УДК 336.719

Белкина Наталья Вячеславовна,
студент,
кафедра Финансов, денежного обращения и кредита,
Высшая школа экономики и менеджмента,
ФГАОУ ВО «Уральский федеральный университет
имени первого Президента России Б.Н.Ельцина»
г.Екатеринбург, Российская Федерация

Стафилова Регина Афанасьевна,
студент,
кафедра Финансов, денежного обращения и кредита,
Высшая школа экономики и менеджмента,
ФГАОУ ВО «Уральский федеральный университет
имени первого Президента России Б.Н.Ельцина»
г.Екатеринбург, Российская Федерация

Фрайс Вероника Эдуардовна,
старший преподаватель,
кафедра Финансов, денежного обращения и кредита,
Высшая школа экономики и менеджмента,
ФГАОУ ВО «Уральский федеральный университет
имени первого Президента России Б.Н.Ельцина»
г.Екатеринбург, Российская Федерация

СОВРЕМЕННЫЕ МЕТОДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОМ СЕКТОРЕ

Аннотация:
В статье показана тенденция развития киберпреступности на современном этапе, а так же приведено описание современных методов защиты персональных данных в рамках функционирования банковской системы РФ.

Ключевые слова:
информационная безопасность, методы защиты, протекционная система, киберпреступность, криптографическая защита, инновационные разработки, блокчейн

Ни для кого не секрет, что с приходом эпохи информационных технологий мир подвергся всеобщей компьютеризации. На сегодняшний день развитие новых технологий идет полным ходом, предоставляя пользователям все большее поле для деятельности и, как следствие, неограниченные возможности в сфере поиска, обработки, хранения и передачи информации.

Вышеназванные обстоятельства, безусловно, приводят к росту и обострению конкуренции среди различных товаропроизводителей на мировой арене, а значит, все более непредсказуемыми и изощренными становятся методы взлома систем безопасности и охоты за конфиденциальной информацией.

Таким образом, постоянное, непрерывное совершенствование средств несанкционированного доступа различных уровней секретности требует ответного повышения качества методов и средств защиты, обуславливающую актуальность данной темы на сегодняшний день.

Рассмотрим ряд методов, обеспечивающих защиту инсайдерской информации в рамках банковской системы, поскольку вышеназванная сфера является наиболее уязвимой, а значит, требующей наиболее детализированную протекционную систему.

Важно так же отметить, что именно банковская сеть требует формирования четкой и эффективной политики в области защиты персональных данных, главным образом, основанной на анализе рисков и возможных угроз, поскольку клиент любого отдельно взятого банка должен быть уверен в сохранности своего капитала, а так же в обеспечении банком конфиденциальности переданной ему личной информации.

Первым способом следует обозначить создание уникальной, изолированной системы обработки данных. Кроме того, немаловажным способом является применение различных средств защиты информационных данных, таких как мониторинг, контентный анализ, средства криптографической защиты данных, а так же биометрический анализ. Однако следует отметить, что каждый из вышеперечисленных способов имеет ряд преимуществ и недостатков.

Определение наиболее подходящего способа защиты информации для каждого конкретного явления зависит от множества факторов, однако максимальную эффективность можно гарантировать исключительно при комплексном подходе к проблеме.

В современном мире при расследовании инцидентов предполагается использование таких методов, как мониторинг и аудит. Новейшие системы аудита способны распознать пользователей и их действия. Однако, система обладает рядом несовершенств. Например, для такой системы невозможно распознание вредоносных операций, которые могут повлечь такие последствия, как утечка информации. В случае отсутствия своевременной реакции инцидент может отрицательно сказаться на работе компании. Методом защиты от несанкционированного доступа к данным является сильная аутентификация. Для того, чтобы получить доступ к запрашиваемым данным в такой системе, необходимо пройти процедуру аутентификации в 2-3 этапа.

Далее, следует назвать лингвистический и морфологический анализ.Данная техника была разработана с опорой на контентный анализ текстов. На сегодняшний день можно назвать два вида анализа - количественный, где идет подсчет частоты встречаемости и весовых коэффициентов слов, и качественный, где ищутся в тексте строки о конкретных нужных темах.

Морфологический анализ позволяет проводить работы со словоформами, лингвистический же дает полный обзор предложения, он нацелен на поиск связи в словах. Также предполагается анализ информации с ранее данными ключевыми фразами. Одно из главных преимуществ этого метода заключается в том, что он разрешает читать конфиденциальную информацию, написанную в, так сказать, зашифрованном виде. Данная техника также совершенно нечувствительна к числу файлов, другими словами, база контентной фильтрации не растет в зависимости от введения новых документов или действий в организации. Эта техника малочувствительна к вариациям слов и к их месту в переложении, к их порядку. Нужно заметить, что использование данных техник в настоящий момент пока что выдает внушительное число ошибок первого и второго рода.

Контейнерный анализ, называющийся по-другому контекстной фильтрацией, был разработан, в отличие от предыдущих методов, не на анализе контента, а на анализе характеристик или атрибутов контейнера с информацией, а значит они не выполняют анализ данного информационного наполнения. Есть возможность анализировать тип приложения, отправителя, адресата, а кроме того характер документа или другого контейнера, где лежит информация. Хорошими образцами данного метода можно назвать те решения, которые были основаны на метках, помечающих конфиденциальный контент. Любой контейнер имеет вышеупомянутую метку, однозначно определяющую тип находящейся внутри контейнера информации.

Эти методы просят немного вычислительных ресурсов. Большой недостаток их заключается в том, что система заботится только о помеченном контенте: в том случае если метки не сущетсвует, контент находится под угрозой. Данный подход нередко включает в себя предварительную категоризацию информации с целью присвоения атрибутов и степеней конфиденциальности документам. Вторым минусом данного подхода можно назвать высокую трудность выполнения категоризации документов вручную, откуда выходит обязательньная автоматизация процесса категоризации. Поэтому здесь существует очень много методов: статистический, где идет подсчет частот ключевых слов, вероятностный, основанный на теореме Байеса, лингвистический, алгоритмы с использованием нейросетей, векторный, ка- тегоризация на основе онтологий. т.е. формальных расшифровок предметных структур за счет понятий и связей между ними.

На сегодняшний день и в условиях современных реалий функционирования банковского бизнеса все чаще и чаще учащаются случаи мошенничества посредствам банковских карт, а так же сервисами дистанционного обслуживания. Так, анализируя данные Сбербанка за 2016 год, можно сделать вывод о том, что число краж денежных средств непосредственно с банковских карт клиентов, осуществленных через интернет, по вине самих владельцев выросло на 78% , что составило 170 тыс. случаев, а доля мошенничества в финансовом секторе в целом достигла 98,5%.

Помимо всего прочего, использование мобильных приложений интернет-банкинга для входа в личный кабинет со своего смартфона подвергает пользователя не меньшему риску, в частности, использование устаревшего четырехзначного кода для осуществления входа, обходя полноценную процедуру ввода логина и пароля.

Таким образом, банки осознают необходимость активного внедрения новейших технологий с целью обеспечения лучшей защиты интересов своих клиентов. Одним из таких инновационных методов, снискавших особую популярность на сегодняшний день, являются биометрические системы, уже доступные на сегодняшний день в практике функционирования онлайн-банкинга Сбербанка, Тинькофф Банка, а так же МТС Банка и Альфа-Банка. Одним из примеров осуществления данного метода может служить вход в приложение по отпечатку пальца пользователя, чей смартфон оснащен специальными аутентикационными датчиками. Кроме того, Бинбанк анонсировал внедрение голосовой авторизации, а так же распознание клиентов по лицу для своих приложений в течение следующих двух лет.

Еще одним не менее интересным, на наш взгляд, примером использования биометрии в своей работе демонстрирует банк Авангард, руководство которого в феврале 2016 объявило о внедрении «процедуры удостоверения, включающей подтверждение личности и полномочий официальных представителей клиента, а так же фотосъемку». Более того, Авангард практикует эксплуатацию более усовершенствованной технологии, подразумевающей фиксировать биометрические параметры процесса подписания – динамические характеристики скорости написания при помощи электронных планшетов, а так же нажим, наклон пера и тд. Данная технология

электронной подписи обеспечивает полную идентичность заверяемых подписей и в разы уменьшает риски подделки.

В подтверждение актуальности вышеназванного метода защиты персональных данных, важно отметить, что в начале 2017 года банковское сообщество заявило о намерениях создать единую базу биометрических параметров своих клиентов, что позволит разным банкам обмениваться между собой данными своих клиентов и во многом упростит процедуру внедрения биометрических систем.[29]

Неменее многообещающие шансы на развитие и введение в нашу повседневную жизнь есть у неимоверно популярной технологии "блокчейн". Это такая распределенная база данных, хранящая данные о всех транзакциях членов системы по принципу «цепочки блоков». Одним из главных плюсов этого метода перед обычными банковскими транзакциями можно назвать неимение посредников, что обусловлено неимением у блокчейн центрального органа и проверкой работы непосредственно участниками.

Основой технологии блокчейн можно считать платежную систему «биткоин», которая обеспечивает фиксацию данных о прошедших между членами системы денежных переводах, которые были в течение всего времени бытия альтернативной денежной единицы. Сам по себе блокчейн выглядит как цепь связанных блоков, несущих в себе конкретный контент.

Структура цепочки блокчейн осуществляется на базе следующих принципов - распределенность, открытость и защита. Пользователи системы представляют собой как бы компьютерную сеть, что полностью характеризует систему как неуязвимую. Цепь Блокчейна стопроцентно зашифрована, а это гарант возможности получить правдивую и открытую информацию. Высокий уровень обещаннойх надежности и безопасности бесспорно дает право применять этот метод и в банковском секторе.

В январе 2017 года АКБ «РосЕвроБанк» сообщил о созданной им системе удаленной идентификации клиентов на базе технологии блокчейн от Microsoft, которая дает кардинально поменять рынок дистрибуции банковских предложений, дать пользователям банков широкий выход к продуктам и сервисам других банков-участников межбанковского консорциума без надобности личного присутствия. Проведение операции требует от клиента лишь через приложение заказать услугу стороннего банка, членом которого он не является, а банки уже за счет метода блокчейн сами завершат процесс идентификации. Так, пользователь имеет возможность выйти на широкий спектр банковских сервисов благодаря единому окну входа. Кроме того, о создании своего блокчейна – по типу системы «Цифровой Контракт», объявил "Внешэкономбанк". Данная система разрабатывается для того, чтобы дать защищенную, безопасную регистрацию и хранение ключевых ходов инвестиционного процесса, например, оформление договоров, приемка продуктов, подтверждение платежей.

Сбербанком России и ФАС России был запущен пилотный проект "Digital Ecosystem" по обмену файлами по принципу технологии блокчейн, что дает результаты в изучении вариантов распределённого хранения файлов. С помощью данной модели становится возможным отправлять и хранить документы в засекреченном виде, кроме того, можно применять электронную подпись. Инновационность этой работы заключается в том, что при документообороте не находят применения операторы связи, а это дает возможность банку снижать издержки.

Таким образом, следует отметить, что на сегодняшний день банки имеют перед собой широкую площадку для внедрения в свою деятельность инновационных технологий защиты информационной безопасности, что, в свою очередь, позволит обеспечить высокий уровень надежности и защищенности от мошеннических действий, а так же повысит уровень доверия и конкурентоспособность того или иного банка. Но не стоит забывать о том, что не стоит оставлять без внимания существующий на сегодняшний день в стране уровень развития банковского сервиса и готовность клиентов к понятию и принятию новшеств в российском банковском бизнесе.

Список используемых источников

1. Идентификация клиентов банка [Электронный ресурс]. URL: http://www.sonda.ru/product/biobank/biobank_15.html
2. Онлайн газета «Известия» https://iz.ru
3. Гамза В.А., Ткачук И.Б. Безопасность банковской деятельности: монография – 3-е изд. / В.А. Гамза., И. Б. Ткачук. - М.: Юрайт, 2014. – 513 с.
4. Т.9. – №1. – С. 124 - 136 3. Неевклидова биометрия: как российские банки теперь распознают клиентов [Электронный ресурс]. URL: http://www.rbc.ru/finances/19/01/2017/587e2c689a79470..
5. Федеральный закон от 27.07.2016 No 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_103797.

[29] По данным газеты «Известия» от 20 января 2017

Belkina Natalia,
Student,
Department of Finance, Money Circulation and Credit,
Graduate School of Economics and Management,
Ural Federal University
named after the first President of Russia B.N.Yeltsin
Ekaterinburg, Russian Federation

Stafilova Regina,
Student,
Department of Finance, Money Circulation and Credit,
Graduate School of Economics and Management,
Ural Federal University
named after the first President of Russia B.N.Yeltsin
Ekaterinburg, Russian Federation

Frais Veronika,
Senior lecturer,
Department of Finance, Money Circulation and Credit,
Graduate School of Economics and Management,
Ural Federal University
named after the first President of Russia B.N.Yeltsin
Ekaterinburg, Russian Federation

MODERN METHODS OF INFORMATION SECURITY IN THE BANKING SECTOR

Abstract:
The article shows the tendency of development of cybercrime at the present stage, as well as a description of modern methods of protecting personal data within the framework of the banking system of the Russian Federation.

Key words:
information security, protection methods, protection system, cybercrime, cryptographic protection, innovative developments, blocking