УДК 633.19

Осипов Максим Олегович студент
5 курс, Пермский ГАТУ,
Россия, г. Пермь

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО РЕЗЕРВНОГО КОПИРОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В ДОШКОЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

Аннотация: Рассмотрена задача повышения надёжности хранения и защиты персональных данных в муниципальном дошкольном образовательном учреждении. Исследование выполнено на материале производственной технологической практики в МАДОУ «Центр развития ребёнка – детский сад № 35» г. Перми. Проведены обследование аппаратной, сетевой и программной инфраструктуры, анализ рисков утраты данных и несоответствия требованиям законодательства в сфере персональных данных. Обоснован выбор архитектуры локальной NAS-платформы на базе open-source решения OpenMediaVault. Разработаны технические требования к системе резервного копирования и оценены ожидаемые организационно-технические эффекты её внедрения.

***Ключевые слова*:** информационная инфраструктура, резервное копирование, персональные данные, NAS, OpenMediaVault, дошкольное образовательное учреждение.

Abstract: The problem of increasing the reliability of storage and protection of personal data in a municipal preschool educational institution is considered. The research is based on the materials of an industrial technological internship at the Child Development Center – Kindergarten No. 35 in Perm, Russia. The study includes a survey of the hardware, network, and software infrastructure, a risk analysis of data loss and non-compliance with legal requirements in the field of personal data. The choice of a local NAS platform architecture based on the open-

source solution OpenMediaVault is justified. Technical requirements for the backup system are developed, and the expected organizational and technical effects of its implementation are evaluated.

Keywords: backup, personal data, NAS, OpenMediaVault, preschool educational institution.

Информационные системы образовательных организаций обрабатывают персональные данные воспитанников, родителей и работников, поэтому требования к их защите должны рассматриваться как базовый элемент устойчивости ИТ-инфраструктуры. Федеральный закон № 152-ФЗ определяет персональные данные как любую информацию, относящуюся к прямо или косвенно определённому физическому лицу, а целью закона называет обеспечение защиты прав и свобод человека при обработке таких данных [1]. Для оператора обязательны конфиденциальность, ограничение целей обработки и организационно-технические меры защиты, предусмотренные статьёй 19 данного закона [1]. Требования к защите персональных данных при их обработке в информационных системах конкретизированы постановлением Правительства Российской Федерации № 1119, а состав организационных и технических мер раскрыт в приказе Роскомнадзора № 21 [2; 3].

Практическая значимость указанной проблемы особенно высока для дошкольных образовательных учреждений, где информационная инфраструктура, как правило, формируется при ограниченном бюджете, отсутствии выделенного ИТ-подразделения и преобладании рабочих станций с длительным сроком эксплуатации. Именно такие условия были выявлены в ходе производственной технологической практики в МАДОУ «ЦРР Д/С № 35» г. Перми, что позволило поставить инженерную задачу проектирования системы централизованного резервного копирования персональных данных.

Цель исследования заключается в обосновании архитектуры и технических требований к системе резервного копирования персональных

данных дошкольного образовательного учреждения с учётом действующих нормативных ограничений и реального состояния инфраструктуры.

Методы исследования включали:

1. обследование организационной, аппаратной, программной и сетевой инфраструктуры учреждения;
2. инвентаризацию оборудования и анализ его технического состояния;
3. анализ локальных процессов работы с персональными данными;
4. сравнительный выбор программно-аппаратной платформы для резервного копирования;
5. проектирование технического задания на создаваемую систему.

Организационная модель учреждения показывает, что функции ИТ-поддержки не вынесены в самостоятельное подразделение: сопровождение техники осуществляется в рамках совмещения и за счёт привлечения внештатного специалиста. Это повышает зависимость качества защиты данных от эпизодических действий и усложняет поддержание единых регламентов эксплуатации.

По результатам обследования установлено, что компьютерный парк включает 8 стационарных ПК и 2 ноутбука, используемых заведующей, заместителями, бухгалтерией, специалистами сопровождения и административным персоналом. При этом 5 из 8 стационарных компьютеров были выпущены в 2015–2018 гг., а часть рабочих мест до модернизации функционировала на накопителях HDD и 4 ГБ оперативной памяти, что объективно снижало производительность при работе с веб-сервисами и электронными системами отчётности.

Таблица 1

Состав и состояние ключевых элементов ИТ-инфраструктуры учреждения

Показатель	Значение
Стационарные ПК	8
Ноутбуки	2
МФУ и принтеры	3
Роутеры/коммутаторы	2
ПК старше 6 лет	5
Доля ПК старше 6 лет, %	62,5

Сетевое взаимодействие организовано по простой схеме: подключение к интернету осуществляется через провайдера ПАО «Ростелеком», далее трафик проходит через роутер Keenetic Omni и коммутатор D-Link DES-1008D, после чего распределяется между проводными рабочими местами и Wi-Fi-сегментом.

Обследование показало, что все устройства размещены в одной подсети без сегментации трафика, резервный канал связи отсутствует, централизованный мониторинг сетевой активности не реализован. Такая конфигурация допустима для малого учреждения, однако при обработке персональных данных создаёт дополнительные риски: расширение зоны потенциального несанкционированного доступа, зависимость от одного канала связи и отсутствие централизованного контроля инцидентов.

Программная среда учреждения сформирована на базе Windows 10 Pro, офисных приложений Microsoft Office 2019, антивирусной защиты Kaspersky и специализированных информационных систем «Сетевой город. Образование», «Электронная очередь в ДОУ», портала госуслуг и сервисов Яндекс 360.

В ходе практики были выявлены существенные недостатки организации резервного копирования и защиты персональных данных. Часть данных хранилась в локальных папках и Excel-файлах без шифрования, резервные копии создавались на USB-носителях и в облачном хранилище без полноценно формализованной политики управления доступом. На отдельных рабочих

станциях отсутствовали сложные пароли, а на некоторых компьютерах были отключены автоматические обновления. С точки зрения нормативного соответствия это повышало вероятность утраты данных и затрудняло обеспечение режима конфиденциальности, закреплённого законом [1–3].

Таблица 2

Основные выявленные проблемы и их последствия

Выявленная проблема	Практическое последствие
Отсутствие централизованного хранилища	Распыление данных по рабочим местам
Резервное копирование на USB-носители	Повышенный риск утраты и компрометации данных
Отсутствие шифрования локальных хранилищ	Уязвимость персональных данных при несанкционированном доступе
Единая подсеть без сегментации	Увеличение зоны сетевого риска
Отсутствие формализованного аудита копирования	Сложность контроля полноты и регулярности резервирования

Для проектируемой системы была выбрана NAS-платформа на базе open-source решения OpenMediaVault. Такой выбор обусловлен тем, что платформа позиционируется как решение класса NAS на базе Debian Linux, поддерживает веб-администрирование, работу по SSH, доступ к хранилищу по различным протоколам и механизмы управления правами пользователей и групп, а также ориентирована на небольшие офисы и аналогичные по масштабу среды [4]. Сервис RSync в OpenMediaVault позволяет организовать задания push/pull, локальные и удалённые операции копирования и запуск по расписанию, а служба Samba обеспечивает разграничение прав доступа к общим ресурсам [4–6].

Выбор OpenMediaVault представляется обоснованным по нескольким причинам. Во-первых, учреждение не располагает серверной комнатой и бюджетом на промышленную СХД, следовательно, требуется малозатратное и энергоэффективное решение. Во-вторых, существующая инфраструктура ориентирована на работу сотрудников без глубоких технических компетенций, а значит, платформа должна иметь простой интерфейс администрирования. В-третьих, необходимо обеспечить совместимость с Windows-станциями и возможность настройки регулярного резервного

копирования по расписанию. По данным официальной документации, OpenMediaVault поддерживает SMB/CIFS, RSync, SSH и механизмы управления правами доступа, что соответствует поставленной задаче [4–6].

В рамках проектирования предложена стратегия резервного копирования Grandfather–Father–Son: ежедневные инкрементные копии, еженедельные полные копии и ежемесячные архивные копии с длительным сроком хранения. Такая схема обеспечивает баланс между объёмом хранилища, скоростью восстановления и сохранением истории изменений. С учётом масштаба учреждения достаточно применения маломощного мини-ПК либо Raspberry Pi 4 с подключённым внешним HDD/SSD объёмом 2–4 ТБ, активным охлаждением и гигабитным Ethernet.

Выполненное проектирование позволяет оценить ожидаемый эффект внедрения. Централизация хранения резервных копий устраняет зависимость от разрозненных USB-носителей, автоматизация процесса снижает нагрузку на административный персонал, а разграничение доступа и шифрование приближают инфраструктуру к требованиям законодательства о персональных данных [1–3]. Кроме того, единая система резервирования повышает устойчивость учреждения при аппаратных отказах рабочих станций и сокращает время восстановления документов, отчётности и служебной переписки.

Таким образом, результаты производственной практики показали, что ключевой инженерной проблемой исследуемого дошкольного учреждения является отсутствие централизованной, автоматизированной и нормативно ориентированной системы резервного копирования персональных данных. На основе обследования инфраструктуры обоснована целесообразность внедрения локальной NAS-платформы на базе OpenMediaVault. Предложенное решение учитывает реальные ресурсные ограничения учреждения, обеспечивает совместимость с существующим компьютерным парком и создаёт основу для дальнейшей выпускной квалификационной работы.

К числу практических предложений относятся:

– поэтапное внедрение NAS-хранилища с выделением отдельного защищённого сегмента доступа;

– утверждение локального регламента резервного копирования и восстановления данных;

– введение обязательной парольной политики и регулярного контроля обновлений;

– проведение периодического инструктажа сотрудников по вопросам кибергигиены и работы с персональными данными;

– тестирование процедуры восстановления не реже одного раза в квартал.

Список литературы:

1. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.
2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ от 01.11.2012 № 1119 // Собрание законодательства РФ. – 2012. – № 45. – Ст. 6257.
3. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ Роскомнадзора от 18.02.2022 № 21 // Официальный интернет-портал правовой информации. – URL: http://publication.pravo.gov.ru/Document/View/0001202104210039 (дата обращения: 20.04.2026).
4. Openmediavault Documentation [Электронный ресурс] // openmediavault : официальный сайт. – URL: https://docs.openmediavault.org/en/8.x/ (дата обращения: 20.04.2026).
5. RSync – openmediavault documentation [Электронный ресурс] // openmediavault : официальный сайт. – URL: https://docs.openmediavault.org/en/latest/administration/services/rsync.html (дата обращения: 20.04.2026).
6. Samba – openmediavault documentation [Электронный ресурс] // openmediavault : официальный сайт. – URL: https://docs.openmediavault.org/en/latest/administration/services/samba.html (дата обращения: 20.04.2026).

7. Об образовании в Российской Федерации : Федеральный закон от 29.12.2012 № 273-ФЗ // Собрание законодательства РФ. – 2012. – № 53 (ч. 1). – Ст. 7598.
8. Санитарные правила СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» : утв. постановлением Главного государственного санитарного врача РФ от 28.09.2020 № 28 // Официальный интернет-портал правовой информации. – URL: http://publication.pravo.gov.ru/Document/View/0001202012210122 (дата обращения: 20.04.2026).