ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ, ЭКОНОМИКЕ И МЕНЕДЖМЕНТЕ

УДК 004
Код РИНЦ 20.00.00 DOI: 10.46554/Russian.science-2021.09-1-3/6

СПОСОБЫ ШИФРОВАНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЕЙ СБЕРБАНКА

© 2021 Александрова Алина Олеговна
студент
Самарский государственный экономический университет
E-mail: Alinalexandrova.a@yandex.ru

Ключевые слова: Сбербанк, дигитализация, информационная безопасность, мошенничество, шифрование, утечка информации.

Данная статья посвящена анализу потери данных и тому, как их защитить. На примере Сбербанка рассмотрены криптографические ресурсы, которые помогают не дать мошенникам похитить важную информацию.

В настоящее время, когда технологии стремительно развиваются наиболее актуальным, становится дигитализация данных. Тем более, из-за сложной сложившейся ситуации в мире, в связи с пандемией вируса, даже мелкие предприятия вынуждены были перейти на цифровой формат существования. Так как многие предприятия были не готовы к такому переходу, следовательно на этом нашлось кому нажиться и фирмы ощутили потребности в шифрование своих данных.

За последнее года по некоторым данным утечка информации возрастает с каждым годом и очень стремительно это представлено на рисунке.[1]

За 2019 год утечка по банковской и финансовой сфере в России составляет 13,2%, а по миру это цифра составляет всего 8,8%. Исходя из выше приведенных данных за 2019 год, мы рассмотрим более подробно финансовую и банковскую сферу в России. Крупнейшем банком России является Сбербанк актив данного банка составляет 33346041 млн. рублей.

Рассмотрим криптографию на данном банке, так как он является самым популярным банком среди пользователей. Криптография стала неотъемлемой частью банковской сферы. В каждом банковском приложение, через которое клиент общается с банком, не обходятся без криптографических решений. Благодаря криптографии клиент и «банк» могут не беспокоиться о сохранности своих сбережений и личных данных, которые переда-

ются через всемирный используемые интернет-каналы, буль то мобильный телефон, терминалы оплаты в магазине или в банкомате, персональный компьютер.

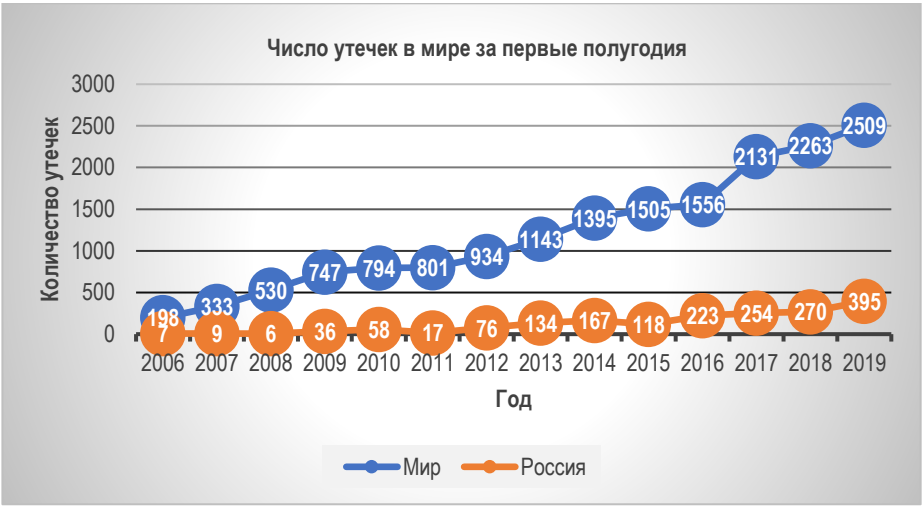

Рис.

В настоящее время криптоаналитиком в банковской сфере нужно решить несколько задач, чтобы обезопась клиент и банк такие как:

1. Обеспечить конфиденциальность электронных документов или транзакций при передаче по открытым каналам связи для исключения доступа к данным третьих лиц;
2. Защита от внесения изменений или искажений в процессе передачи и хранения электронных документов ли транзакций;
3. Идентификация клиента или банка в электронных документах или транзакциях;
4. Подтверждение достоверности банковской части системы при использовании клиентами систем дистанционного банковского обслуживания;
5. Подтверждение факта создания электронных документов или транзакций клиентом или банком;
6. Подтверждение подлинности клиента системой дистанционного банковского обслуживания.

Первая задача решается с помощью технологии шифрования, а все последующие с помощью технологии ЭП (электронной подписи).

Сбербанк использует такие криптографические ресурсы как:[2]

1. GET/v1/crypto – получение криптографической информации.

Данный ресурс позволяет получать информацию по крипто-профилю и сертификатам пользователя, сертификатам удостоверяющих центров, и сертификату технологического криптографиля банка.

2. POST /v1/crypto/cert-requests – создание запроса на новый сертификат.

Данный ресурс позволяет создавать запросы на выпуск нового сертификата.

Для создания документа на выпуск нового сертификата ЭП (электронной подписи) необходимо отправить данный запрос, в котором нужно передать авторизационный токен (Access Token) и данные по выпускаемому сертификату. Авторизационный токен передается в параметре Authorization заголовка запроса.

3. GET /v1/crypto/cert-requests/{externalId}/state – получение статуса.

Данный ресурс позволяет получить информацию по статус запроса на новый сертификат. Полученную информацию можно использовать для анализа и контроля статуса запроса на новый сертификат.

Для получения информации по статусу необходимо отправить запрос – GET, в котором необходимо передать авторизационный токен (Access Token) и идентификатор запроса на новый сертификат (externalId). Авторизационный токен передается в параметре Authorization заголовка запроса.

4. POST /v1/crypto/cert-requests/{externalId}/activate – активация сертификата.

Данный ресурс позволяет создавать запросы на активацию выпущенного сертификата, для дальнейшей возможности подписывать документы и запросы.

Для активации сертификата ЭП (электронной подписи) необходимо отправить запрос-POST, в котором передать авторизационный токен к данным пользователя (Access Token) и идентификатор документа externalId из запроса cert- requests. авторизационный токен передается в параметре Authorization заголовка запроса.

5. GET /v1/crypto/cert-requests/{externalId}/print – печать сертификата.

Данный ресурс позволяет получить печатную форму сертификата.

Для получения печатной формы сертификата необходимо отправить GET-запрос, в котором передать авторизационный токен к данным клиента (**Access Token**) и идентификатор запроса.

Так же в приложение «сбербанк онлайн» есть вкладка «безопасность», в которой Вы можете ознакомиться со статьями на тему безопасности своих личных данных и средств, так же изменить настройки безопасности, например, дополнительный пароль и тому подобное. В данной вкладке можно проверить ваше приложение на вирус.

Но несмотря на все меры обезопасить клиента и банк, все-таки находятся такие мошенники, которые обманным путем умудряются похитить сбережения или личные данные.

Самые популярные схемы мошенников:[3]

1. Звонок из службы безопасности банка
2. Перевод по ошибки
3. Брокерские или дилерские услуги
4. Опрос от Сбербанка
5. Автоматизированные кол-центры
6. Звонок из прокуратуры
7. Приложение- кошелек с «защищенной картой»

Сбербанк придумывает все более надежные методы защиты от мошенничества, а также новые предложения для клиентов сбербанка. Следовательно, развитие шифрования очень важный этап в жизни человечества.

---

[1] https://www.infowatch.ru/analytics/reports/27614.

[2] https://developer.sberbank.ru/doc/v3/sbbol/partners-crypto#src-3622309226_safe-id-aWQtLjMuONCa0YDQuNC_0YLQvtCz0YDQsNGE0LjRh9C10YHQutC40LXRgNC10YHRg9GA0YHi3ZOZXdGb3JtYXQudjE4LXJlc291cmNl.

[3] https://www.sberbank.ru/ru/person/dist_services/cybersecurity/cybersecurity_situations.

WAYS TO ENCRYPT CONFIDENTIAL INFORMATION OF SBERBANK USERS

© 2021 Alexandrova Alina Olegovna
Student
Samara State University of Economics
E-mail: Alinalexandrova.a@yandex.ru

Keywords: Sberbank, digitalization, information security, fraud, encryption, information leakage.

This article is devoted to the analysis of data loss and how to protect them. Using the example of Sberbank, cryptographic resources that help prevent fraudsters from stealing important information are considered.