Научно-исследовательская работа на тему:

Анализ различных методов аутентификации и безопасности информации в сети Интернет

Автор:

Крючкова София Ивановна

Россия, ЯНАО, г. Тарко-Сале

МБОУ «СОШ № 2», 10 класс

Научный руководитель, учитель:

Алиева Руфина Манзуровна

Учитель физики

МБОУ «СОШ № 2» г. Тарко-Сале

2024 год

**Оглавление**

[Аннотация 3](#_Toc1)

[Введение 4](#_Toc2)

[Глава 1. Основы аутентификации и безопасности информации в сети Интернет. 6](#_Toc3)

[1.1 Основные принципы аутентификации. 6](#_Toc4)

[1.2 Виды угроз безопасности информации в Интернете](#_Toc5) 7

[Глава 2. . Опрос и создание буклета о методах аутентификации и защите персональных данных. 8](#_Toc6)

[2.1. Планирование и проведение опроса о предпочтительных методах аутентификации и информировании и способах защиты 8](#_Toc7)

[2.2. Создание буклета с информацией о методах аутентификации и защите персональных данных.](#_Toc8) 8

[2.3. Оценка эффективности информирования: повторный опрос после ознакомления с методами защиты информации](#_Toc9) 9

[Список использованной литературы](#_Toc12) 11

[Приложение 1 Результаты первого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.. I](#_Toc13)

[Приложение 2. Результаты второго вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.. I](#_Toc14)

[Приложение 3. Результаты третьего вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.. I](#_Toc15)

[Приложение 4. Результаты четвертого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет. I](#_Toc16)I

[Приложение 5. Результаты пятого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.](#_Toc17) II

[Приложение 6. Результаты шестого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.](#_Toc18) III

**Анализ различных методов аутентификации и безопасности информации в сети Интернет**

**Крючкова София Ивановна**

**Россия, ЯНАО, г. Тарко-Сале**, **МБОУ «СОШ № 2»**, **10 класс**

**Аннотация**

В настоящее время Интернет становится важной частью нашей жизни, учебы и работы. На большинство Интернет-ресурсов необходимо проходить регистрацию с последующей аутентификацией. Уязвимость безопасности, когда пользователь не может подтвердить свою личность, позволяет злоумышленникам создавать поддельные физические и виртуальные продукты.

**Цель исследования:** проанализировать различные методы аутентификации и собрать рекомендательный образ в виде буклета для распространения информации о защиты личных данных в сети Интернет.

Для достижения цели исследования поставлены следующие **задачи:**

1. Изучить и проанализировать литературу по этой теме
2. Выявить основные проблемы методов аутентификации, с которыми сталкиваются пользователи сети Интернет
3. Составить рекомендации в виде буклета по информации о методах аутентификации и защиты информации в сети Интернет

**Объект исследования** — процесс повышения осведомленности учеников и учителей наш ей школы о методах аутентификации и защиты своих данных

**Предмет исследования** — распространение информации о методах дополнительной аутентификации и защиты своих данных в виде буклета

**Методы исследования:**

—теоретические (анализ литературы, изучение материала, обобщение опыта);

— эмпирические (формирование и контроль знаний, диагностика, анализ результатов).

В ходе исследования изучены самые известные методы аутентификации и способы дополнительной защиты личных данных, а также проведен опрос среди учеников и учителей нашей школы о информационной безопасности. На основе всех полученных данных сформулирован и разработан буклет по безопасности данных в сети Интернет, который получили ученики нашей школы.

**Введение**

Сейчас безопасность является одним из самых значимых аспектов, особенно когда речь идет об Интернете и онлайн-сервисах. Аутентификация — это процесс проверки подлинности пользовательского аккаунта, который обычно осуществляется путем ввода логина и пароля. Однако, традиционный метод аутентификации по логину и паролю имеет множество недостатков и уязвимостей, которые могут привести к утечке данных и несанкционированному доступу к аккаунту.

**Актуальность исследования** обусловлена необходимостью обеспечения безопасности данных в условиях быстрого развития технологий и увеличения объема передаваемой информации. Знания в области защиты личных данных позволят ученикам и учителям не становится жертвами мошенников.

**Проблема исследования** заключается в том, что современные методы аутентификации, такие как пароли, отпечатки пальцев или сканирование лица, не всегда являются достаточно надежными и могут быть подвержены взлому. Это связано с тем, что многие из них основаны на использовании статических данных, которые могут быть легко скомпрометированы. Решением проблемы может быть распространение информации о дополнительных методах защиты и предложения алгоритма действий в случае становлением жертвы мошенников.

**Цель исследования:** проанализировать различные методы аутентификации и собрать рекомендательный образ в виде буклета для распространения информации о защиты личных данных в сети Интернет.

Для достижения цели исследования поставлены следующие **задачи:**

1. Изучить и проанализировать литературу по этой теме
2. Выявить основные проблемы методов аутентификации, с которыми сталкиваются пользователи сети Интернет
3. Составить рекомендации в виде буклета по информации о методах аутентификации и защиты информации в сети Интернет

**Объект исследования** — процесс повышения осведомленности учеников и учителей наш ей школы о методах аутентификации и защиты своих данных

**Предмет исследования** — распространение информации о методах дополнительной аутентификации и защиты своих данных в виде буклета

**Гипотеза:** использование биометрических методов аутентификации, таких как сканирование лица или отпечатка пальца, может быть более надежным и безопасным способом защиты информации в сети Интернет, чем использование паролей или других статических данных.

**Методы исследования:**

* теоретические (анализ литературы, изучение материала, обобщение опыта);
* эмпирические (формирование и контроль знаний, диагностика, анализ результатов).

**Практическая значимость данной работы** в том, чторезультаты исследования могут быть использованы для разработки более надежных и безопасных методов аутентификации и передачи информации в сети Интернет. Это может быть полезно для различных групп людей, таких как разработчики программного обеспечения, специалисты по информационной безопасности, а также пользователи Интернета, которые хотят защитить свои данные от взлома. Результаты исследования могут быть использованы для создания новых методов аутентификации и безопасности информации, а также для улучшения существующих методов.

**Основные этапы исследования:**

* Найти и изучить литературу по данной теме;
* Выбрать материал для дальнейшего составления опыта и вопросов для диагностики;
* Сделать опрос среди педагогов и учеников в нашей школе по способам аутентификации и защиты личных данных в сети Интернет;
* Анализ результатов опроса, проведенного среди учителей и учеников и формулирование вывода;
* Составление рекомендаций в виде буклета и его последующее распространение среди учеников и учителей школы

Теоретическая часть состоит из основных определений по выбранной теме и устанавливает основы знания о методах аутентификации. Практическая часть включает в себя диагностические и аналитические данные, описание инструментов для составления и анализа общего опыта.

**Анализ различных методов аутентификации и безопасности информации в сети Интернет**

**Крючкова София Ивановна**

**Россия, ЯНАО, г. Тарко-Сале**, **МБОУ «СОШ № 2»**, **10 класс**

**Глава 1. Основы аутентификации и безопасности информации в сети Интернет.**

**1.1. Основные принципы аутентификации**

Чтобы обеспечить безопасность информации, необходимо точно выяснить, кто получает доступ к ней, и проверить, что это тот, за кем он себя выдаёт. При этом используются процедуры аутентификации и идентификации.

* **Идентификация** — это процесс определения личности человека по его идентификатору, например, по имени или номеру телефона.
* **Аутентификация** — это проверка соответствия личности человека и его идентификатора с помощью уникальной информации, такой как пароль или отпечаток пальца.

Для подтверждения подлинности человек должен предоставить уникальный идентификатор, называемый фактором аутентификации. Существуют четыре типа факторов аутентификации:

1. человек имеет какой-то предмет, например токен;
2. человек знает какую-то информацию, например пароль;
3. человек имеет определенные биологические особенности, такие как отпечаток пальцев;
4. человек находится в каком-то месте, например, с определенной IP-адресом

**Методы защиты данных с помощью аутентификации:**

Существуют различные методы аутентификации, которые повышают безопасность информации пользователя в сети Интернет.

Один из самых распространенных методов - *двухфакторная аутентификация* (2FA), которая проверяет подлинность пользователя, используя два различных фактора, таких как пароль и логин, а также дополнительные PIN-коды, ключи или токены. Однако, этот метод может быть сложным для пользователей, особенно если доступ ко второму способу аутентификации не всегда доступен.

*Биометрическая аутентификация* использует биометрические данные, такие как отпечатки пальцев, сетчатка глаза, голос или лицо, для проверки подлинности пользователя. Этот метод более прост в использовании и надежен, так как каждый человек имеет уникальные биометрические черты. Однако, алгоритмы счета данных могут быть неточными, что может привести к блокировке доступа к аккаунту.

*Аутентификация на основе поведения* (Behavioral authentication) использует алгоритмы анализа поведения и статистические модели для проверки подлинности пользователя. Этот метод не требует использования альтернативных методов входа и позволяет не запоминать пароли. Однако, алгоритмы могут ошибаться, а поведение человека может меняться из-за различных факторов.

*Аутентификация на основе блокчейна* (Blockchain authentication) использует технологию блокчейна для проверки подлинности пользователя. Этот метод предоставляет высоконадежную систему защиты от взлома и подделки данных, но требует больших затрат в ресурсах и увеличивает время на аутентификацию из-за сложности процесса.

В целом, каждый из этих методов имеет свои преимущества и недостатки, и выбор конкретного метода зависит от потребностей пользователя и уровня безопасности, который требуется для его информации.

**1.2. Типы угроз безопасности информации в сети Интернет**

Некоторые разновидности угроз безопасности онлайн-записей, связанные с плохой аутентификацией, обычно включают:

1. Несанкционированный доступ к структурам: если степень аутентификации недостаточна, злоумышленники могут более легко получить доступ к системам и записям, ставя под угрозу их конфиденциальность.
2. Социальная инженерия. Злоумышленники могут использовать уязвимые или неверные методы аутентификации для контроля клиентов и получения конфиденциальных данных, включая пароли.
3. Подмена личности. Некачественная аутентификация может привести к подделке учетных данных человека и получению несанкционированного доступа к активам или фактам.
4. Компрометация частной информации. Если факторы аутентификации слабы, данные потребителей могут быть скомпрометированы и использованы для мошенничества или кражи личных данных.

Таким образом, информированность о способах защиты персональных данных может помочь сократить угрозы безопасности информации в сети Интернет. Несмотря на важность этой информации, знание о методах дополнительной аутентификации дается только на уроках информатики, чего недостаточно для формирования осведомленности.

**2 Глава. Опрос и создание буклета о методах аутентификации и защите персональных данных**

**2.1. Планирование и проведение опроса о предпочтительных методах аутентификации и информировании и способах защиты**

В качестве технологии исследования для темы было выбрано анкетирование. Изучая различные методы аутентификации и безопасности информации в сети Интернет было выделено несколько вопросов, касаемых актуальности и надежности некоторых способов защиты данных. Были опрошены ученики и учителя нашей школы. Результаты опроса могут подтвердить, что недостаточное знание о методах аутентификации и защите данных может привести к серьезным последствиям, таким как возможность стать жертвой мошенничества или кибератак. Школьники и педагоги, которые сталкивались с взломом из-за недостаточной аутентификации, могут стать примером того, как важно осознавать риски и принимать меры по обеспечению безопасности в Интернете.  
Было проведено анкетирование, в котором поучаствовало 16 человека. (приложение №1–7)

**Выводы:**

1. Чаще всего участники опроса использовали пароль как способ аутентификации, а сканирование лица и отпечаток пальца – реже всего. (приложение №1)
2. Среди способов аутентификации большинство опрашиваемых указали отпечаток пальца как самый безопасный. (приложение №2)
3. Практически половина опрашиваемых (42,3%) никогда не меняют пароль. (приложение №3)
4. Оптимальной длиной для безопасности пароля большинство участников опроса выбрали 6 и 8 символов соответственно. (приложение №4)
5. Для предотвращения кибер-взломов опрашиваемые чаще всего используют надежные пароли и не открывают подозрительные ссылки и файлы (приложение №5)
6. Большая часть опрашиваемых сталкивалась с попытками хакерских атак на их аккаунты (приложение №6)
7. Сталкиваясь с попытками хакерских атак, участники опроса чаще всего меняли пароль на своем аккаунте. (приложение №7)

**2.2. Создание буклета с информацией о методах аутентификации и защите персональных данных.**

Анализируя ответы в опросе, можно сделать вывод, что большая часть опрашиваемых не информированы о дополнительных методах защиты персональной информации и аутентификации. Используя информацию из изученной литературы в главе 1, вероятно предполагать, что высокий процент столкновения с хакерскими атаками на аккаунты может быть связан с низким уровнем защиты их способа аутентификации, такого, как пароль.

Для информирования учащихся и педагогов нашей школы мы разработали образовательный буклет "Безопасность в сети: Руководство по методам аутентификации и защите данных" (приложение №8). В качестве источника информации для буклета было решено выбрать «Защита информации ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ Общие положения» под редактурой Надежды Талановой. Используя методические положения для создания буклета, мы сформулировали общий **план буклета**.

1. Основная идея буклета: Четкое формирование представления о том, чем является аутентификация и важность дополнительной защиты личной информации;
2. Целевая аудитория: Ученики и педагоги нашей школы;
3. Подбор конкретной информации для буклета;
4. Размещение информации и иллюстраций;
5. Проверка буклета на наличие ошибок;
6. Подписание буклета, печать и представление буклета публике.

**2.3 Оценка эффективности информирования: повторный опрос после ознакомления с методами защиты информации.**

Распространив буклет "Безопасность в сети: Руководство по методам аутентификации и защите данных" среди анкетируемых, через некоторый период времени (месяц) был проведен повторный опрос, который показал эффективность информирования среди педагогов и учеников нашей школы. Диаграмма 1 показывает количество анкетируемых, испытывающие хакерские атаки до использования рекомендаций (Приложение №6) и после (приложение №10):

Диаграмма 1. Уровень хакерских атак до и после информирования о дополнительных методах аутентификации.

Проанализировав результаты диагностики, мы видим, что использование рекомендаций по дополнительным способам аутентификации и защиты личной информации позволило снизить количество хакерских атак, испытывающие анкетированные ученики и педагоги. Благодаря знаниям, данных в буклете, личные данные анкетируемых находятся в безопасности, понижая уровень киберпреступлений в сети Интернет. Таким образом, буклет исполнил свою образовательную функцию.

**Заключение.**

Информированность в сфере защиты данных важная часть работы в сети Интернет. Понимая эффективность и удобность различных методов аутентификации, можно выбрать для себя самый безопасный способ, дабы защитить свою личную информацию и не стать жертвой мошенников. От отсутствия знаний и действий в сторону защиты своих аккаунтов могут пострадать не только ваши данные, но и данные ваших близких, ведь мошенники часто используют взломанные аккаунты для вымогания денег или создания скомпрометированного контента.

По нашему мнению, и эффективному результату работы практического продукта (буклета), необходимо информирование населения о способах защиты данных и дополнительных методов аутентификации, чтобы сократить количество киберпреступлений и сделать Интернет более безопасным местом.

**Список использованной литературы:**

Учебники, учебные пособия:

1. Посметухова, К.Н. Обзор и краткий анализ современных методов аутентификации / К.Н. Посметухова, А.У.Актаева // Наука и реальность. - 2023. - № 2 (14). - С. 58–62
2. Кибардин А.В. Защита информации: аутентификация и разграничение доступа, УрФУ, 2013. — 50 с.Электронное текстовое издание.
3. Кислинская М.В., методист ГАПОУ РБ «Белорецкий медицинский колледж»; методические рекомендации по созданию буклета, от «28» февраля 2018 г., протокол № 6

Электронные ресурсы:

1. https://moluch.ru/archive/123/34077/
2. https://studfile.net/preview/2555229/page:8/

**Приложение 1. Результаты первого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.**



Диаграмма 2. Результаты первого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.

**Приложение 2. Результаты второго вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.**

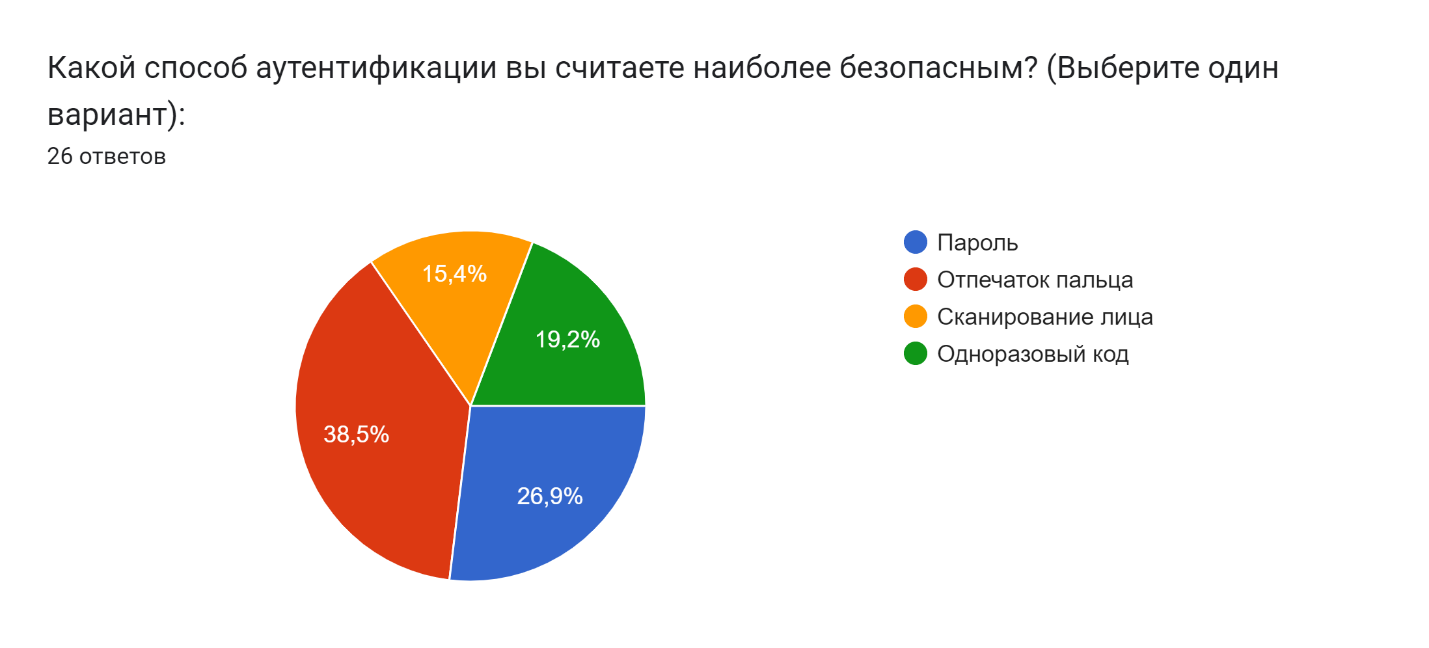


Диаграмма 3. Результаты второго вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.

**Приложение 3. Результаты третьего вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.**

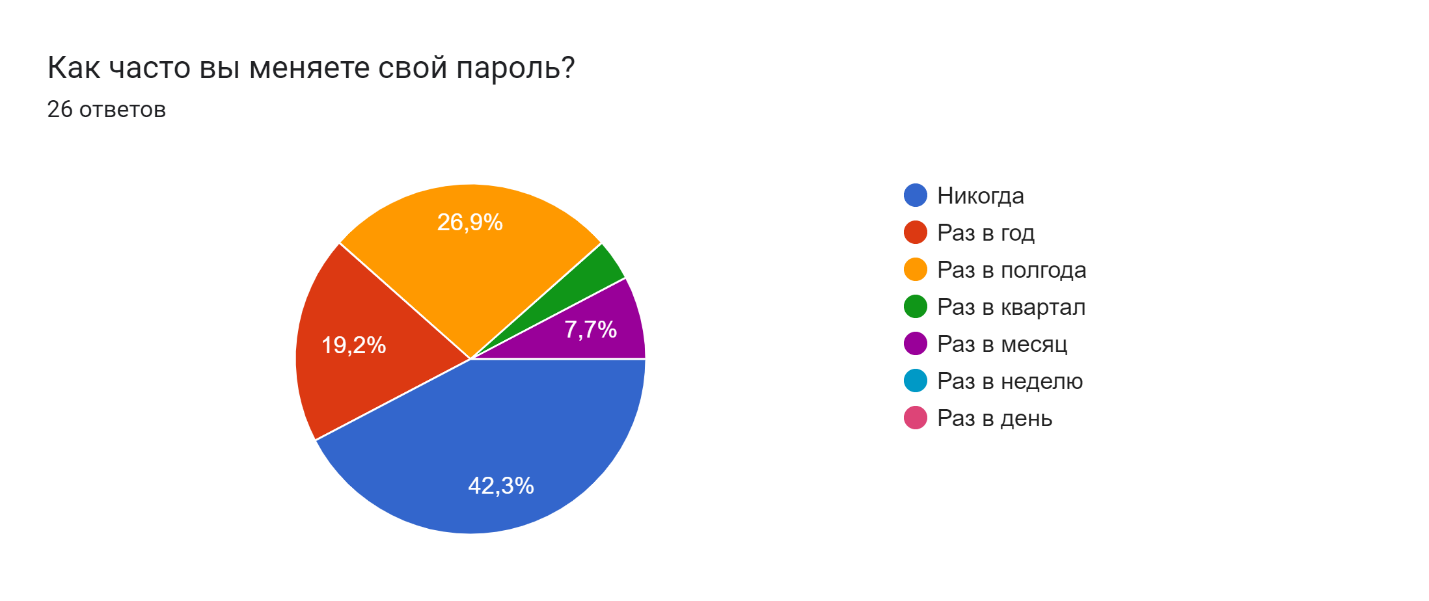


Диаграмма 4. Результаты третьего вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.

**Приложение 4. Результаты четвертого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.**

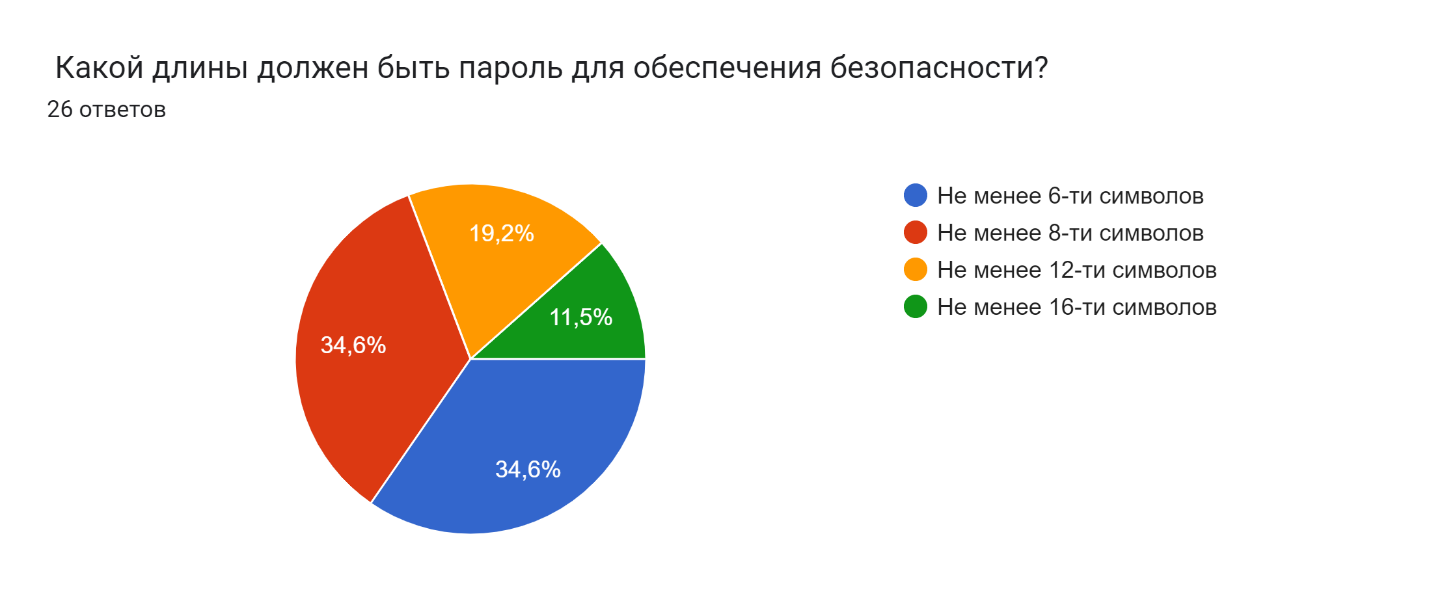


Диаграмма 5. Результаты четвертого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.

**Приложение 5. Результаты пятого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.**

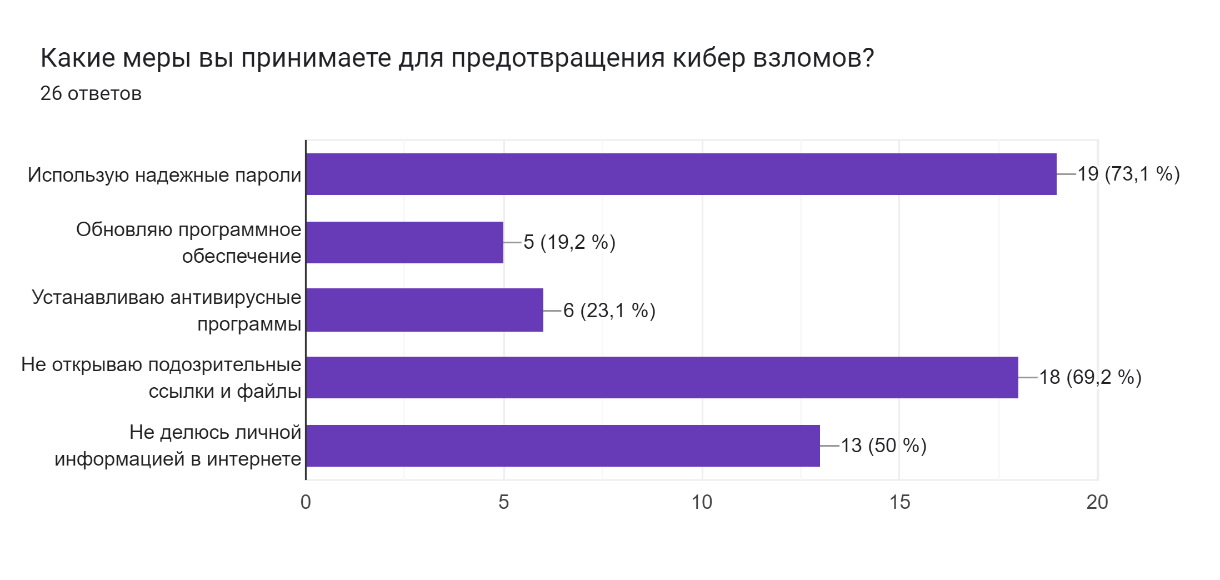


Диаграмма 6. Результаты пятого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.

**Приложение 6. Результаты шестого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.**



Диаграмма 7. Результаты шестого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.

**Приложение 7. Результаты седьмого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.**

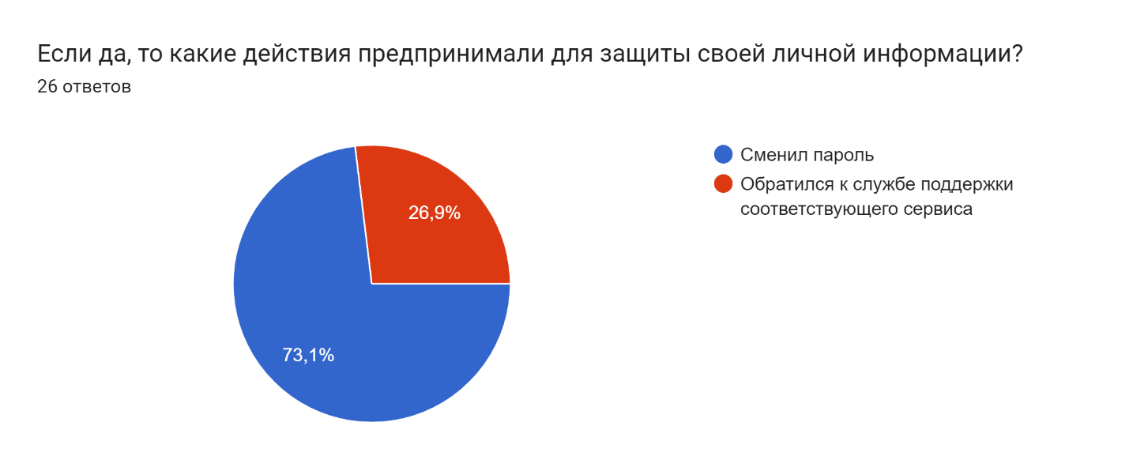
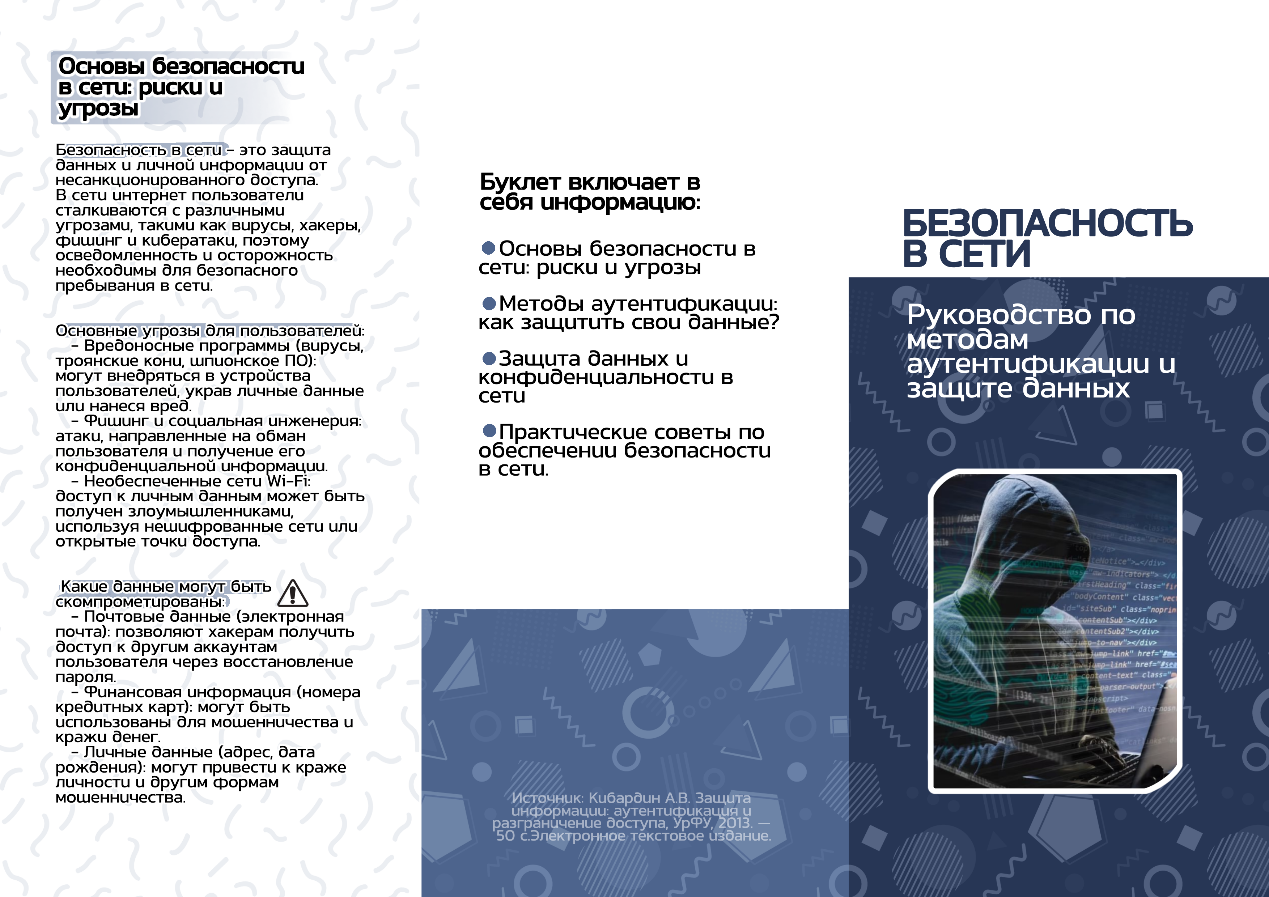
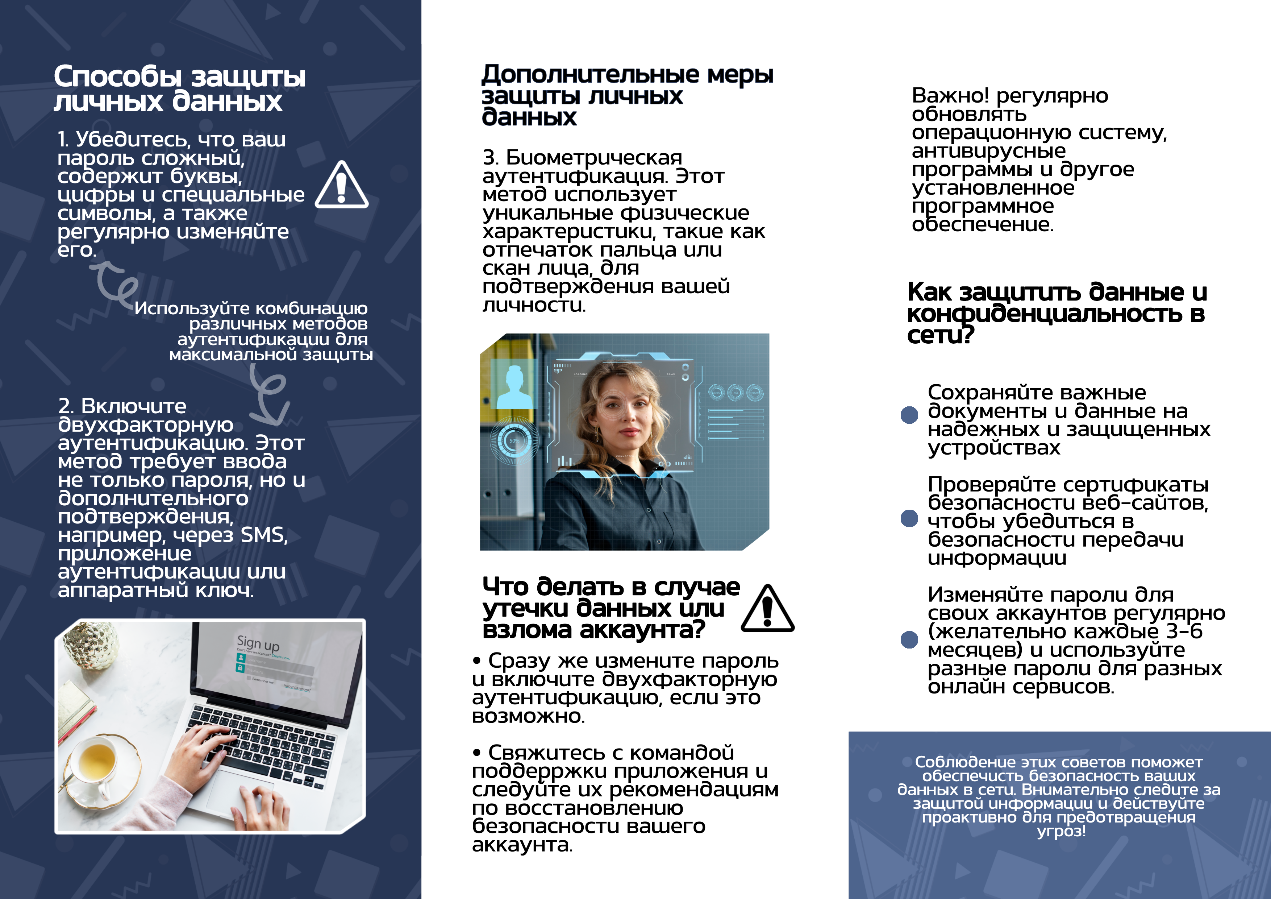


Диаграмма 8. Результаты седьмого вопроса опроса по способам аутентификации и защиты личных данных в сети Интернет.

**Приложение 8. Передняя сторона буклета**



**Приложение 9. Задняя сторона буклета**



**Приложение 10. Результаты опроса по способам аутентификации и защиты личных данных в сети Интернет о хакерских атаках после выполнения рекомендаций**

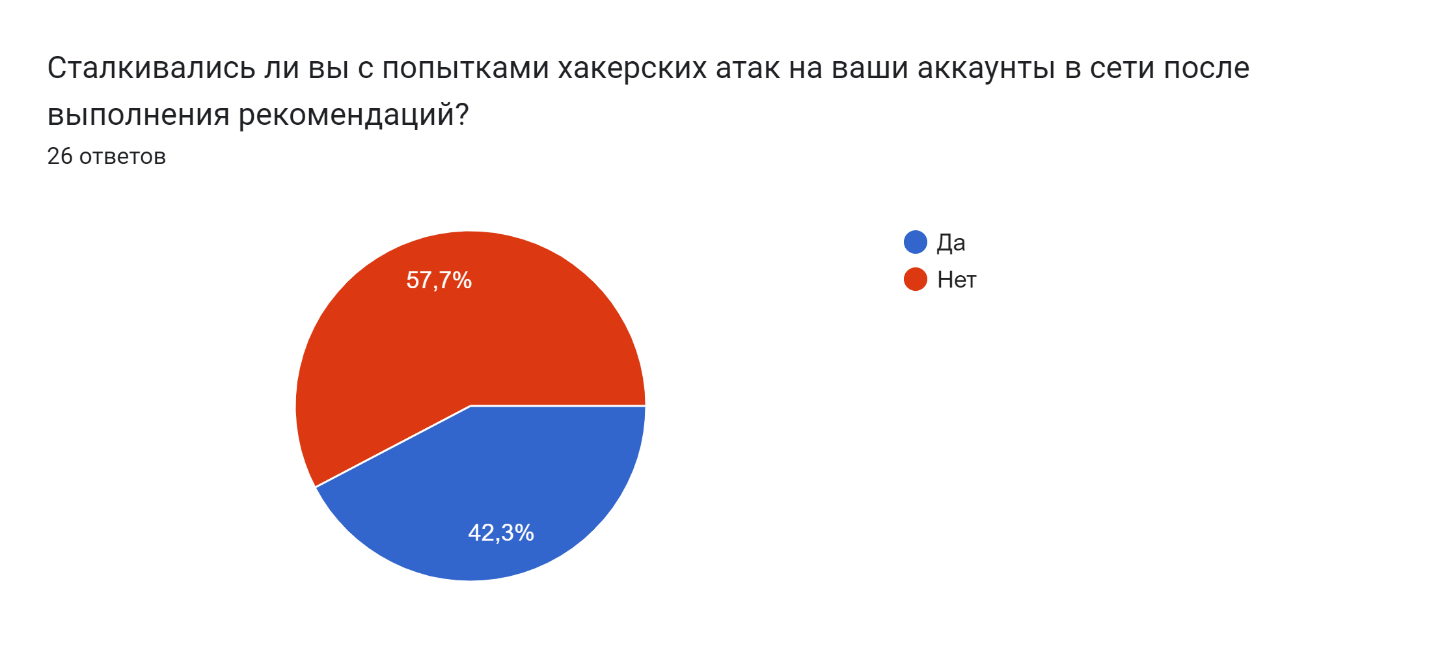


Диаграмма 9. Результаты опроса по способам аутентификации и защиты личных данных в сети Интернет о хакерских атаках после выполнения рекомендаций