Куликов Г.Г., Нуриахметова Д.Д. Модель двухканальной автоматизированной защиты проведения банковских операций посредством верификации клиентов по номеру телефона. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVIII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2018. – С. 155-159.

УДК 004.056.53

МОДЕЛЬ ДВУХКАНАЛЬНОЙ АВТОМАТИЗИРОВАННОЙ ЗАЩИТЫ ПРОВЕДЕНИЯ БАНКОВСКИХ ОПЕРАЦИЙ ПОСРЕДСТВОМ ВЕРИФИКАЦИИ КЛИЕНТОВ ПО НОМЕРУ ТЕЛЕФОНА

Г.Г. Куликов, Д.Д. Нуриахметова

AUTOMATED PROTECTION MODEL OF CARRYING OUT BANKING OPERATIONSIN THROUGH CUSTOMERSVERIFICATION BY PHONE NUMBER

G.G. Kulikov, D.D. Nuriakhmetova

Аннотация. В предлагаемой модели повышенной безопасности проведения банковских операций рассматривается процедура обеспечения защиты от несанкционированного доступа к данным и внутреннего мошенничества посредством верификации клиентов по номеру телефона.

Ключевые слова: банковские операции, безопасность банковских операций, внутреннее мошенничество, несанкционированный доступ, верификация клиентов.

Abstract. The proposed model of increased security for banking operations examines the procedure for ensuring protection against unauthorized access to data and internal fraud through customers verification by phone number.

Keywords: banking operations, security of banking operations, internal fraud, unauthorized access, customers verification.

Банковская деятельность всегда была связана с обработкой и хранением большого количества конфиденциальных данных. В первую очередь это персональные данные о клиентах, об их вкладах и обо всех осуществляемых операциях. Наиболее вероятный способ утечки конфиденциальной информации – несанкционированный доступ сотрудниками банка [1,2].

Мошенничество можно рассматривать как один из видов операционного риска, который может нанести любому банку существенный урон.

Наиболее опасно для банка – внутреннее мошенничество [3]. Так, лица, причастные к угрозам в отношении порядка деятельности банка, порядка совершения банковских операций, как правило, являются сотрудниками банка [4]. Сотрудник банка может проводить банковские операции без ведома клиента в своих интересах, например, изменять данные клиентской записи, оформлять кредиты или подключать финансовые сервисы.

Для предотвращения рисков внутреннего мошенничестваи несанкционированного доступа к данным предлагается модель повышенной безопасности банковских операций посредством второго дополнительного

канала верификации клиента по доверенному номеру телефона. Доверенный номер телефона – это номер мобильного телефона, предоставляемый клиентов для подтверждения совершения операций в банке для применения мажоритарной логики.

Доверенный номер телефона является надежным идентификатором клиента и позволит повысить степень защиты от несанкционированного доступа к данным и внутреннего мошенничества. При проведении банковских бизнес-процессов следует внедрить дополнительный фактор проверки с помощью доверенного номера телефона. Это позволит усилить процедуру идентификации клиента и подтверждения клиентских операций в банке. Таким образом, будет обеспечено закрытие доступа сотрудникам банка к данным клиентам без его ведома, благодаря чему риски несанкционированного доступа к данным и риски внутреннего мошенничества будут снижены.

В предлагаемой модели повышенной безопасности совершения банковских операций клиент должен пройти процедуру верификации по номеру телефона. Сотрудник банка инициирует отправку на доверенный номер телефона клиента СМС-сообщение. Клиент сообщает полученный пароль. Далее сотрудник банка вводит одноразовый пароль, продиктованный клиентом, в специальное поле. Если введенный пароль совпадает с отправленным клиенту, то верификация считается подтверждённой.

Для обеспечения необходимого уровня формализации при дальнейшей программной реализации предлагаемого алгоритма последующее его описание будем проводить на формальном графоаналитическом примитивном метаязыке UML [5], ориентированном на системное моделирование.

Процедура верификации клиента по номеру телефона для получения доступа к совершению банковской операции сотрудником банка схематически показана на коммуникационной диаграмме (рис. 1).

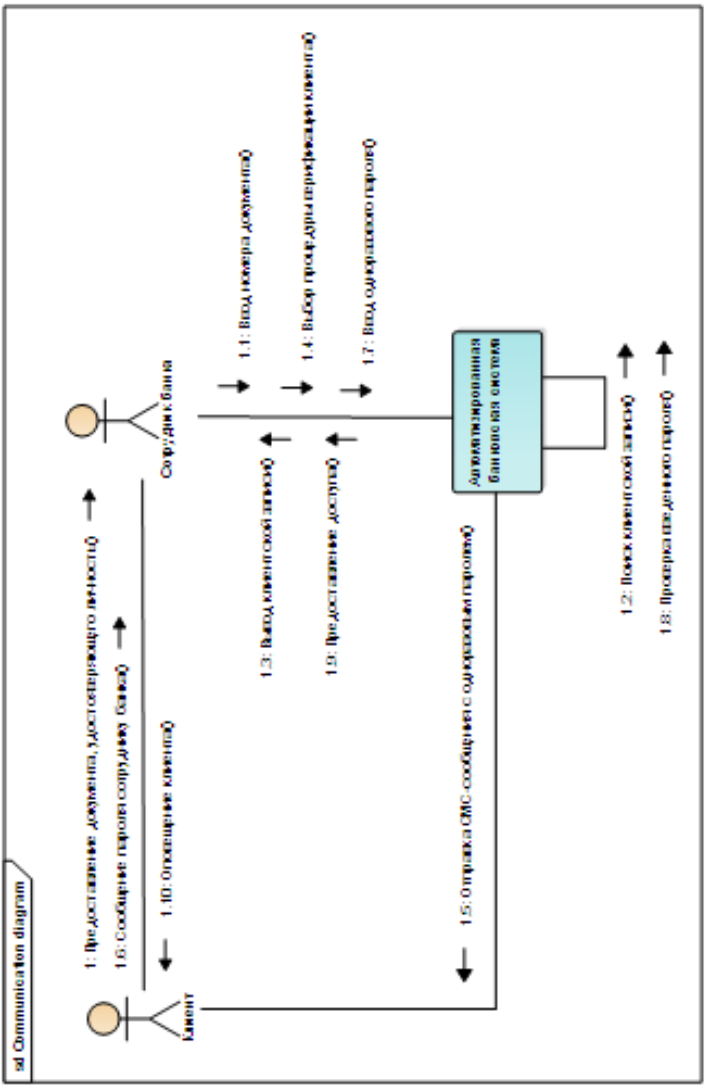

Рис. 1. Коммуникационная диаграмма

На рис. 2 представлена диаграмма последовательности процедуры верификации клиента.

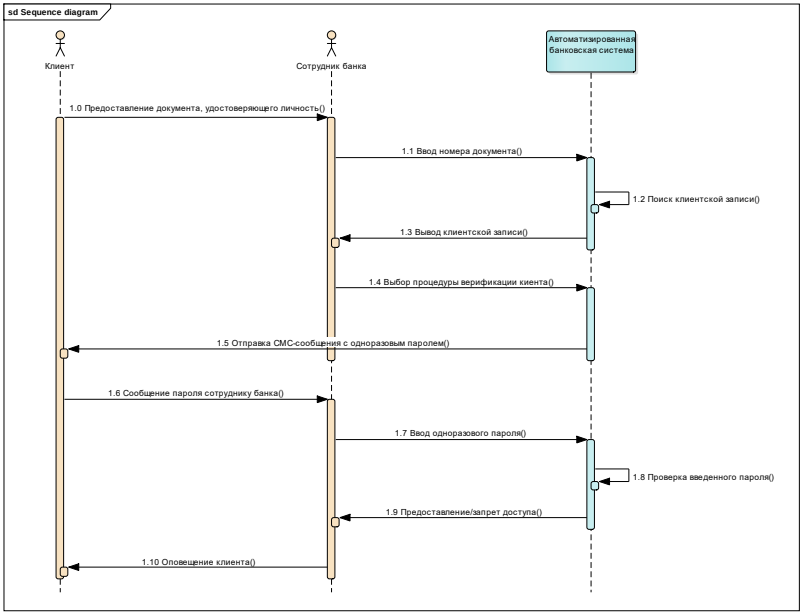

Рис.2. Диаграмма последовательности

Библиографический список

1. Банковские операции / Н.Н. Мартыненко, О.М. Маркова, О.С. Рудакова, Н.В. Сергеева. М.: Юрайт, 2014. 475 с.

2. Внуков А.А. Защита информации в банковских системах: учеб. пособие для бакалавриата и магистратуры. 2-е изд., испр. и доп. М.: Юрайт, 2017. С. 10-11.

3. Седых Ю.Н. Мошенничество среди сотрудников банка // Молодой ученый. 2012. №4. 169 с.

4. Гамза В.А., Ткачук И.Б. Безопасность коммерческого банка: организационно правовые и криминалистические проблемы. М.: Издательство Шумилова И.И., 2002. 43 с.

5. Национальный Открытый Университет "ИНТУИТ" [Электронный ресурс]. URL: https://www.intuit.ru/studies/courses/1007/229/lecture/5954 (дата обращения: 24.09.2018).

Куликов Геннадий Григорьевич
Уфимский государственный авиационный технический университет,
г. Уфа, Россия

Kulikov G.G.
Ufa State Aviation Technical University,
Ufa, Russia

Нуриахметова
Диана Дмитриевна
Уфимский государственный
авиационный технический
университет,
г. Уфа, Россия

Nuriakhmetova D.D.
Ufa State Aviation
Technical University,
Ufa, Russia