Муниципальное бюджетное общеобразовательное учреждение

Заларинская средняя общеобразовательная школа №1

Индивидуальный итоговый проект на тему:

«Аутентификация - как один из ключевых методов обеспечения информационной безопасности»

Работу подготовил:

ученик 10 «А» класса

Андреев Кирилл

Руководитель:

Кузеванова Яна Кирилловна,

учитель информатики

р.п.Залари

2023 г.

Содержание

Введение

Актуальность: в современном мире безопасность данных играет ключевую роль. Особенно важно обеспечить надежную аутентификацию пользователей для защиты информации от несанкционированного доступа. Аутентификация позволяет проверить личность пользователя и предотвратить несанкционированный доступ к данным или ресурсам. Технологии аутентификации постоянно усовершенствуются с целью обеспечения более надежной и удобной защиты данных.

Появление социальных сетей, онлайн-игр, электронных платформ для обучения и развлечений открывает новые возможности для подростков, но одновременно влечет за собой ряд проблем, связанных с информационной безопасностью.

Цель: изучить использование систем аутентификации подростками, как средства защиты персональных данных.

Задачи:

- Изучить понятие информационной безопасности.
- Изучить понятие аутентификации и ее основные методы.
- Разработать и провести анкетирование среди подростков МБОУ Заларинская СОШ №1 на выявление использования дополнительных средств защиты персональных данных.
- На основе полученных результатов разработать памятку по защите персональных данных.

Гипотеза: большинство школьников не прибегают к дополнительной защите персональных данных.

Объект: защита персональных данных.

Предмет: аутентификация.

Методы исследования:

- Анализ теоретического материала.
- Анкетирование.

1. Теоретическая часть

1.1.Понятие информационной безопасности

Информационная безопасность — это набор процедур и инструментов, которые обеспечивают всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения.

1.2.Понятие аутентификации и ее основные методы

Аутентификация – этап защиты информации, на котором проверяется подлинность личности пользователя. Иными словами, эта процедура позволяет удостоверить, что субъект, который обращается к некой защищенной информации, действительно является тем, за кого себя выдает.

Востребованность в усовершенствованных методах аутентификации:

Проблема безопасности в современных сетях состоит в том, что злоумышленники не ограничиваются попытками «увести» данные граждан, – зачастую им интересна кража цифровой личности пользователей. Когда на личность пользователя завязаны многие сервисы и системы (государственные, финансовые и прочие), то обеспечение их безопасности драматически возрастает. Это увеличивает нагрузку на средства аутентификации и требует выработки новых ее методов.

1.3.Основные методы аутентификации

- Однофакторная: паролевая; биометрическая; цифровые сертификаты и электронные подписи
- Многофакторная аутентификация

Парольная аутентификация – наиболее распространенный и наименее эффективный метод удостоверения личности в информационных системах предполагает использование символьного пароля. При кажущейся простоте применения парольный метод аутентификации имеет немало недостатков. При эксплуатации надежность защиты зависит от сложности заданного пароля. Чем пароль труднее, чем больше разнообразных символов содержит, тем сложнее его подобрать злоумышленникам. «Простой» пароль легко

взломать банальным перебором, а «трудный» — тяжело запомнить самому пользователю, особенно если на нескольких ресурсах он использует разные пароли.

Повысить эффективность парольной защиты может применение временных (одноразовых) паролей, когда для каждой попытки войти в систему пользователь должен запрашивать новый пароль. Временные пароли не нужно хранить или помнить наизусть – пользователю достаточно иметь на руках устройство, на которое они отправляются, например, телефон. Для передачи одноразового пароля, как правило, используют Push-уведомления или SMS-сообщения. Второй способ понемногу уходит в прошлое, поскольку SMS относительно просто перехватить. Впрочем, применение одноразовых паролей относится уже к аутентификации по двум факторам.

Биометрическая аутентификация – метод аутентификации, использующий персональные биометрические данные, опирается на использование уникальных параметров человеческого тела: голос, лицо, отпечаток пальца и проч. Эти параметры считываются регистрирующим устройством, у которого есть сканер или камера – это умеют делать большинство современных смартфонов, поэтому распознавание лица и отпечатка пальца сегодня применяется во многих мобильных приложениях и операционных системах.

Биометрические параметры неотделимы от самого пользователя, они уникальны и позволяют установить личность человека с высокой точностью. Если говорить про недостатки биометрии, то можно отметить, что нередки случаи, когда злоумышленники подделывают отличительные черты человека, перехватывают чужие биометрические показатели и в дальнейшем ими пользуются.

Но в целом уровень доверия к этому методу постепенно возрастает. К биометрической аутентификации вовсю прибегают банки: если раньше биометрия помогала удостоверять личность сотрудников, то теперь это распространилось и на клиентов. Банковские приложения позволяют

подтверждать денежные операции по отпечатку пальца, а в «физических» отделениях личность клиента может быть верифицирована при помощи сканирования лица специальной камерой.

Стоит отметить, что уже несколько лет в России работает Единая биометрическая система – запущенная Центральным Банком и «Ростелекомом» цифровая платформа, позволяющая идентифицировать получателей финансовых услуг по голосу и лицу.

Цифровые сертификаты и Электронная цифровая подпись

Обмениваясь данными с современным веб-сайтом, пользователь сталкивается с криптографическим электронным «удостоверением», подтверждающим, что подключение производится к настоящему ресурсу, а не к его фишинговой копии. Такое «удостоверение» называется цифровым сертификатом. Сертификат сопоставляет криптографический ключ с его владельцем, поэтому его можно использовать для аутентификации пользователей.

Цифровой сертификат составляет часть системы электронной цифровой подписи, поскольку тоже основан на инфраструктуре открытых ключей. Ключ связывает сертификат с личностью человека, которому он принадлежит, и помогает проверить релевантность цифровой подписи. Электронная подпись поддерживает подтверждение авторства – то есть с ее помощью можно удостовериться, что документ исходит от определенного лица и имеет юридическую силу.

При таком методе аутентификации подлинным считается пользователь, обладающий секретным ключом шифрования. Метод с использованием цифрового сертификата считается более надежным, нежели парольный, хотя и у него есть недостатки. В частности, поскольку владелец обязуется сам хранить ключ шифрования, это создает риски кражи данных, если злоумышленник изыщет способ им завладеть.

Многофакторная аутентификация – из сказанного выше видно, что любой метод, использующий один фактор аутентификации, имеет как

плюсы, так и минусы. Нетрудно догадаться, что, объединив несколько факторов в рамках одной системы, можно взаимно компенсировать недостатки каждого из них. Набор методов, опирающихся на несколько факторов, называется многофакторной аутентификацией. Чаще всего используется аутентификация по двум факторам.

Наиболее известным методом двухфакторной аутентификации (2FA) является совместное использование постоянного и временного паролей. При этом пользователь знает постоянный пароль, а при попытке авторизоваться в системе (на сайте или приложении) он получает одноразовый код на персональное устройство, которое называется аппаратным токеном. При двухфакторной аутентификации в роли такого устройства де-факто выступает мобильный телефон пользователя. В роли аппаратных токенов могут выступать различные устройства – USB-ридеры, смарт-карты и так далее.

2. Практическая часть

2.1. Анкета на выявление использования дополнительных средств защиты персональных данных среди подростков

- Пользуетесь ли вы приложением Сбербанк? Да/Нет.

Если да, то используете двойную аутентификацию? (например, биометрия) Да/Нет

- Пользуетесь ли вы социальными сетями? Да/Нет.

Если да, то используете двойную аутентификацию? Да/Нет (например, смс-код)

- Пользуетесь ли вы приложением Steam? Да/Нет.

Если да, то используете двойную аутентификацию? Да/Нет (например, приложения-аутентификаторы)

2.2.Анализ результатов, проведенного анкетирования

В опросе участвовало 40 обучающихся 10-х классов МБОУ Заларинская СОШ № 1.

По результатам проведенного анкетирования 35 учащихся используют приложение Сбербанк, что составляет 87% от всего количества участников. Часть пользователей приложения «Сбербанк» используют однофакторную аутентификацию (пароль), 12 человек используют двухфакторную (пароль + биометрия).

Из второго вопроса следует, что 36 анкетируемых используют социальные сети. Все 36 обучающихся при входе в социальные сети используют только пароль, не прибегая к дополнительным средствам защиты персональных данных, что является угрозой их информационной безопасности.

Итогом третьего вопроса является следующее: 23 ученика пользуются приложением Steam, а 17 учеников не пользуются. Среди пользователей данного приложения свои личные данные защищают двухфакторной аутентификацией 21 участник анкетирования.

По данным проведенного анкетирования можно сделать вывод, что ученики 10-х классов практически не используют двухфакторную аутентификацию, как дополнительное средство защиты персональных данных. На основе беседы и проведенного анализа анкетирования были выявлены следующие причины, по которым ученики не используют двухфакторную аутентификацию:

1. Неудобство: Другой фактор, который отталкивает учеников от использования двухфакторной аутентификации, - это считающееся ими неудобство. Для включения двухфакторной аутентификации необходимо предоставить номер телефона или использовать приложение для генерации одноразовых кодов. Некоторым ученикам может показаться, что это лишний шаг, который требует дополнительных усилий и времени.

2. Неверное представление об угрозах: Некоторые ученики могут недооценивать угрозы, связанные с безопасностью данных. Они могут считать, что им нечего скрывать или что никому не интересны их персональные данные. Это заблуждение может привести к небрежному отношению к безопасности и отсутствию использования двухфакторной аутентификации.

3. Недостаток осведомленности: Одной из основных причин, по которым ученики 10-х классов не используют двухфакторную аутентификацию, является недостаток осведомленности о ее преимуществах и значимости. Многие подростки просто не знают о том, что такая функция существует или не понимают, как она может помочь защитить их персональные данные от несанкционированного доступа.

В связи с выявленными причинами был разработан буклет (приложение 1), в котором отражены возможные методы двухфакторной аутентификации. Представлена информация о специальных приложениях, биометрии данных и др.методах.

Заключение

В современном цифровом мире, где все больше подростков активно используют интернет и социальные сети, вопросы безопасности и приватности становятся особенно актуальными. Важно обеспечить подросткам надежную аутентификацию, чтобы защитить их от потенциальных угроз и злоумышленников.

Аутентификация является неотъемлемой составляющей информационной безопасности. Ее эффективное применение способствует предотвращению несанкционированного доступа и защите данных подростков, обеспечивая безопасность и конфиденциальность в цифровой эпохе.

В ходе работы было изучено понятие информационной безопасности, понятие аутентификации и ее основные методы. Было разработано и проведено анкетирование среди подростков МБОУ Заларинская СОШ №1 на выявление использования дополнительных средств защиты персональных данных. Проведенный анализ анкетирования показал, что большинство школьников не прибегают к дополнительной защите персональных данных, что подвергает выдвинутую гипотезу. На основе полученных результатов анкетирования была разработана памятка по защите персональных данных. Таким образом, поставленные задачи выполнены, цель работы достигнута.

Список литературы

1. Википедия : [сайт]. – URL: Аутентификация — Википедия (wikipedia.org) (дата обращения 11.01.2024)

2. [сайт]. – URL: Системы и методы аутентификации | ekassir.com Общие сведения об информационной безопасности (InfoSec) | Microsoft Security (дата обращения 19.12.2023)

3. SKILLFACTORY MEDIA : [сайт]. – URL: Информационная безопасность: что это и зачем нужна, понятия и принципы (skillfactory.ru HYPERLINK "https://blog.skillfactory.ru/glossary/informaczionnaya-bezopasnost/?ysclid=ltfl5fvlbl184710114") (дата обращения 19.12.2023)

4. OTUS JOURNAL : [сайт]. – URL: Аутентификация от А до Я OTUS (дата обращения 20.12.2023)

5. Epochta : [сайт.] – URL: Что такое аутентификация и какая она бывает | www.epochta.ru (дата обращения 20.12.2023)

Приложение 1.