального образовательного учреждения
Московской области
«Колледж «Подмосковье»

1. Общие положения

- 1.1. Служба компьютерного обеспечения является структурным подразделением государственного бюджетного профессионального образовательного учреждения Московской области «Колледж «Подмосковье» (далее – Колледж)
- 1.2. Службу компьютерного обеспечения возглавляет руководитель службы, назначаемый на должность и освобождаемый от должности директором Колледжа. Руководитель службы несет персональную ответственность за выполнение возложенных на службу функций.
- 1.3. Структура и штатная численность службы утверждается в соответствии со структурой и штатным расписанием Колледжа.

2. Основные функции и задачи

- 2.1. Создание и техническая поддержка электронно-библиотечной системы и электронной информационно-образовательной среды Колледжа.
- 2.2. Контроль работы серверного оборудования и техническое обслуживание компьютеров и оргтехники.
- 2.3. Сопровождение работы электронного документооборота.
- 2.4. Информационное обеспечение и сопровождение учебного процесса.
- 2.5. Профилактические работы на сервере и рабочих станциях.
- 2.6. Установка, настройка, техническое сопровождение и обслуживание (формирование заказ на закупку при необходимости)
 - серверов;
 - активного сетевого оборудования;
 - аппаратных и программных средств защиты информации;
 - аппаратных и программных средств контроля и управления сетевой инфраструктурой;
 - средств резервного копирования и восстановления данных;
 - периферийного оборудования;
 - программного обеспечения;
 - офисной техники.
- 2.7. Координация работ с поставщиками и производителями вычислительной и офисной техники по вопросам гарантийного обслуживания и ремонта.
- 2.8. Своевременное обеспечение расходными материалами оргтехники по заявкам сотрудников Колледжа.

- 2.9. Планирование информационной инфраструктуры, структуры внутренней сети.
- 2.10. Установка на серверы и рабочие станции сетевого программного обеспечения, конфигурирование систем и программного обеспечения.
- 2.11. Организация доступа к локальным и глобальным сетям, в том числе - сети «Интернет».
- 2.12. Регистрация пользователей, назначение идентификаторов (логинов) и паролей.
- 2.13. Установка и настройка сетевых сервисов. Поддержание их в рабочем состоянии.
- 2.14. Протоколирование системных и сетевых событий, событий доступа к ресурсам – для последующего анализа.
- 2.15. Защита от вирусов. Обновление антивирусных баз.
- 2.16. Установка ограничений (если потребуется) для пользователей по использованию рабочей станции или серверов; времени; степени использования ресурсов.
- 2.17. Составление заявки на ремонт неисправного, приобретение нового и модернизацию устаревшего аппаратного оборудования серверов и рабочих станций, сетевого оборудования.
- 2.18. Техническое обслуживание электронной техники путем регламентации проведения профилактических работ, обеспечивает ее работоспособное состояние, рациональное использование.
- 2.19. Администрирование официального сайта Колледжа.
- 2.20. Проведение единой технической политики Колледжа и координации работ по обеспечению безопасности персональных данных в Колледже.
- 2.21. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе:
 - мероприятий по закрытию технических каналов утечки персональных данных при их обработке;
 - мероприятий по защите от несанкционированного доступа к персональным данным;
 - мероприятий по выбору средств защиты персональных данных при их обработке;
 - контроль за обеспечением уровня защищенности персональных данных.
- 2.22. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- 2.23. Участие в подготовке объектов Колледжа к аттестации по выполнению требований обеспечения безопасности персональных данных.

- 2.24. Разработка организационных распорядительных документов по обеспечению безопасности персональных данных в Колледже.
- 2.25. Организация в установленном порядке расследования причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.
- 2.26. Проведение периодического контроля эффективности мер защиты персональных данных в Колледже. Учет и анализ результатов контроля.
- 2.27. Организация повышения осведомленности руководства и сотрудников Колледжа по вопросам обеспечения безопасности персональных данных.
- 2.28. Подготовка отчетов об уровне безопасности персональных данных в Колледже.
- 2.29. Развитие и совершенствование прикладных информационных систем и информационно-технической инфраструктуры Колледжа.
- 2.30. Обеспечение штатного функционирования прикладных информационных систем и информационно-технической инфраструктуры Колледжа.
- 2.31. Организация и контроль исполнения проектов в области информационных технологий, а также обеспечение предоставления заданного набора и качества информационных сервисов структурным подразделениям Колледжа.
- 2.32. Разработка и внедрение организационных и технических мероприятий по комплексной защите информации в Колледже.
- 2.33. Организация взаимодействия между структурными подразделениями Колледжа по вопросам защиты информации.
- 2.34. Контроль соблюдения нормативных требований по надежной защите информации.
- 2.35. Разработка и реализация мер по устранению выявленных недостатков по защите информации.
- 2.36. Проведение аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.
- 2.37. Разработка регламента допуска сотрудников Колледжа к отдельным каналам информации, плана защиты информации, положений об определении степени защищенности ресурсов автоматизированных систем.
- 2.38. Разработка и внедрение организационных и технических мероприятий по комплексной защите информации в Колледже, содержание которой составляет государственную или коммерческую тайну.

- 2.39. Выбор, установка, настройка и эксплуатация систем защиты в соответствии с действующим законодательством.
- 2.40. Обеспечение соответствия проводимых работ технике безопасности, правилам и нормам охраны труда.
- 2.41. Проведение аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности, представление в установленном порядке действующей отчетности.
- 2.42. Осуществление методического руководства деятельностью других структурных образовательной организации по вопросам защиты информации.

3. Права и ответственность сотрудников службы

- 3.1. Определять содержание и конкретные формы своей деятельности с функциями и задачами, указанными в положении о службе компьютерного обеспечения.
- 3.2. Представлять на рассмотрение и утверждение проекты документов: правила по технике безопасности при выполнении работ, положения, должностные инструкции и др.
- 3.3. Вносить предложения по штатному расписанию сотрудников службы.
- 3.4. Представлять Колледж в различных учреждениях и организациях в пределах своей компетенции, принимать участие в работе конференций, совещаний и семинаров.
- 3.5. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.
- 3.6. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.
- 3.7. Контролировать деятельность структурных подразделений Колледжа в части выполнения ими требований по обеспечению безопасности персональных данных.
- 3.8. Вносить предложения директору Колледжа о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.
- 3.9. Привлекать в установленном порядке необходимых специалистов из числа сотрудников Колледжа для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

- 3.10. Служба компьютерного обеспечения несет ответственность за сохранность переданных ему материальных ценностей. Работники виновные, в причинении ущерба имуществу Колледжа, переданному службе, несут ответственность в порядке, предусмотренном действующим законодательством.
- 3.11. Ответственность за надлежащее и своевременное выполнение функций службы несет руководитель службы.
- 3.12. На руководителя службы/сотрудников службы возлагается персональная ответственность в случае:
- необеспечения сохранности принятых на ответственное хранение программных и технических средств;
 - необеспечения сохранности принимаемой информации и достоверности передаваемой информации;
 - несвоевременного или некачественного исполнения документов и поручений вышестоящего руководства;
 - допущения использования информации сотрудниками службы в неслужебных целях;
 - ненадлежащего контроля за режимом доступа к информации, повлекшего утечку информации, повреждение информационных баз данных;
 - несоблюдения трудового распорядка сотрудниками службы.

Руководитель службы
компьютерного обеспечения _____ С.В. Чечуров