**УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АТЫРАУСКОЙ ОБЛАСТИ**

**КГКП «АТЫРАУСКИЙ ПОЛИТЕХНИЧЕСКИЙ ВЫСШИЙ КОЛЛЕДЖ**

**ИМЕНИ САЛАМАТА МУКАШЕВА»**

**Дневник-отчет**

**о прохождении профессиональной практики**

Специальность: 06120100 – Вычислительная техника и информационные сети ( по видам)

Группа:ВТиИСа-22(9)р\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Студент: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
                     (Ф.И.О)

Наименование практики: ПМ 08 «Обеспечение работоспособности IоT устройств»

ПМ 09 «Обеспечение информационной безопасности локальных вычислительных сетей и Internet»  
ПМ 10 «Управление системами и сетями организации»

**АТЫРАУ – 2025**

**ОТЧЕТПО ПРАКТИКЕ**

\_\_\_\_\_Производственная\_\_\_\_

указать вид практики

с «\_\_» \_\_\_\_\_\_\_20\_\_\_г по «\_» \_\_\_\_\_\_\_\_\_20\_\_\_\_г

Выполнил(а) студент(ка) группы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ВТиИСа-22(9)р\_\_\_\_\_\_\_\_

Ф.И.О. студента\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель практики от

колледжа\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е. Е. Аманжолов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель практики от

предприятия \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Оценка по практике\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

М.О

М.П.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №п. п | Наименование выполненных (изученных) работ в соответствии с программой профессиональной практики за каждый день | Сроки выполнения отдельных тем, работ профессиональной практики | | Подпись руководителя профессионалной практики |
| начало | завершение |  |
| 1. | Знакомства с рабочим местом,  Изучение техники безопасности и правил работы с оборудованием | 07.04.25 | 10.05.25 |  |
| 2. | Ознакомление с оборудованием:  Ноутбуки, терминалы, серверы | 11.04.25 | 18.04.25 |  |
| 3. | Изучение настройки и обслуживания ноутбуков для повседневной работы | 21.04.25 | 22.04.25 |  |
| 4. | Замена старых интернет кабелей на новые в 3 этажах учреждении | 23.04.25 | 25.04.25 |  |
| 5. | Подготовка кабинетов к предстоящим мероприятиям | 28.04.25 | 29.04.25 |  |
| 6. | Организация мероприятия для школьников выпускных классов | 30.04.25 | 02.05.25 |  |
| 7. | Работать с серверами в практике  (под присмотром куратора) | 05.05.25 | 12.05.25 |  |
| 8. | Замена старых интернет каблей в кабинетах | 13.05.25 | 16.05.25 |  |
| 9. | Техническое обслуживание в серверах и исправление проводных дефектов | 19.05.25 | 23.05.25 |  |
| 10. | Повседневная тех. поддержка нуждающимся в учреждении | 26.05.25 | 12.06.25 |  |
| 11. | Заключение | 13.06.25 | 14.06.25 |  |
| 12. | Подготовка отчётной документации по практике | 14.06.25 | 16.05.25 |  |

**1.Описание изученных конструкций, оборудование,технологических процессов, механизации, автоматизации производства ипередовых методов труда, и т. д.**  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Подпись обучающегося\_\_\_\_\_\_\_\_\_\_ «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20 \_\_\_г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(непосредственный руководитель профессиональной практики)

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20 \_\_\_г.

**2. Поощрения и взыскания обучающегося практиканта.**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 **3. Заключения руководителя профессиональной практики (от организации,**

**предприятия, учреждения).**  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Подпись руководителя профессиональной практики (от организации,  
предприятия, учреждения)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
«\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_г.

М.П.

**СОДЕРЖАНИЕ ОТЧЕТА**

1. Краткое содержание о предприятии
2. Правила техники безопасности, соблюдаемые на предприятии
3. Аппаратное и программное обеспечение: состав и назначение
4. Методы обеспечения кибербезопасности
5. Топология и структура локальной вычислительной сети
6. Резервное копирование и восстановление данных в облачных системах
7. Мониторинг состояния сетевого оборудования и серверов

Заключение

Список использованных источников и литературы

**КРАТКОЕ СОДЕРЖАНИЕ: Атырауский Политехнический Высший Колледж имени Саламат Мукашев**

**Атырауский Политехнический Высший Колледж имени Саламата Мукашева (АПВК) —** это образовательное учреждение в городе Атырау, Казахстан, которое готовит специалистов среднего звена для различных отраслей промышленности, в основном ориентированных на нефтегазовый сектор региона.

**Ключевые особенности и направления деятельности:**

* **История и развитие:**
* **Один из старейших:** Колледж является одним из старейших учебных заведений Республики Казахстан, готовящих специалистов для нефтегазовой отрасли. Его история берет начало в 1930-х годах прошлого века.
* **Основание:** Учебное заведение было основано в 1930 году как Гурьевский горно-нефтяной техникум по решению Высшего совета народного хозяйства СССР. Это было связано с острой нехваткой местных технических кадров для освоения богатых ресурсов Урало-Эмбинского региона, особенно в Гурьевском нефтяном производстве.
* **Имя Саламата Мукашева:** В 2014 году колледжу было присвоено имя Саламата Мукашева, выдающегося государственного и общественного деятеля, который сам окончил Гурьевский нефтяной техникум в 1947 году. Это подчеркивает его вклад в развитие региона и республики.
* **Специализации:** Основное внимание уделяется подготовке кадров для таких сфер, как:
  + **Нефтегазовая промышленность (эксплуатация нефтяных и газовых скважин, бурение, обслуживание оборудования).**
  + **Энергетика (электрооборудование, теплоэнергетика).**
  + **Информационные технологии.**
  + **Строительство.**
  + **Экономика и учет.**
* **Практическая направленность:** Обучение в колледже ориентировано на приобретение практических навыков. Студенты проходят производственную практику на ведущих предприятиях Атырауской области, что способствует их быстрому трудоустройству.
* **Материально-техническая база:** Колледж располагает современными лабораториями, мастерскими и учебными классами, оснащенными необходимым оборудованием для проведения занятий и практических работ.
* **Востребованность выпускников:** Выпускники АПВК востребованы на рынке труда благодаря высокому уровню подготовки и соответствию образовательных программ потребностям региональных предприятий.
* **Цель:** Основная цель колледжа — обеспечение региона квалифицированными кадрами, способными эффективно работать в условиях современной экономики.

**ПРАВИЛА ТЕХНИКИ БЕЗОПАСНОСТИ**

**Правила техники безопасности в IT-отделе**

Безопасность в IT-отделе выходит за рамки только физической защиты и включает в себя как физическую безопасность, так и информационную безопасность, а также эргономику рабочего места. Вот основные правила, которые должны соблюдаться:

Физическая безопасность и эргономика

1. **Рабочее место:** 
   * **Порядок:** Всегда поддерживайте порядок на рабочем месте. Провода не должны мешать проходу или создавать риск спотыкания.
   * **Освещение:** Убедитесь, что рабочее место достаточно освещено, чтобы избежать напряжения глаз.
   * **Вентиляция:** Помещения, где находится IT-оборудование, должны хорошо вентилироваться, чтобы предотвратить перегрев техники и обеспечить комфортную температуру для сотрудников.
2. **Электрооборудование:** 
   * **Исправность:** Используйте только исправное оборудование и кабели без видимых повреждений.
   * **Подключение:** Подключайте оборудование к заземленным розеткам. Избегайте перегрузки электрических сетей.
   * **Отключение:** Перед проведением любых работ с внутренними компонентами компьютера или другого оборудования, всегда отключайте его от электросети.
3. **Пожарная безопасность:** 
   * **Огнетушители:** Знайте расположение огнетушителей и умейте ими пользоваться (особенно порошковыми или углекислотными для электроники).
   * **Легковоспламеняющиеся материалы:** Не храните легковоспламеняющиеся материалы рядом с оборудованием.
   * **Курение:** Курение в помещениях с IT-оборудованием строго запрещено.
4. **Эргономика:** 
   * **Монитор:** Расположите монитор на расстоянии вытянутой руки, верхний край экрана должен быть на уровне глаз или чуть ниже.
   * **Кресло:** Используйте эргономичное кресло с поддержкой спины и регулируемой высотой.
   * **Положение тела:** Следите за правильной осанкой. Делайте регулярные перерывы (каждые 45-60 минут) для разминки и отдыха глаз.
   * **Клавиатура и мышь:** Расположите их таким образом, чтобы запястья оставались прямыми.

**Информационная безопасность**

1. **Пароли:** 
   * **Сложные пароли:** Используйте сложные, уникальные пароли для всех учетных записей.
   * **Регулярная смена:** Регулярно меняйте пароли.
   * **Конфиденциальность:** Никогда не сообщайте свои пароли **никому и не записывайте их в легкодоступных местах.**
2. **Доступ к данным:** 
   * **Принцип наименьших привилегий:** Предоставляйте доступ к данным только тем сотрудникам, которым он необходим для выполнения их обязанностей.
   * **Контроль доступа:** Регулярно пересматривайте и обновляйте права доступа.
3. **Защита от вредоносного ПО:** 
   * **Антивирус:** Убедитесь, что на всех рабочих станциях и серверах установлены актуальные антивирусные программы.
   * **Обновления:** Регулярно обновляйте операционные системы и программное обеспечение для закрытия уязвимостей.
   * **Осторожность:** Будьте крайне осторожны при открытии подозрительных писем, ссылок или вложений.
4. **Резервное копирование:** 
   * **Регулярность:** Регулярно создавайте резервные копии критически важных данных.
   * **Хранение:** Храните резервные копии в безопасном месте, желательно в нескольких локациях, включая удаленное хранилище.
5. **Пользовательское поведение:** 
   * **Не оставлять без присмотра:** Не оставляйте свои компьютеры без присмотра разблокированными.
   * Конфиденциальность: Обсуждайте конфиденциальную информацию только в безопасных местах, где нет риска прослушивания.
   * **Удаленное подключение:** Используйте только защищенные VPN-соединения для удаленного доступа к корпоративным ресурсам.

**Общие правила**

1. **Обучение:** Регулярно проходите обучение по технике безопасности и информационной безопасности.
2. **Отчетность:** Сообщайте руководству или ответственному за безопасность о любых инцидентах или потенциальных угрозах.
3. **Доступ к серверным:** Доступ в серверные комнаты должен быть ограничен и контролироваться уполномоченным персоналом.

**Соблюдение этих правил помогает минимизировать риски как для здоровья сотрудников, так и для сохранности важной информации и оборудования IT-отдела.**

**АППАРАТНОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

**Аппаратное и Программное Обеспечение: Элегантное Взаимодействие**

В мире информационных технологий существуют два основополагающих элемента, которые, подобно двум сторонам одной медали, гармонично дополняют друг друга, обеспечивая бесперебойное функционирование всех вычислительных систем. Речь идет об аппаратном обеспечении (Hardware) и программном обеспечении (Software). Их синергия создает ту технологическую среду, в которой мы живем и работаем.

**Аппаратное Обеспечение:** Физическая Основа

Представьте аппаратное обеспечение как искусно спроектированный и построенный каркас, физическое тело любой компьютерной системы.

* **Центральный процессор (CPU):** Это, безусловно, "сердце" и "мозг" системы, центр принятия решений, обрабатывая все инструкции и вычисления.
* **Оперативная память (RAM):** Подобно операционному столу хирурга, это пространство для быстрой и временной обработки данных,
* **Устройства хранения данных:** Это "долгосрочная память" компьютера, где бережно хранятся все наши цифровые активы — от важных документов до любимых фотографий.
* **Материнская плата:** Можно сравнить ее с центральной нервной системой, которая объединяет все компоненты в единое целое, обеспечивая их слаженное взаимодействие.
* **Видеокарта:** Это "глаза" и "художник" компьютера, ответственный за преобразование цифровых сигналов в яркое и четкое изображение на вашем экране.
* **Устройства ввода и вывода:** Это наши средства общения с компьютером — клавиатура и мышь для передачи наших намерений, а монитор и принтер для получения результатов его работы.

**Программное Обеспечение:** Интеллект и Назначение

Если аппаратное обеспечение — это тело, то программное обеспечение — это его интеллект, набор инструкций и команд, которые вдыхают жизнь в физические компоненты, позволяя им выполнять осмысленные задачи.

Здесь мы можем выделить две основные категории:

* **Системное программное обеспечение:** Это "дирижер" всего оркестра. Его главная роль — управлять аппаратными ресурсами и создавать комфортную среду для работы пользователя и других программ.
  + **Операционная система (ОС):** Безусловно, это ключевой элемент, мост между пользователем и "железом". Будь то Windows, macOS или Linux, она управляет процессами, файлами и памятью, предоставляя интуитивно понятный интерфейс.
  + **Драйверы:** Это "переводчики", позволяющие ОС корректно общаться с каждым уникальным аппаратным устройством, обеспечивая их гармоничную работу.
* **Прикладное программное обеспечение (Приложения):** Это те "инструменты", которые мы используем для решения конкретных задач и реализации наших идей.
  + **Офисные пакеты:** Помогают нам создавать документы, таблицы и презентации.
  + **Веб-браузеры:** Открывают для нас бескрайние просторы Интернета.
  + **Графические редакторы:** Дают возможность творить и обрабатывать изображения.

Каждое приложение разработано для выполнения своей специализированной функции, превращая компьютер из простого устройства в мощный инструмент для творчества, работы и общения.

**МЕТОДЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ**

**Методы Обеспечения Кибербезопасности**

Обеспечение кибербезопасности — это комплексный подход, направленный на защиту информационных систем, сетей и данных от несанкционированного доступа, использования, раскрытия, нарушения, изменения или уничтожения. Это критически важно для любой организации в современном цифровом мире. Ниже представлены ключевые методы, используемые для достижения этой цели.

**1. Управление доступом (Access Control)**

* **Принцип наименьших привилегий:** Предоставление пользователям и системам только минимально необходимых прав доступа для выполнения их задач.
* **Многофакторная аутентификация (MFA/2FA):** Требование двух или более факторов для проверки личности (например, пароль и код из SMS/приложения).
* **Управление идентификацией и доступом (IAM):** Централизованная система для управления цифровыми удостоверениями и правами доступа.
* **Сегментация сети:** Разделение сети на изолированные сегменты для ограничения распространения потенциальных угроз.

**2. Защита от вредоносного ПО (Malware Protection)**

* **Антивирусное и антишпионское ПО:** Установка и регулярное обновление программ для обнаружения и удаления вредоносных программ.
* **Системы обнаружения и предотвращения вторжений (IDS/IPS):** Мониторинг сетевого трафика на предмет подозрительной активности и блокировка угроз.
* **"Песочницы" (Sandboxing):** Изолированная среда для безопасного запуска подозрительных файлов и программ.

**3. Обновления и Патчи (Patch Management)**

* **Регулярное обновление ПО:** Своевременная установка обновлений для операционных систем, приложений и прошивок для устранения известных уязвимостей.
* **Автоматизация:** Использование инструментов для автоматического развертывания патчей и обновлений.

**4. Резервное копирование и восстановление (Backup and Recovery)**

* **Регулярное создание резервных копий:** Периодическое копирование критически важных данных и конфигураций.
* **Хранение "вне сайта":** Хранение резервных копий в удаленных или облачных хранилищах для защиты от локальных катастроф.
* **Тестирование восстановления:** Регулярная проверка возможности восстановления данных из резервных копий.

**5. Сетевая безопасность (Network Security)**

* **Межсетевые экраны (Firewalls):** Устройство или ПО, контролирующее входящий и исходящий сетевой трафик на основе заданных правил.
* **Виртуальные частные сети (VPN):** Создание зашифрованных соединений для безопасного удаленного доступа к корпоративным ресурсам.
* **Защита от DDoS-атак:** Методы и сервисы для смягчения атак типа "отказ в обслуживании".
* **Сканирование уязвимостей и тестирование на проникновение (Vulnerability Scanning & Penetration Testing):** Регулярный анализ систем на наличие слабых мест и имитация атак для выявления уязвимостей.

**6. Обучение пользователей и повышение осведомленности (User Education & Awareness)**

* **Тренинги по кибербезопасности:** Регулярное обучение сотрудников основам безопасного поведения в сети (распознавание фишинга, работа с паролями).
* **Имитация фишинговых атак:** Проведение контролируемых фишинговых кампаний для оценки уровня осведомленности сотрудников.

**7. Шифрование данных (Data Encryption)**

* **Шифрование данных "в покое" (Data at Rest):** Защита данных, хранящихся на дисках и в базах данных.
* **Шифрование данных "в движении" (Data in Transit):** Защита данных при их передаче по сети (например, через HTTPS, TLS).

**8. Мониторинг и логирование (Monitoring and Logging)**

* **Системы управления информацией и событиями безопасности (SIEM):** Сбор, агрегация и анализ логов из различных источников для выявления аномалий и инцидентов безопасности.
* **Регулярный аудит:** Проверка журналов событий и системных конфигураций на предмет подозрительной активности.

**9. Планирование реагирования на инциденты (Incident Response Planning)**

* **План реагирования:** Разработка и тестирование четкого плана действий на случай кибератаки (обнаружение, сдерживание, искоренение, восстановление).
* **Формирование команды реагирования:** Назначение ответственных лиц и их ролей в случае инцидента.

Применение этих методов в комплексе позволяет значительно повысить уровень киберзащищенности организации.

**ТОПОЛОГИЯ И СТРУКТУРА ЛОКАЛЬНОЙ СЕТИ**

**Топология и Структура Локальной Сети**

При проектировании и развертывании локальной вычислительной сети (ЛВС, или LAN - Local Area Network) ключевое значение имеют два понятия: топология и структура. Они определяют, как физически и логически соединены устройства в сети и как по ней передаются данные.

**Топология Локальной Сети**

Сетевая топология описывает физическое или логическое расположение элементов сети (узлов, таких как компьютеры, принтеры, серверы, и связей между ними). Она определяет, как данные могут перемещаться между устройствами. Выбор топологии напрямую влияет на производительность сети, её надежность, масштабируемость и стоимость развёртывания.

**Различают физическую и логическую топологии:**

* Физическая топология — это реальное расположение устройств и кабелей. Как они фактически проложены и соединены в пространстве.
* Логическая топология — это путь, по которому данные перемещаются по сети, независимо от физического расположения. Например, в сети со звездообразной физической топологией данные могут логически передаваться по принципу шины или кольца.

**Основные типы физических топологий:**

1. **Шина (Bus Topology):**
   * **Описание:** Все устройства подключены к единому центральному кабелю (магистрали). Данные передаются по этому кабелю во всех направлениях.
   * **Преимущества:** Простая в установке для небольших сетей, требует меньше кабеля.
2. **Звезда (Star Topology):**
   * **Описание:** Каждое устройство подключается к центральному устройству (хабу или коммутатору) отдельным кабелем.
   * **Преимущества:** Высокая отказоустойчивость (отказ одного устройства или кабеля не влияет на остальные), простотадобавления/удаления устройств, легкая диагностика проблем.
3. **Кольцо (Ring Topology):**
   * **Описание:** Устройства соединены по кругу, образуя замкнутое кольцо. Данные передаются в одном направлении от устройства к устройству.
   * **Преимущества:** Упорядоченная передача данных, отсутствие коллизий (столкновений данных).
4. **Сетка (Mesh Topology):**
   * **Описание:** Каждое устройство соединено со всеми остальными устройствами в сети.
   * **Преимущества:** Максимальная отказоустойчивость и надежность (множество путей для передачи данных), высокая производительность.
   * **Недостатки:** Очень высокая стоимость из-за большого количества кабелей и портов, сложность установки и управления. Часто используется в высоконадежных сетях, таких как магистральные или беспроводные сети.
5. **Дерево (Tree Topology):**
   * **Описание:** Иерархическая структура, представляющая собой комбинацию нескольких топологий "звезда", соединенных магистралью, по принципу шины.
   * **Преимущества:** Легко расширяема, удобно для управления большими сетями.
   * **Недостатки:** Отказ главной магистрали может нарушить работу всей сети, более сложная установка.
6. **Гибридная (Hybrid Topology):**
   * **Описание:** Сочетание двух или более различных топологий. Например, две "звезды", соединенные "шиной".
   * **Преимущества:** Гибкость, позволяет оптимизировать сеть под конкретные нужды, сочетая достоинства разных топологий.

**Структура Локальной Сети**

Структура локальной сети относится к совокупности всех компонентов (как аппаратных, так и программных), которые обеспечивают ее функционирование, а также к принципам их взаимодействия. Это более широкое понятие, чем топология, включающее в себя не только физическое расположение, но и логическую организацию, используемое оборудование и протоколы.

**Основные компоненты структуры ЛВС:**

1. **Конечные устройства (End Devices/Nodes):**
   * **Компьютеры:** Рабочие станции, серверы, ноутбуки.
   * **Периферийные устройства:** Принтеры, сканеры, IP-телефоны.
   * **IoT-устройства:** "Умные" датчики, камеры.
2. **Сетевые устройства (Networking Devices):**
   * **Сетевые карты (NIC - Network Interface Card):** Устанавливаются в каждое конечное устройство для его подключения к сети.
   * **Коммутаторы (Switches):** Центральные устройства в звездообразной топологии, которые интеллектуально перенаправляют данные только на нужный порт, обеспечивая эффективную передачу.
   * **Маршрутизаторы (Routers):** Соединяют различные сети (например, локальную сеть с Интернетом или с другой ЛВС), выбирая оптимальные пути для передачи данных.
   * **Точки доступа Wi-Fi (Wireless Access Points - WAP):** Позволяют беспроводным устройствам подключаться к проводной сети.
   * **Межсетевые экраны (Firewalls):** Защищают сеть от несанкционированного доступа, фильтруя трафик**.**
3. **Среда передачи данных (Transmission Media):**
   * **Кабели:** 
     + **Витая пара (Twisted Pair):** Наиболее распространена (UTP, STP).
     + **Оптоволоконный кабель (Fiber Optic):** Для высокоскоростных и дальних соединений.
   * **Беспроводные соединения:** Wi-Fi, Bluetooth.
4. **Сетевое программное обеспечение:**
   * **Операционные системы:** Сетевые ОС на серверах (Windows Server, Linux) и клиентские ОС на рабочих станциях.
   * **Сетевые протоколы:** Набор правил, определяющих формат и способ передачи данных (например, TCP/IP, Ethernet, Wi-Fi).
   * **Сетевые службы:** DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), файловые и печатные службы.
5. **Серверы:**
   * **Файловые серверы:** Для централизованного хранения и обмена файлами.
   * **Серверы печати:** Для управления сетевыми принтерами.
   * **Веб-серверы:** Для хостинга веб-сайтов и приложений.
   * **Серверы баз данных:** Для хранения и обработки данных.

**РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ В ОБЛАЧНЫХ СИСТЕМАХ**

**Резервное копирование и восстановление данных в облачных системах —** это процесс сохранения копий данных на удаленных серверах облачного провайдера и возможность их восстановления в случае потери или повреждения оригиналов. Это ключевой элемент стратегии кибербезопасности и непрерывности бизнеса.

**Основные аспекты:**

* **Автоматизация:** Облачные сервисы часто предлагают автоматическое и регулярное резервное копирование по заданному расписанию.
* **Масштабируемость:** Возможность легко увеличивать или уменьшать объем хранилища по мере необходимости.
* **Географическая избыточность:** Данные обычно хранятся в нескольких географически распределенных центрах обработки данных, что повышает отказоустойчивость.
* **Экономичность:** Отсутствие необходимости в покупке и обслуживании собственного оборудования для хранения.
* **Безопасность:** Облачные провайдеры применяют высокие стандарты шифрования и физической безопасности для защиты данных.
* **Восстановление:** Процесс восстановления данных, как правило, прост и управляется через веб-интерфейс или API, позволяя быстро вернуть данные к определенному состоянию.

Таким образом, облачное резервное копирование обеспечивает надежную защиту данных и быстрое восстановление с минимальными затратами, перекладывая бремя управления инфраструктурой на провайдера.

**МОНИТОРИНГ СОСТОЯНИЯ ОБОРУДОВАНИЯ И СЕРВЕРОВ**

Эффективный мониторинг состояния оборудования и серверов критически важен для поддержания работоспособности, производительности и безопасности любой ИТ-инфраструктуры. Он позволяет проактивно выявлять и устранять потенциальные проблемы до того, как они перерастут в серьезные сбои, что приводит к сокращению времени простоя, повышению эффективности и улучшению надежности.

**Ключевые Аспекты Мониторинга Оборудования и Серверов**

**аспекты комплексного мониторинга:**

* **Метрики Производительности:** Это включает отслеживание загрузки процессора, использования памяти, операций ввода-вывода диска, пропускной способности сети и задержек. Мониторинг этих метрик помогает выявлять "узкие места", конфликты ресурсов и необычную активность, которая может указывать на проблему.
* **Доступность и Время Безотказной Работы (Uptime):** Регулярная проверка того, что серверы и критически важное оборудование находятся в сети и доступны, является основополагающей. Это часто включает в себя тесты ping, проверку портов и подтверждение того, что службы работают должным образом.
* **Использование Ресурсов:** Помимо просто производительности, понимание того, как потребляются ресурсы с течением времени, помогает в планировании мощностей и обеспечении достаточных ресурсов для текущих и будущих потребностей.
* **Экологические Факторы:** Для физических серверов и сетевого оборудования жизненно важен мониторинг условий окружающей среды, таких как температура, влажность и состояние электропитания, чтобы предотвратить сбои оборудования.
* **События Безопасности:** Ведение журналов и анализ событий безопасности, таких как попытки входа в систему, активность брандмауэра и доступ к конфиденциальным данным, помогает обнаруживать и реагировать на потенциальные нарушения безопасности.
* **Файлы Журналов (Логи):** Системные, прикладные и журналы безопасности содержат ценную информацию о событиях, ошибках и предупреждениях. Централизованное управление журналами и их анализ необходимы для устранения неполадок и выявления закономерностей.

**Инструменты и Стратегии для Эффективного Мониторинга**

Существует широкий спектр инструментов и стратегий для мониторинга, от встроенных инструментов операционной системы до сложных решений корпоративного уровня:

* **Инструменты Операционной Системы:** Большинство операционных систем (Windows, Linux) предлагают базовые инструменты мониторинга, такие как Диспетчер задач, Монитор производительности, top, htop и iostat, которые могут предоставлять информацию в реальном времени.
* **SNMP (Simple Network Management Protocol):** Широко используется для мониторинга сетевых устройств и серверов, SNMP позволяет различным устройствам обмениваться управляющей информацией.
* **WMI (Windows Management Instrumentation):** Для сред Windows WMI предоставляет стандартизированный способ доступа к управляющей информации об операционной системе и оборудовании.
* **Программное Обеспечение для Мониторинга:** Специализированные решения для мониторинга предлагают расширенные функции, такие как:
  + **Мониторинг на основе агентов:** Программные агенты, установленные на серверах, собирают данные и отправляют их на центральный сервер мониторинга.
  + **Без агентский мониторинг:** Использует протоколы, такие как SNMP или WMI, для удаленного сбора данных.
  + **Оповещения и Уведомления:** Настраиваемые оповещения (электронная почта, SMS, push-уведомления) при превышении пороговых значений или обнаружении проблем.
  + **Панели Мониторинга и Отчеты:** Визуализация метрик и создание отчетов для исторического анализа и планирования мощностей.
  + Автоматизация: Сценарии реагирования на определенные события, такие как перезапуск службы.
  + **Примеры популярных инструментов мониторинга:** Zabbix, Nagios, Prometheus, Grafana, Datadog, PRTG Network Monitor, SolarWinds.
* **Службы Мониторинга Облачных Провайдеров:** Облачные платформы, такие как AWS, Azure и Google Cloud, предлагают свои собственные надежные службы мониторинга (например, AWS CloudWatch, Azure Monitor), интегрированные с их соответствующими экосистемами.

**ЗАКЛЮЧЕНИЕ**

Атырауский Политехнический Высший Колледж имени Саламата Мукашева является ключевым образовательным центром в Атырау, Казахстан. Колледж делает упор на практическое обучение, что обеспечивает высокую востребованность его выпускников на рынке труда.

Эффективная работа IT-отдела колледжа, как и любой современной организации, немыслима без строгого соблюдения **правил техники безопасности**. Это включает в себя не только **физическую безопасность** рабочих мест и оборудования, но и всеобъемлющую **информационную безопасность**, охватывающую защиту данных, контроль доступа и борьбу с вредоносным ПО

Для обеспечения стабильности и безопасности информационных систем колледж активно применяет **методы кибербезопасности**, включающие управление доступом, регулярные обновления, резервное копирование и защиту от угроз. В контексте современных вызовов, **резервное копирование и восстановление данных в облачных системах** становится неотъемлемой частью стратегии обеспечения непрерывности работы и защиты информации. Понимание **топологии и структуры локальной сети** также критически важно для эффективного построения и управления IT-инфраструктурой колледжа.

В целом, АПВК не только готовит ценные кадры для региона, но и демонстрирует комплексный подход к обеспечению собственной технологической безопасности и эффективности, что является примером для других образовательных и промышленных учреждений.

**Список использованных источиков и литературы**

<https://www.wikipedia.org>

<https://eubank.kz/>

<https://itmag.kz/>

<https://smartbank.kz/>

<https://newrelic.com/>

<https://it-grad.kz/>