КГКП «Костанайский колледж сферы обслуживания»
Управления образования акимата Костанайской области

СОГЛАСОВАНО
Председатель первичной профсоюзной организации КГКП «Костанайский колледж сферы обслуживания»
Управления образования акимата Костанайской области
_____ Бимаганбетов Е.А.
«01» 09 2026 г.

УТВЕРЖДАЮ
Директор
КГКП «Костанайский колледж сферы обслуживания»
Управления образования акимата Костанайской области
_____ Жанарсланова Д.Б.
«01» 09 2026 г.

ИНСТРУКЦИЯ ПО ОХРАНЕ ТРУДА И ТЕХНИКЕ БЕЗОПАСНОСТИ ДЛЯ ИНЖЕНЕРА ПО ОБОРУДОВАНИЮ КОЛЛЕДЖА

1. Общие положения

1.1. Данная инструкция по охране труда и технике безопасности предназначена для инженера по оборудованию колледжа и устанавливает обязательные требования по безопасному выполнению профессиональных обязанностей в целях сохранения жизни и здоровья.

1.2. Инженер по оборудованию должен соблюдать нормы и правила охраны труда, техники безопасности, санитарные требования, противопожарные правила и правила эксплуатации электронно-вычислительной техники и сетевого оборудования.

1.3. К работе допускаются лица не моложе 18 лет, прошедшие:
- обязательный предварительный и периодический медицинский осмотр;
- вводный инструктаж по охране труда;
- первичный инструктаж на рабочем месте;
- обучение безопасным методам работы с компьютерной техникой, серверным оборудованием и электроустановками до 1000 В (при необходимости получения группы по электробезопасности).

1.4. Основными опасными и вредными производственными факторами для инженера по оборудованию являются:
- повышенное зрительное напряжение при длительной работе с кодом и экраном монитора;
- длительная статическая нагрузка на позвоночник и мышцы кистей рук (риск развития синдрома запястного канала);
- воздействие электромагнитных полей и статического электричества;
- опасность поражения электрическим током при коммутации кабелей, обслуживании серверных стоек и ПК.

1.5. Инженер по оборудованию несет ответственность за соблюдение требований охраны труда и может быть привлечен к дисциплинарной и иной ответственности в случае нарушения установленных норм.

2. Требования безопасности перед началом работы

2.1. Проверить рабочее место: оно должно быть чистым, свободным от посторонних предметов, коробки с сетевым оборудованием или патч-корды не должны загромождать доступ к выходам и проходы.

2.2. Убедиться в исправности электрических розеток, вилок, блоков питания, сетевых фильтров и кабелей подключения персонального компьютера. Не допускается использовать поврежденные или оголенные провода.

2.3. Проветрить помещение серверной или рабочего кабинета перед началом работы для обеспечения надлежащего температурного режима.

2.4. Отрегулировать высоту офисного кресла и угол наклона монитора так, чтобы верхняя точка экрана находилась на уровне глаз, исключая чрезмерное напряжение шеи.

2.5. Убедиться, что на рабочем месте достаточное освещение, отсутствуют блики от окон или ламп на экране монитора.

2.6. Разместить периферийные устройства (клавиатуру, мышь, графический планшет) и необходимую техническую документацию удобно для работы.

2.7. Включить компьютер, дождаться полной загрузки операционной системы. Убедиться в корректной работе вентиляторов охлаждения системного блока.

2.8. Надеть при необходимости очки для защиты глаз от компьютерного излучения или специализированные СИЗ (например, антистатический браслет или перчатки при разборе системных блоков).

2.9. Проверить доступ к корпоративной сети, серверам и базам данных колледжа. При обнаружении аппаратных сбоев или признаков повреждения изоляции оборудования немедленно сообщить администрации и не приступать к работе.

3. Требования безопасности во время работы

3.1. Поддерживать порядок на рабочем месте: инструменты для администрирования, накопители, кабели и тестовые устройства должны располагаться упорядоченно.

3.2. Соблюдать регламентированный режим труда и отдыха: после каждого часа непрерывной разработки или администрирования делать 5-10-минутный перерыв для выполнения гимнастики для глаз и разминки суставов.

3.3. Следить за правильным положением рук на клавиатуре во избежание перенапряжения кистей. Держать спину ровно, опираясь на спинку кресла.

3.4. Не перегружать электросеть: не подключать к одному сетевому фильтру или источнику бесперебойного питания (ИБП) избыточное количество тестовых стендов и периферии.

3.5. Бережно обращаться с компьютерной техникой: предотвращать попадание жидкостей на клавиатуру и электронные платы. Не производить замену комплектующих ПК или серверов во включенном состоянии.

3.6. Не использовать несертифицированное или вредоносное программное обеспечение, строго соблюдать политики информационной безопасности колледжа.

3.7. При обслуживании серверных шкафов и коммутационных узлов следить за надежностью крепления оборудования и аккуратностью укладки кабельных трасс.

3.8. При появлении симптомов зрительного утомления, головной боли или мышечного онемения приостановить работу и сделать легкую физическую разминку.

3.9. Не отвлекаться на посторонние факторы при проведении критических обновлений системного ПО, конфигурации серверов или баз данных колледжа.

3.10. Соблюдать правила внутреннего трудового распорядка. При обнаружении перегрева техники, запаха плавящейся изоляции или сильного гула кулеров немедленно обесточить оборудование.

4. Требования безопасности в аварийных ситуациях

4.1. При возникновении пожара, задымления или появлении запаха гари в кабинете или серверной немедленно прекратить работу, отключить электропитание (в том числе ИБП, если это безопасно), эвакуироваться и сообщить администрации.

4.2. В случае поражения электрическим током сотрудника или студента в компьютерном классе — незамедлительно отключить электропитание с помощью главного рубильника (автомата), оказать первую помощь пострадавшему и вызвать «Скорую помощь».

4.3. При возникновении короткого замыкания, искрения в системном блоке или сервере — отключить подачу питания кнопкой на ИБП или выдернуть шнур из розетки, после чего вызвать инженера по электробезопасности.

4.4. При внезапном сбое систем кондиционирования в серверной комнате, повлекшем критический перегрев оборудования, произвести штатное аварийное завершение работы серверов и доложить руководству.

4.5. При угрозе террористического акта (получение сообщения об опасности, обнаружение подозрительного предмета в учебном классе) действовать по инструкции учреждения: не прикасаться к предмету, оповестить руководство и покинуть здание.

4.6. При масштабной кибератаке, шифровании данных или критической утечке персональных данных колледжа — локализовать угрозу путем отключения поврежденных сегментов от сети и незамедлительно доложить руководству.

4.7. В случае резкого ухудшения собственного самочувствия остановить выполнение задач, известить коллег и обратиться в медицинский пункт колледжа.

4.8. Все аварийные ситуации и технические инциденты должны фиксироваться в установленном порядке с уведомлением ответственного за охрану труда.

5. Требования безопасности по окончании работы

5.1. Завершить компиляцию программного кода, закрыть сессии администрирования, сохранить конфигурационные файлы систем и корректно выйти из сред разработки.

5.2. Проверить резервное копирование данных (если оно настроено на конец рабочего дня), отключить съемные накопители и токены ЭЦП от рабочих станций.

5.3. Выключить персональный компьютер, тестовые стенды и неосновное сетевое оборудование (за исключением серверов непрерывного цикла).

5.4. Обесточить бытовые электроприборы и локальные сетевые фильтры на рабочем месте.

5.5. Навести порядок на столе, убрать инструменты, съемные жесткие диски и документацию, содержащую конфиденциальные данные, в закрывающиеся шкафы.

5.6. При обнаружении скрытых технических дефектов (повреждение изоляции кабелей, неисправность кулеров ИБП) составить заявку для технической службы или сообщить ответственному за охрану труда.

5.7. Закрыть окна в кабинете, убедиться, что кондиционеры переведены в штатный режим работы, выключить освещение.

5.8. Покинуть помещение, запереть дверь кабинета на ключ и сдать его на пост охраны колледжа.

6. Ответственность

6.1. Инженер по оборудованию несет ответственность за нарушение требований данной инструкции в соответствии с действующим законодательством РК.

6.2. За невыполнение или ненадлежащее выполнение обязанностей по охране труда инженер по оборудованию может быть привлечен к дисциплинарной, административной или уголовной ответственности в зависимости от тяжести последствий.

6.3. Инженер по оборудованию обязан соблюдать конфиденциальность учетных данных, паролей доступа к серверам и базам данных колледжа, и не передавать их третьим лицам.