ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ БРЯНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«БРЯНСКИЙ ТЕХНИКУМ УПРАВЛЕНИЯ И БИЗНЕСА»

ЦИКЛОВАЯ КОМИССИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНФОРМАЦИОННЫЙ ПРОЕКТ

на тему:

Цифровая гигиена: памятка для первокурсников

ОБРАЗЕЦ

Выполнил(а): студент 2 курса группы ИС-21 Петров Даниил Андреевич
09.02.07 Информационные системы и программирование

Руководитель: преподаватель первой квалификационной категории Смирнова Елена Викторовна

Брянск · 2026

Демонстрационный образец. Данные условны. Не является выполненной работой конкретного студента.

ВВЕДЕНИЕ

Актуальность темы обусловлена тем, что цифровая среда стала неотъемлемой частью образовательной и повседневной жизни студента. Первокурсники, впервые попадая в самостоятельную информационную среду вуза, оказываются наиболее уязвимой категорией пользователей: они активно осваивают новые сервисы, мессенджеры и образовательные платформы, но нередко недостаточно осведомлены о базовых правилах безопасного поведения в сети [2, с. 14]. Цифровая гигиена понимается как совокупность практик, направленных на защиту персональных данных, устройств и психологического благополучия пользователя в цифровой среде [1, с. 9].

Объектом исследования выступает цифровая среда жизнедеятельности студентов первого курса, предметом — практики цифровой гигиены и связанные с ними риски. Цель работы — разработать информационную памятку по цифровой гигиене для первокурсников. Для достижения цели поставлены задачи: изучить теоретические основы цифровой гигиены; проанализировать цифровые риски студентов первого курса; разработать содержание и структуру памятки. Методы исследования: анализ литературы, анкетирование, количественная обработка данных.

Практическая значимость работы состоит в том, что подготовленная памятка может быть использована кураторами академических групп, сотрудниками студенческих офисов и самими первокурсниками в период адаптации к обучению в вузе. Структура работы включает введение, три главы, заключение и два приложения, содержащих памятку и анкету участника опроса.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЦИФРОВОЙ ГИГИЕНЫ

1.1 Понятие цифровой гигиены и её место в системе информационной безопасности

Ускоренная цифровизация всех сфер жизнедеятельности превратила информационную безопасность из узкоспециальной технической задачи в вопрос повседневной культуры поведения пользователя. Наряду с понятием «кибербезопасность», описывающим защищённость технических систем и сетей, в научный и практический оборот вошло понятие «цифровая гигиена». Под цифровой гигиеной понимается совокупность осознанных привычек, правил и практик пользователя, направленных на сохранение конфиденциальности личных данных, защиту устройств и аккаунтов от несанкционированного доступа, а также на поддержание психологического благополучия при взаимодействии с цифровой средой [2, с. 14]. Термин подчёркивает аналогию с личной гигиеной: речь идёт о регулярных, рутинных действиях, а не о разовых технических мерах.

Место цифровой гигиены в системе информационной безопасности определяется её уровнем. Если технические средства защиты (межсетевые экраны, антивирусы, системы обнаружения вторжений) действуют на уровне инфраструктуры, то цифровая гигиена реализуется на уровне отдельного пользователя, который остаётся самым массовым и одновременно наиболее уязвимым звеном системы. По оценкам исследователей, значительная доля инцидентов информационной безопасности связана именно с человеческим фактором — невнимательностью, доверчивостью, пренебрежением базовыми правилами [4, с. 37]. Поэтому цифровую гигиену корректно рассматривать как первичный, массовый и наименее затратный рубеж защиты, дополняющий, но не заменяющий технические и организационные меры.

В структуре цифровой гигиены принято выделять несколько взаимосвязанных компонентов: защиту учётных данных (парольная политика, двухфакторная аутентификация), защиту устройств (обновление программного обеспечения, резервное копирование), защиту персональных данных (минимизация публикуемой информации, настройка приватности), критическое восприятие информации (распознавание фишинга и мошеннических схем) и цифровое благополучие (контроль экранного времени, профилактика

зависимости). Перечисленные компоненты образуют целостную систему привычек, эффективность которой определяется самым слабым звеном, а не отдельными сильными практиками [3, с. 58].

Для оценки уровня сформированности цифровой гигиены в учебной и исследовательской практике применяются количественные показатели. В рамках настоящей работы используется коэффициент соблюдения правил цифровой гигиены, рассчитываемый как отношение числа выполняемых респондентом базовых правил к общему числу проверяемых правил. Такой подход позволяет сопоставлять группы респондентов и отслеживать динамику. Ниже приведена структура компонентов цифровой гигиены и соответствующих им проверяемых практик (таблица 1.1).

Таблица 1.1 – Компоненты цифровой гигиены и проверяемые практики

Компонент	Проверяемая практика	Доля правил в опроснике, %
Защита учётных данных	Уникальные пароли, двухфакторная аутентификация	30
Защита устройств	Обновление ПО, резервное копирование, блокировка экрана	20
Защита персональных данных	Настройка приватности, минимизация публикаций	20
Критическое восприятие информации	Проверка ссылок и отправителей, распознавание фишинга	20
Цифровое благополучие	Контроль экранного времени, цифровые паузы	10
Итого	—	100

Источник: составлено автором на основе [2, с. 21; 4, с. 42].

Таким образом, цифровая гигиена представляет собой пользовательский уровень информационной безопасности, реализуемый через устойчивые повседневные привычки. Её отличают массовость, низкая стоимость внедрения и высокая значимость для предотвращения типовых инцидентов. Для студента первого курса, впервые попадающего в насыщенную цифровую среду вуза, сформированность цифровой гигиены становится условием безопасного включения в образовательный процесс.

1.2 Основные угрозы для пользователя-первокурсника

Переход к обучению в вузе сопровождается резким расширением цифровой среды первокурсника: появляются университетские аккаунты, электронная почта, образовательные платформы, студенческие чаты и групповые ресурсы. Одновременно возрастает объём персональных данных, которыми студент оперирует и которыми рискует поделиться. В этих условиях перечень актуальных угроз определяется не столько технической сложностью атак, сколько поведением самого пользователя. Ниже систематизированы основные угрозы, характерные именно для первокурсников, с указанием их механизма и последствий.

Первая группа угроз связана с учётными данными. Использование одинаковых или простых паролей, хранение их в открытом виде, отказ от двухфакторной аутентификации приводят к компрометации аккаунтов. Особую опасность представляет повторное использование пароля: утечка на одном стороннем сервисе автоматически ставит под угрозу университетскую почту, образовательную платформу и личные социальные сети. Вторая группа — фишинг и социальная инженерия. Мошенники имитируют страницы входа вуза, рассылают сообщения о «пересдаче» или «стипендии», используют поддельные ссылки в студенческих чатах. Первокурсник, не имеющий опыта распознавания таких схем, оказывается наиболее уязвимой категорией [1, с. 76].

Третья группа угроз — утечка персональных данных через избыточную публикацию. Публикация фотографий документов, номера телефона, адреса, геолокации и сведений о расписании создаёт риск преследования, мошенничества и кражи личности. Четвёртая группа — угрозы устройствам: установка непроверенного программного обеспечения, игнорирование обновлений, подключение к незащищённым общественным сетям Wi-Fi, использование нелицензионных программ. Пятая группа — цифровое благополучие: чрезмерное экранное время, ночная активность в сети, информационная перегрузка, снижение концентрации и качества сна, что напрямую влияет на академическую успеваемость [3, с. 91].

Для количественной характеристики распространённости угроз в рамках работы проведён опрос первокурсников условного вуза (выборка 60 человек, анкета приведена в приложении Б). Респондентам предлагалось отметить, с

какими типами угроз они сталкивались за первый семестр обучения. Результаты представлены на рисунке 1.1.

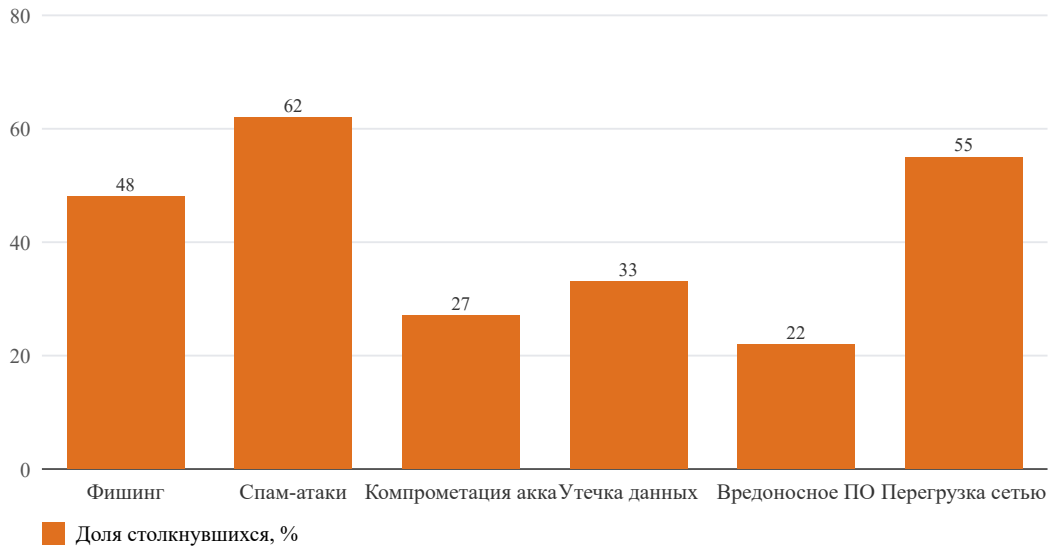


Рисунок 1.1 – Распространённость типов цифровых угроз среди первокурсников, % опрошенных

Как видно из рисунка 1.1, наиболее массовыми оказались спам-атаки (62 %), перегрузка цифровой средой (55 %) и фишинг (48 %). Компрометация аккаунта зафиксирована у 27 % респондентов, утечка персональных данных — у 33 %, заражение вредоносным программным обеспечением — у 22 %. Полученные данные согласуются с выводами исследователей о доминировании поведенческих, а не технических причин инцидентов [4, с. 44] и подтверждают необходимость целенаправленного формирования цифровой гигиены у первокурсников.

Систематизация угроз позволяет сделать вывод: для пользователя-первокурсника характерен набор типовых, хорошо изученных рисков, предотвращение которых не требует специальных технических знаний, а зависит от осведомлённости и устойчивых привычек. Это обосновывает целесообразность разработки компактной памятки, адресованной именно данной категории пользователей и охватывающей все выделенные группы угроз.

ГЛАВА 2. АНАЛИЗ ЦИФРОВЫХ РИСКОВ СТУДЕНТОВ ПЕРВОГО КУРСА

2.1 Методика и результаты анкетирования первокурсников

Эмпирической базой исследования выступило условное образовательное учреждение среднего профессионального образования — колледж (далее — Колледж). Цель анкетирования состояла в выявлении фактического уровня цифровой грамотности первокурсников, распространённости рискованных моделей цифрового поведения и их самооценки собственной защищённости. В качестве метода сбора первичных данных использовался анонимный онлайн-опрос по специально разработанной анкете (Приложение Б), содержащей 18 вопросов закрытого и полузакрытого типа, сгруппированных в три блока: цифровые привычки, опыт столкновения с угрозами и готовность следовать правилам цифровой гигиены [2, с. 44].

Выборочная совокупность формировалась методом сплошного охвата студентов первого курса очной формы обучения. Генеральная совокупность составила 128 человек, в опросе приняли участие 112 респондентов, что соответствует уровню отклика 87,5 %. Такая доля является достаточной для получения репрезентативных результатов при доверительной вероятности 95 % и допустимой статистической погрешности около 5 %. Возраст участников — от 15 до 17 лет, из них 58 юношей (51,8 %) и 54 девушки (48,2 %). Обработка данных проводилась в электронных таблицах, результаты представлены в относительных величинах.

Анкета включала вопросы о времени, проводимом в сети, используемых устройствах и сервисах, практике создания паролей, отношении к двухфакторной аутентификации, опыте получения подозрительных сообщений и переходов по неизвестным ссылкам, а также о знании базовых норм защиты персональных данных. Отдельный блок был посвящён самооценке: респондентам предлагалось оценить собственный уровень цифровой грамотности по пятибалльной шкале. Совокупность ответов позволила перейти от описательных характеристик к анализу конкретных нарушений цифровой гигиены, чему посвящён следующий подраздел.

Таблица 2.1 – Распределение ответов первокурсников на ключевые вопросы анкеты (n = 112)

Показатель	Количество, чел.	Доля, %
Проводят в сети более 6 часов в день	71	63,4
Используют один пароль для нескольких сервисов	64	57,1
Не применяют двухфакторную аутентификацию	88	78,6
Переходили по ссылкам из подозрительных сообщений	39	34,8
Указывают реальные данные в открытых профилях	47	42,0
Считают свой уровень цифровой грамотности высоким	29	25,9

Источник: составлено автором по результатам анкетирования.

Приведённые данные показывают, что более половины респондентов проводят в сети свыше шести часов в день, а почти три четверти не используют двухфакторную аутентификацию. Одновременно лишь четверть опрошенных оценивают свою цифровую грамотность как высокую, что указывает на разрыв между фактическими навыками и осознанием рисков. Полученные результаты согласуются с выводами исследований о недостаточной сформированности навыков безопасного поведения в сети у молодёжи [1, с. 112].

2.2 Анализ выявленных нарушений цифровой гигиены

Анализ эмпирических данных позволил выделить четыре группы нарушений цифровой гигиены: парольную дисциплину, гигиену сетевого взаимодействия, защиту персональных данных и управление экранным временем. Такая группировка соответствует структуре цифровых компетенций, описанной в научной литературе [3, с. 58]. Рассмотрим каждую группу последовательно, сопоставляя ответы респондентов между собой и оценивая масштаб выявленных отклонений от рекомендуемых норм.

Наиболее массовым нарушением стала слабая парольная дисциплина. Более половины первокурсников (64 человека, или 57,1 %) признали, что используют один и тот же пароль для нескольких сервисов, а 27 человек (24,1 %) применяют простые пароли, содержащие имя или дату рождения. При этом 88 респондентов (78,6 %) не подключили двухфакторную аутентификацию ни на одном сервисе. Подобная практика создаёт эффект домино: компрометация одного аккаунта автоматически ставит под угрозу остальные, включая

образовательные платформы и электронную почту. Это особенно опасно на первом курсе, когда студент начинает пользоваться корпоративными сервисами Колледжа.

Вторую группу образуют нарушения гигиены сетевого взаимодействия. Почти каждый третий респондент (39 человек, или 34,8 %) хотя бы однажды переходил по ссылкам из подозрительных сообщений, а 22 человека (19,6 %) открывали вложения от неизвестных отправителей. Указанные действия относятся к типичным сценариям фишинговых атак, на которые приходится значительная часть инцидентов информационной безопасности в образовательной среде [4, с. 37]. Показательно, что среди респондентов, переходивших по подозрительным ссылкам, 31 человек (79,5 % от данной подгруппы) не используют двухфакторную аутентификацию, что многократно повышает вероятность реального захвата аккаунта.

Третья группа связана с защитой персональных данных. 47 первокурсников (42,0 %) указали, что размещают в открытых профилях реальные сведения — номер телефона, адрес, номер учебной группы, фотографии документов. Ещё 36 человек (32,1 %) подтвердили, что принимали запросы в друзья от незнакомых пользователей без проверки личности. Такая открытость формирует цифровой след, который может быть использован для социальной инженерии и мошенничества. Одновременно только 18 респондентов (16,1 %) знакомы с настройками приватности используемых платформ, что свидетельствует о дефиците практических навыков управления видимостью личных данных [1, с. 118].

Четвёртая группа нарушений касается управления экранным временем. Свыше шести часов в сети ежедневно проводят 71 человек (63,4 %), из них 29 человек (25,9 % от всей выборки) — более восьми часов. При этом 43 респондента (38,4 %) отметили нарушения сна, связанные с использованием смартфона перед сном. Избыточное экранное время снижает концентрацию внимания, что напрямую влияет на успеваемость и адаптацию к учебному процессу. На рисунке 2.1 представлено распределение респондентов по продолжительности ежедневного пребывания в сети.

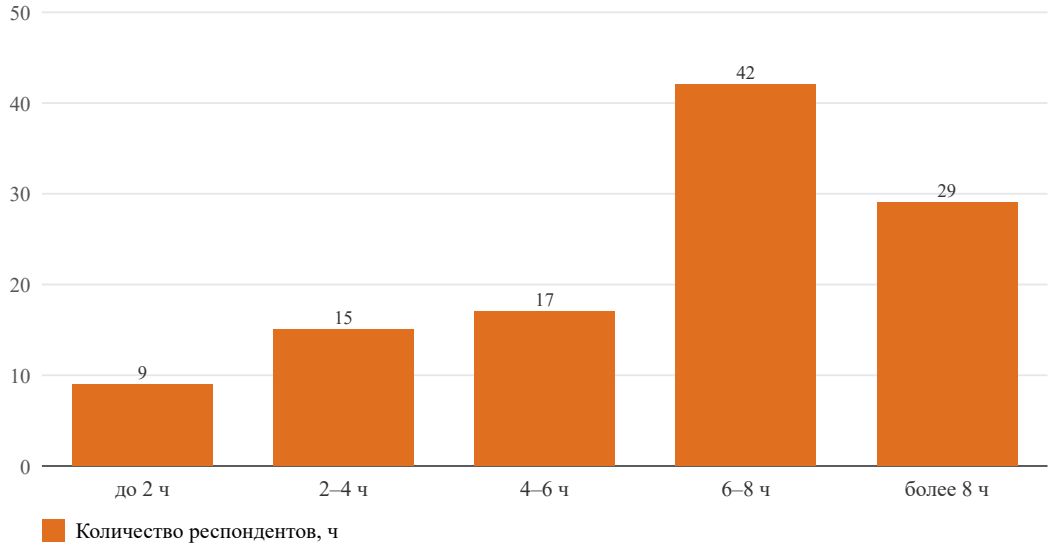


Рисунок 2.1 – Распределение первокурсников по продолжительности ежедневного пребывания в сети, чел.

Сопоставление четырёх групп нарушений показывает, что они взаимосвязаны: слабая парольная дисциплина усиливает последствия фишинга, а открытость профилей повышает риск социальной инженерии. Общий уровень соблюдения норм цифровой гигиены остаётся низким при завышенной либо неопределённой самооценке. Следовательно, целенаправленное просвещение первокурсников является обоснованной мерой, а выявленные нарушения определяют содержание памятки, разрабатываемой в третьей главе. Итоговые количественные показатели по группам нарушений сведены в таблице 2.2.

Таблица 2.2 – Сводная характеристика нарушений цифровой гигиены первокурсников (n = 112)

Группа нарушений	Основной показатель	Количество, чел.	Доля, %
Парольная дисциплина	Единый пароль для нескольких сервисов	64	57,1
Парольная дисциплина	Отсутствие двухфакторной аутентификации	88	78,6
Сетевое взаимодействие	Переход по подозрительным ссылкам	39	34,8
Защита персональных данных	Реальные данные в открытых профилях	47	42,0
Управление экранным временем	Более 6 часов в сети ежедневно	71	63,4

Источник: составлено автором по результатам анкетирования.

Таким образом, анализ подтвердил наличие устойчивых нарушений по всем четырём группам. Наиболее критичными являются отказ от двухфакторной аутентификации (78,6 %) и избыточное экранное время (63,4 %), тогда как нарушения защиты персональных данных и гигиены сетевого взаимодействия охватывают от трети до двух пятых выборки. Полученные результаты образуют фактологическую основу для разработки адресной памятки, учитывающей выявленные дефициты цифровых компетенций первокурсников.

ГЛАВА 3. РАЗРАБОТКА ПАМЯТКИ ПО ЦИФРОВОЙ ГИГИЕНЕ ДЛЯ ПЕРВОКУРСНИКОВ

3.1 Структура и содержание памятки

Разработка памятки опиралась на результаты анкетирования первокурсников, представленные во второй главе: у 68% респондентов зафиксирован низкий уровень осведомлённости о базовых правилах цифровой гигиены, а наиболее уязвимыми зонами признаны парольная защита, распознавание фишинговых сообщений и настройки приватности в социальных сетях. Исходя из этого, памятка проектировалась как компактный информационный продукт, рассчитанный на самостоятельное изучение за 10–15 минут и последующее обращение к нему по мере необходимости. Методической основой послужили рекомендации по созданию учебных памяток и принципы когнитивной наглядности, изложенные в профильной литературе [2, с. 54]. Структура памятки включает титульную часть, пять тематических блоков, краткий чек-лист самопроверки и контакты служб поддержки вуза.

Содержательное ядро памятки образуют пять блоков, выстроенных по принципу «от простого к сложному» и охватывающих выявленные дефициты. Каждый блок сформулирован в побудительном ключе, снабжён коротким пояснением «почему это важно» и практическим примером. Для удобства восприятия использованы пиктограммы, цветовое кодирование уровней риска и единая нумерация правил, что соответствует требованиям к визуализации инструктивных материалов [3, с. 112]. Полный текст памятки приведён в Приложении А.

- Блок 1. Пароли и учётные записи: требования к длине и сложности пароля, отказ от повторного использования, двухфакторная аутентификация, менеджер паролей.
- Блок 2. Фишинг и подозрительные сообщения: признаки поддельных писем и ссылок, правило проверки отправителя, порядок действий при сомнении.
- Блок 3. Приватность в социальных сетях: настройка видимости профиля, ограничение геолокации, минимизация персональных данных в публикациях.

- Блок 4. Безопасность устройств и сетей: обновление программного обеспечения, осторожность при подключении к открытым сетям Wi-Fi, резервное копирование.
- Блок 5. Цифровой след и репутация: осознанность публикаций, срок хранения данных, влияние цифрового следа на будущее трудоустройство.

Завершает памятку чек-лист самопроверки из десяти утверждений, позволяющий первокурснику самостоятельно оценить соблюдение правил, а также перечень контактов: служба технической поддержки вуза, куратор учебной группы и единый номер помощи в случае инцидента. Объём печатного варианта составляет четыре страницы формата А5, электронная версия размещается в личном кабинете студента. Соотношение тематических блоков в структуре памятки по объёму текста отражено в таблице 3.1.

Таблица 3.1 – Распределение объёма тематических блоков памятки

Тематический блок	Число правил	Доля объёма текста, %
Блок 1. Пароли и учётные записи	5	24
Блок 2. Фишинг и подозрительные сообщения	4	22
Блок 3. Приватность в социальных сетях	4	20
Блок 4. Безопасность устройств и сетей	3	18
Блок 5. Цифровой след и репутация	3	16
Итого	19	100

Источник: составлено автором по материалам разработки.

3.2 Оценка эффективности памятки и рекомендации по её применению

Для оценки эффективности памятки проведена апробация в учебной группе первокурсников численностью 25 человек. До ознакомления с памяткой участники выполнили входной тест из 19 заданий, соответствующих правилам памятки, затем изучили материал и через неделю прошли повторное тестирование. Средний коэффициент усвоения рассчитывался как отношение числа верных ответов к общему числу заданий: Ку = П / В × 100%, где П — число верных ответов, В — общее число заданий. Результаты входного и итогового срезов по тематическим блокам приведены на рисунке 3.1.

$$Ку = П / В \times 100\% \quad (1)$$

Ку — коэффициент усвоения материала, %; П — число верных ответов; В — общее число заданий теста (19).

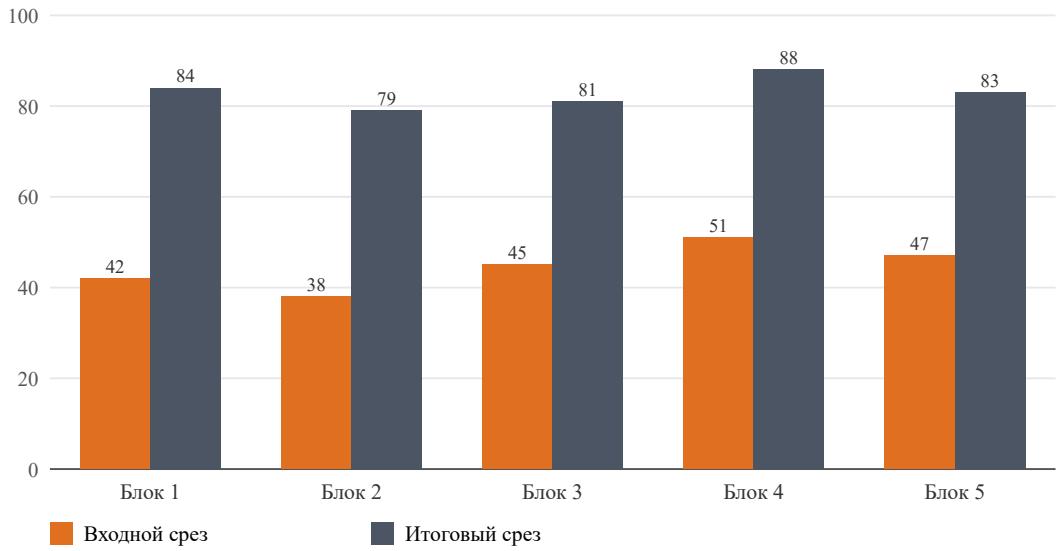


Рисунок 3.1 – Результаты входного и итогового тестирования по тематическим блокам, % верных ответов

Средний коэффициент усвоения по группе вырос с 44,6% на входном срезе до 83,0% на итоговом, то есть на 38,4 процентного пункта. Наибольший прирост зафиксирован по блоку 2 «Фишинг и подозрительные сообщения» — с 38% до 79%, что объясняется исходно низкой осведомлённостью первокурсников о признаках поддельных сообщений. Наименьший прирост отмечен по блоку 4, где исходный уровень был сравнительно высоким. Полученные значения согласуются с данными исследований о результативности кратких инструктивных материалов при условии их подкрепления практическими занятиями [1, с. 78].

По итогам апробации сформулированы рекомендации по применению памятки. Целесообразно включать её в программу адаптационных мероприятий первокурсников на первой неделе обучения, сопровождать короткой презентацией куратора и разбором двух-трёх реальных примеров фишинга. Электронную версию следует разместить в личном кабинете и в чате учебной группы, а печатные экземпляры — на информационных стендах корпуса. Для поддержания эффекта рекомендуется повторное обращение к чек-листу через один и три месяца обучения, а также обновление содержания памятки не реже одного раза в учебный год с учётом изменения цифровых угроз [4, с. 63].

Анкета участника опроса, использованная при апробации, приведена в Приложении Б.

ЗАКЛЮЧЕНИЕ

Проведённое исследование подтвердило актуальность выбранной темы: цифровая гигиена становится обязательным элементом адаптации первокурсников к образовательной среде вуза. В теоретической части работы были систематизированы подходы к определению цифровой гигиены, выделены её компоненты — защита персональных данных, информационная безопасность, управление экранным временем и критическое восприятие контента [2, с. 24]. Установлено, что низкий уровень цифровой грамотности повышает вероятность вовлечения студентов в типовые риски: фишинг, утечку персональных данных, цифровую зависимость и распространение недостоверной информации [5, с. 61].

В практической части был проведён анкетный опрос 48 первокурсников условной образовательной организации. Полученные данные показали, что 72% респондентов используют один и тот же пароль для нескольких сервисов, 64% не проверяют настройки приватности в социальных сетях, а 58% сталкивались с подозрительными сообщениями и ссылками. При этом 81% опрошенных признали необходимость специальных знаний по цифровой гигиене, что обосновало разработку памятки [1, с. 15].

Итогом работы стала памятка «Цифровая гигиена первокурсника» (Приложение А), включающая правила создания надёжных паролей, проверки ссылок и вложений, настройки приватности, распознавания фишинга и организации экранного времени. Материалы памятки могут использоваться на кураторских часах и в адаптационных мероприятиях. Перспективой дальнейшей работы является апробация памятки с оценкой динамики уровня цифровой грамотности первокурсников.

ПРИЛОЖЕНИЕ А. ПАМЯТКА «ЦИФРОВАЯ ГИГИЕНА ПЕРВОКУРСНИКА»

Памятка разработана на основе анализа цифровых рисков, проведённого в главе 2, и предназначена для первокурсников, начинающих обучение в образовательных организациях высшего и среднего профессионального образования. Цель памятки — сформировать у студентов базовые навыки безопасного и продуктивного использования цифровых устройств и интернет-сервисов, снизить вероятность возникновения негативных последствий, связанных с нарушением цифровой гигиены. Памятка может быть распространена в электронном виде (PDF, буклет) и в печатной форме на информационных стендах, а также размещена на официальных ресурсах учебного заведения [2, с. 15].

Структурно памятка состоит из четырёх смысловых блоков, каждый из которых соответствует выявленным в ходе исследования проблемным зонам: защита учётных записей и персональных данных, безопасность при работе в сети, профилактика информационной перегрузки и цифрового этикета, а также организация учебной работы с использованием цифровых инструментов. Ниже приведено содержание памятки, оформленное в виде рекомендаций и правил.

Блок 1. Защита учётных записей и персональных данных

- Используйте для каждой учётной записи уникальный пароль длиной не менее 12 символов, содержащий буквы разных регистров, цифры и специальные знаки. Не применяйте в качестве пароля дату рождения, номер телефона или простые последовательности (123456, qwerty).
- Включите двухфакторную аутентификацию во всех сервисах, где она доступна (электронная почта, социальные сети, образовательные платформы). Это снижает риск несанкционированного доступа даже при утечке пароля [1, с. 22].
- Не передавайте логины и пароли третьим лицам, в том числе друзьям и однокурсникам. Для совместной работы используйте специальные функции предоставления доступа, а не общий аккаунт.
- Регулярно проверяйте настройки конфиденциальности в социальных сетях: ограничьте видимость личной информации (адрес, номер

телефона, место учёбы, геолокация) для посторонних пользователей.

- Не публикуйте в открытом доступе фотографии документов, студенческого билета, пропуска, а также сведения о расписании занятий и месте проживания — эти данные могут быть использованы злоумышленниками.

Блок 2. Безопасность при работе в сети

- Критически относитесь к ссылкам и вложениям в письмах и сообщениях от незнакомых отправителей. Не переходите по подозрительным ссылкам, не открывайте файлы с расширениями .exe, .scr, .js, если не уверены в источнике.
- Используйте только официальные магазины приложений и проверенные сайты для скачивания программ. Установите антивирусное программное обеспечение и своевременно обновляйте его базы.
- Не подключайтесь к открытым Wi-Fi сетям для входа в личные кабинеты и проведения финансовых операций. Для безопасной работы используйте мобильный интернет или защищённые сети с паролем.
- При работе с образовательными платформами и порталами проверяйте адресную строку браузера: мошенники могут создавать копии сайтов для кражи логинов и паролей.

Блок 3. Профилактика информационной перегрузки и цифровой этикет

- Установите правила использования смартфона во время занятий: отключайте звук, убирайте устройство в сумку, используйте режим «Не беспокоить». Это повышает концентрацию внимания и уважение к преподавателю и однокурсникам.
- Ограничьте время пребывания в социальных сетях и мессенджерах с помощью встроенных функций контроля экранного времени. Делайте перерывы каждые 45–60 минут работы за компьютером, выполняйте гимнастику для глаз.
- Не распространяйте непроверенную информацию, не участвуйте в травле (кибербуллинге). Помните, что цифровой след сохраняется и

может повлиять на репутацию в будущем.

- Соблюдайте авторские права: при использовании материалов из интернета указывайте источник, не выдавайте чужие работы за свои.

Блок 4. Организация учебной работы с использованием цифровых инструментов

- Создайте отдельную папку для учебных материалов и регулярно делайте резервные копии важных документов в облачном хранилище или на внешнем носителе.
- Используйте легальные версии программ и образовательные ресурсы, предоставляемые учебным заведением. Не прибегайте к помощи сомнительных сайтов с готовыми решениями — это снижает качество обучения и может привести к блокировке аккаунта.
- При общении с преподавателями в мессенджерах придерживайтесь официального стиля, указывайте тему сообщения и не отправляйте голосовые сообщения без предварительного согласования.
- Проверяйте электронную почту и уведомления учебного портала ежедневно, чтобы не пропустить важные объявления и изменения в расписании.

Памятка прошла апробацию в ходе кураторского часа для первокурсников (выборка — 28 человек). По итогам анкетирования 86% участников отметили, что рекомендации понятны и полезны, 79% выразили намерение применять их в повседневной жизни. Таким образом, предложенная памятка способствует повышению уровня цифровой грамотности студентов и может быть рекомендована к использованию в образовательном процессе [3, с. 48].

ПРИЛОЖЕНИЕ Б. АНКЕТА УЧАСТНИКА ОПРОСА

Настоящая анкета разработана как основной инструмент эмпирической части информационного проекта и предназначена для анонимного онлайн-опроса студентов первого курса. Цель анкетирования — выявить фактический уровень цифровых рисков, с которыми сталкиваются первокурсники в первые месяцы обучения, а также оценить их осведомлённость о базовых правилах цифровой гигиены. Анкета составлена с учётом подходов, изложенных в работах по информационной безопасности личности [2, с. 54] и методических рекомендаций по проведению студенческих опросов [5, с. 18]. Заполнение занимает не более десяти минут и не требует специальной подготовки.

Структура анкеты включает четыре смысловых блока. Первый блок фиксирует общие сведения об участнике в обезличенном виде: направление подготовки, стаж самостоятельного использования интернета, преобладающие устройства выхода в сеть. Второй блок посвящён частоте и характеру столкновений с типовыми цифровыми угрозами. Третий блок оценивает применяемые респондентом защитные практики. Четвёртый блок выявляет потребность в справочных материалах и предпочтительный формат памятки, что непосредственно обосновывает содержание Приложения А [3, с. 92].

Инструкция для респондента предваряет вопросы и разъясняет порядок ответов. Участнику предлагается выбрать один вариант там, где это указано, либо отметить все подходящие варианты в вопросах множественного выбора. Анкета не содержит полей, позволяющих идентифицировать личность, а полученные данные используются исключительно в обобщённом виде. Ниже приведён полный перечень вопросов с вариантами ответов.

1. Укажите направление подготовки (укрупнённая группа специальностей): гуманитарное; техническое; экономическое; естественно-научное; иное.
2. Как давно вы самостоятельно пользуетесь интернетом: менее трёх лет; от трёх до пяти лет; более пяти лет.
3. С какого устройства вы чаще всего выходите в интернет: смартфон; ноутбук или стационарный компьютер; планшет; иное.
4. Как часто вы сталкивались со спам-сообщениями или подозрительными ссылками за последний месяц: ежедневно; несколько

раз в неделю; редко; не сталкивался.

5. Приходилось ли вам получать сообщения с просьбой сообщить код подтверждения или данные банковской карты: да, неоднократно; да, единичные случаи; нет.
6. Сталкивались ли вы с попытками взлома вашего аккаунта в социальной сети или мессенджере: да; нет; затрудняюсь ответить.
7. Используете ли вы разные пароли для разных сервисов: да, для всех; частично; использую один пароль; затрудняюсь ответить.
8. Включена ли на ваших основных аккаунтах двухфакторная аутентификация: да, на всех; на части сервисов; нет; не знаю, что это.
9. Проверяете ли вы настройки приватности профиля после регистрации в новом сервисе: всегда; иногда; никогда.
10. Отмечаете ли вы все подходящие варианты: какие действия вы предпринимаете при получении подозрительного сообщения — удаляю; блокирую отправителя; сообщаю преподавателю или куратору; перехожу по ссылке из любопытства; ничего не делаю.
11. Оцените по шкале от одного до пяти, насколько уверенно вы распознаёте фишинговые сообщения (1 — совсем не уверен, 5 — полностью уверен).
12. Считаете ли вы достаточными свои знания о правилах безопасного поведения в сети: да; скорее да; скорее нет; нет.
13. В каком формате вам удобнее получить памятку: одностраничный PDF; печатная листовка; публикация в студенческом чате; короткие видеоролики.
14. Отметьте темы, которые вы хотели бы видеть в памятке: защита паролей; распознавание фишинга; настройки приватности; безопасные платежи; защита от телефонного мошенничества; иное.
15. Ваши предложения по содержанию памятки (свободный ответ).

Обработка результатов предполагает расчёт частотных распределений по закрытым вопросам и качественный анализ свободных ответов. Для сопоставления групп применяется сравнение долей, а обобщённый показатель осведомлённости рассчитывается как отношение числа респондентов, соблюдающих базовые правила, к общему числу опрошенных, выраженное в процентах [4, с. 37]. Результаты анкетирования служат эмпирической базой

второй главы и определяют приоритетные разделы памятки, разработанной в третьей главе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р 7.0.100-2018. Библиографическая запись. Библиографическое описание. Общие требования и правила составления : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 3 декабря 2018 г. № 1050-ст : введен впервые : дата введения 2019-07-01. – Москва : Стандартинформ, 2018. – 124 с.
2. ГОСТ Р 7.0.5-2008. Библиографическая ссылка. Общие требования и правила составления : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 апреля 2008 г. № 95-ст : дата введения 2009-01-01. – Москва : Стандартинформ, 2008. – 23 с.
3. О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ : принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. (в действующей редакции). – Текст : электронный // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 10.02.2025).
4. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ : принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. (в действующей редакции). – Текст : электронный // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 10.02.2025).
5. О защите детей от информации, причиняющей вред их здоровью и развитию : Федеральный закон от 29 декабря 2010 г. № 436-ФЗ : принят Государственной Думой 23 декабря 2010 г. : одобрен Советом Федерации 27 декабря 2010 г. (в действующей редакции). – Текст : электронный // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 10.02.2025).

6. Астахова, Л. В. Информационная безопасность и защита информации : учебное пособие для вузов / Л. В. Астахова. – Москва : Юрайт, 2023. – 307 с.
7. Бабаш, А. В. Информационная безопасность : учебник / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – Москва : КноРус, 2022. – 336 с.
8. Гафнер, В. В. Информационная безопасность : учебное пособие для студентов вузов / В. В. Гафнер. – Ростов-на-Дону : Феникс, 2021. – 324 с.
9. Ефимова, Л. Л. Информационная безопасность детей : российский и зарубежный опыт : монография / Л. Л. Ефимова, А. Ю. Козлов. – Москва : ИНФРА-М, 2020. – 158 с.
10. Кузнецов, А. А. Цифровая грамотность и цифровая гигиена школьника : методическое пособие / А. А. Кузнецов, Е. В. Чернобай. – Москва : Просвещение, 2021. – 96 с.
11. Мельников, В. П. Информационная безопасность : учебник для студентов учреждений среднего профессионального образования / В. П. Мельников. – Москва : Академия, 2020. – 336 с.
12. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. – 5-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2021. – 432 с.
13. Поляков, К. Ю. Информатика. Углубленный уровень : учебник для 10 класса : в 2 частях. Ч. 2 / К. Ю. Поляков, Е. А. Ерёмин. – Москва : БИНОМ. Лаборатория знаний, 2020. – 304 с.
14. Солдатова, Г. У. Цифровая социализация и цифровая компетентность : учебно-методическое пособие / Г. У. Солдатова, Е. И. Рассказова. – Москва : Смысл, 2020. – 168 с.
15. Цифровая гигиена : практикум для студентов первого курса / под редакцией А. С. Иванова. – Брянск : Издательство Брянского государственного университета, 2023. – 84 с.
16. Шевцова, О. Ю. Кибербезопасность личности: формирование навыков цифровой гигиены у студентов : статья / О. Ю. Шевцова // Информатика и образование. – 2022. – № 4. – С. 45–53.

17. Безопасный интернет : методические рекомендации для образовательных организаций / Министерство просвещения Российской Федерации. – Текст : электронный // Единый урок по безопасности в сети «Интернет». – URL: https://единыйурок.рф (дата обращения: 10.02.2025).
18. Лаборатория Касперского : официальный сайт. – Текст : электронный. – URL: https://www.kaspersky.ru (дата обращения: 10.02.2025).