

Секция «Современные социальные трансформации: факторы, условия, результаты»

Технологии социально-информационной безопасности в социальной работе

Научный руководитель – Веричева Ольга Николаевна

Соколова Дарья Сергеевна

Студент (бакалавр)

Костромской государственной университет имени Н.А. Некрасова, Кострома, Россия

E-mail: dashasokolova533@gmail.com

Актуальность исследования технологий социально-информационной безопасности в социальной работе определена рядом факторов. Во-первых, государственное регулирование в этой сфере представлено рядом нормативных актов, таких как ФЗ «О персональных данных» от 27.07.2006 № 152-ФЗ и ФЗ «О защите детей от информации» от 29.12.2010 № 436-ФЗ. Однако, несмотря на наличие законодательной базы, злоумышленники находят новые способы обхода защиты, что требует совершенствования механизмов безопасности.

Во-вторых, статистика МВД РФ фиксирует снижение на 0,2 % зарегистрированных киберпреступлений, в том числе на 15,3 % – совершенных с использованием расчетных карт и на 15,4 % – совершенных с использованием компьютерной техники и средств мобильной связи [3]. Особенно остро проблема затрагивает социально уязвимые группы, становясь инструментом мошенничества, психологического давления и манипуляции.

В-третьих, разработана теоретико-методологическое обоснование. Значительное место в аспекте технологий социально-информационной безопасности в социальной работе занимают исследования: Е. А. Евстифеевой, Р. Н. Мамедова, А. В. Старшиновой, А. А. Тягуновой и В. Н. Ясенева и других.

Современные технологии активно внедряются в социальную сферу, но подготовка специалистов по вопросам кибербезопасности недостаточна. Многие специалисты по социальной работе не владеют методами защиты данных, что повышает риски утечек и неправомерного использования информации. Данное противоречие подчеркивает необходимость разработки эффективных методов социально-информационной безопасности (Дементьев, 2021, с. 45).

Практическое значение исследования заключается в разработке рекомендаций по повышению уровня информационной безопасности в социальной работе. В первую очередь, необходимо внедрить систематическое обучение специалистов по социальной работе, направленное на развитие цифровой грамотности и формирование навыков использования современных средств защиты данных. Обучение должно проводиться не только на уровне отдельных учреждений, но и системно, что позволит создать единый стандарт защиты информации во всех организациях, оказывающих социальные услуги. Дополнительно, результаты исследования могут послужить основой для модернизации внутренней инфраструктуры социальных учреждений, что позволит эффективно противостоять угрозам утечки информации и кибератакам. Особое внимание следует уделить интеграции инновационных технологий в повседневную практику работы, что обеспечит не только защиту данных, но и повышение доверия со стороны клиентов социальных служб (Старшинова, Иванова, Петров, 2020, с.147).

Перспективы исследований включают разработку интегрированных систем мониторинга для оперативного реагирования на угрозы. Предлагается создание межведомственных рабочих групп из IT-специалистов, юристов и соцработников для выработки единых стандартов защиты данных. Это повысит эффективность инноваций в соцзащите. Важно также адаптировать законодательство к цифровой экономике и формировать культуру

безопасности. Реализация этих мер станет основой комплексной стратегии информационной безопасности, укрепит доверие населения и повысит качество соцуслуг (Дементьев, 2018, с. 222; Абасбеков, 2023, с.9).

Особое внимание в исследовании уделено анализу существующих проблем в работе с информационными системами социальных учреждений. Внедрение современных технологий требует значительных финансовых и организационных затрат, что становится серьезным препятствием для многих организаций. Однако государственная поддержка и развитие цифровой инфраструктуры могут стать решающими факторами в повышении уровня информационной безопасности.

Опытно-экспериментальное исследование проводилось на базе Института педагогики и психологии Костромского государственного университета. В нем приняли участие 100 респондентов: студенты, преподаватели и специалисты социальной сферы. Результаты показали, что 96,7% опрошенных относят к персональным данным имя, фамилию, дату рождения и номер паспорта, однако только 46,7% включают в этот список биографические сведения, а 56,7% [U+2012] фотографии. ФЗ «О персональных данных» знают 90% респондентов, но 10% затруднились с ответом или выбрали неверный вариант. Основными угрозами участники исследования назвали несанкционированный доступ (93,3%) и слабую защиту информационных систем (86,7%), при этом лишь 53,3% осознают опасность вирусных атак. Из защитных мер чаще всего используют сложные пароли (80%), но регулярно их меняют только 43,3%. Биометрическая и многофакторная аутентификация применяются редко (53,3% и 13,3% соответственно). Половина респондентов (50%) никогда не проходила обучение по защите персональных данных, а 23,3% делают это регулярно. Кроме того, низкий уровень доверия клиентов к специалистам затрудняет сбор информации и продуктивное взаимодействие. Результаты демонстрируют, что комплексный подход, включающий модернизацию нормативной базы, системное обучение специалистов и активное внедрение инновационных технологий, позволяет существенно снизить риски утечек информации и повысить эффективность работы социальных служб.

Таким образом, проведенное исследование подтверждает, что обеспечение социально-информационной безопасности требует комплексного подхода, включающего как совершенствование нормативно-правовой базы, так и развитие профессиональных компетенций специалистов. В условиях цифровизации защита персональных данных становится критически важной для эффективного функционирования социальных учреждений и повышения качества оказываемых услуг. Разработка и реализация рекомендаций, вытекающих из данного исследования, позволит создать условия для устойчивого развития социальной работы в цифровую эпоху, снизить риски утечек информации и обеспечить безопасность как работников, так и клиентов социальных служб.

Источники и литература

- 1) Абасбеков Н. З. Классификация угроз информационной безопасности. //Вестник информационной безопасности. 2023.№ 1 (58). С 9-10.
- 2) Дементьев С. А. Информационная безопасность человека в контексте рисков и угроз информационной эпохи: дис. ... д-ра филос. наук: 09.00.11. Краснодар, 2018. 343 с.
- 3) Краткая характеристика состояния преступности в Российской Федерации за январь 2025 года. Министерство внутренних дел Российской Федерации. офиц. сайт. [U+2012] URL: <https://мвд.рф/reports/item/61640492/> (дата обращения: 24.02.2025).
- 4) Современные технологии социальной работы: учебное пособие / А. В. Старшинова, Е. Б. Архипова, М. В. Миронова [и др.]; под общей редакцией А. В. Старшиновой. Екатеринбург: УрФУ, 2019. 168 с.

Иллюстрации



Справка о проверке на наличие заимствований

Имя файла: Ломоносов-2025. Соколова Дарья (2).docx

Автор: Не указан

Заглавие:

Год публикации: 2025

Комментарий: [по билету NRBB-Q73H-MJZV-WEWB]

Коллекции: Интернет 2.0, Научные статьи 2.0, Русскоязычная Википедия, Англоязычная Википедия, Коллекция Энциклопедий, Библиотека Либрусек, Университетская библиотека, Коллекция КФУ, ВКР Российского университета кооперации, Коллекция АПУ ФСИН, Коллекция ПГУТИ, Репозиторий открытого доступа СПб гос. ун-та, Научная электронная библиотека "КиберЛенинка", ЦНМБ Сеченова, Авторефераты ВАК, Диссертации ВАК, Диссертации РГБ, Авторефераты РГБ, Готовые рефераты, ФИПС. Изобретения, ФИПС. Полезные модели, ФИПС. Промышленные образцы, Коллекция Руконт, Библиотека им. Ушинского, Готовые рефераты (часть 2), Открытые научные источники, НЭБ, БиблиоРоссики, Правовые документы I, Правовые документы II, Правовые документы III, Собрание законодательства Российской Федерации



Результат проверки

Оценка оригинальности документа: 86%

Оригинальные фрагменты: 85,78%

Обнаруженные заимствования: 13,43%

Цитирование: 0,79%

86%

13% 1%

Работу проверил: Воронина И.В.

Дата:

Подпись: