КОДЕКС ЭТИКИ
ИСПОЛЬЗОВАНИЯ
ДАННЫХ

БЕЛАЯ КНИГА

СВОД ЛУЧШИХ ПРАКТИК В СФЕРЕ ДОБРОСОВЕСТНОГО ИСПОЛЬЗОВАНИЯ ДАННЫХ

1010
0101
1010

УДАЛЕННАЯ ИДЕНТИФИКАЦИЯ

Пользователь проходит полную идентификацию в Компании 1. Пользователю присваивается уникальный идентификатор. Пользователь, прошедший идентификацию в Компании 1, обращается за сервисом в Компанию N. Компания N, с согласия пользователя осуществляет сверку идентификаторов с Компанией 1, устанавливает клиента* – и оказывает услугу

* практика не распространяется на ситуации обязательной идентификации, определенные федеральным законом 115-ФЗ. Важно отметить, что в рамках этой практики Компания 1 при проведении идентификации не вправе обогащать свои данные. Ее задача лишь оказать услугу по идентификации.

НАПРИМЕР:

Пользователь обращается, например, к сервису государственных услуг. Производится полная идентификация Пользователя, то есть осуществляется идентификация, обработка исохранение данных о Пользователе.
Пользователю присваивается уникальный идентификатор. При обращении Пользователя, например, на интернет-площадку, эта интернет-площадка не осуществляет идентификацию, а с согласия Пользователя, устанавливает его по уникальному идентификатору, осуществив сверку идентификаторов с сервисом государственных услуг

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

- ПОЛЬЗОВАТЕЛЬ ПОЛУЧАЕТ «БЕСШОВНЫЙ ДОСТУП» К СЕРВИСАМ И ЭКОНОМИТ СВОЁ ВРЕМЯ
- КОМПАНИИ ЭКОНОМЯТ ВРЕМЯ НА ОБСЛУЖИВАНИЕ
- КОМПАНИИ ПОВЫШАЮТ ДОСТУПНОСТЬ УСЛУГ ДЛЯ КЛИЕНТОВ ЗА СЧЁТ СНЯТИЯ ВХОДНОГО БАРЬЕРА
- РЕШЕНИЕ ОБЕСПЕЧИВАЕТ БЕЗОПАСНОСТЬ КЛИЕНТОВ

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ РОДСТВЕННИКОВ СОТРУДНИКОВ ПРИ ПРОВЕРКАХ В РАМКАХ СОБЛЮДЕНИЯ АНТИКОРРУПЦИОННОГО ЗАКОНОДАТЕЛЬСТВА

При возможном возникновении конфликта интересов или оценки работодателем возможности коррупционных действий, работник сообщает работодателю данные о родственниках, потенциальных участниках такого конфликта или таких действий.
Работодатель для оценки ситуации обрабатывает персональные данные родственников без получения от них согласия

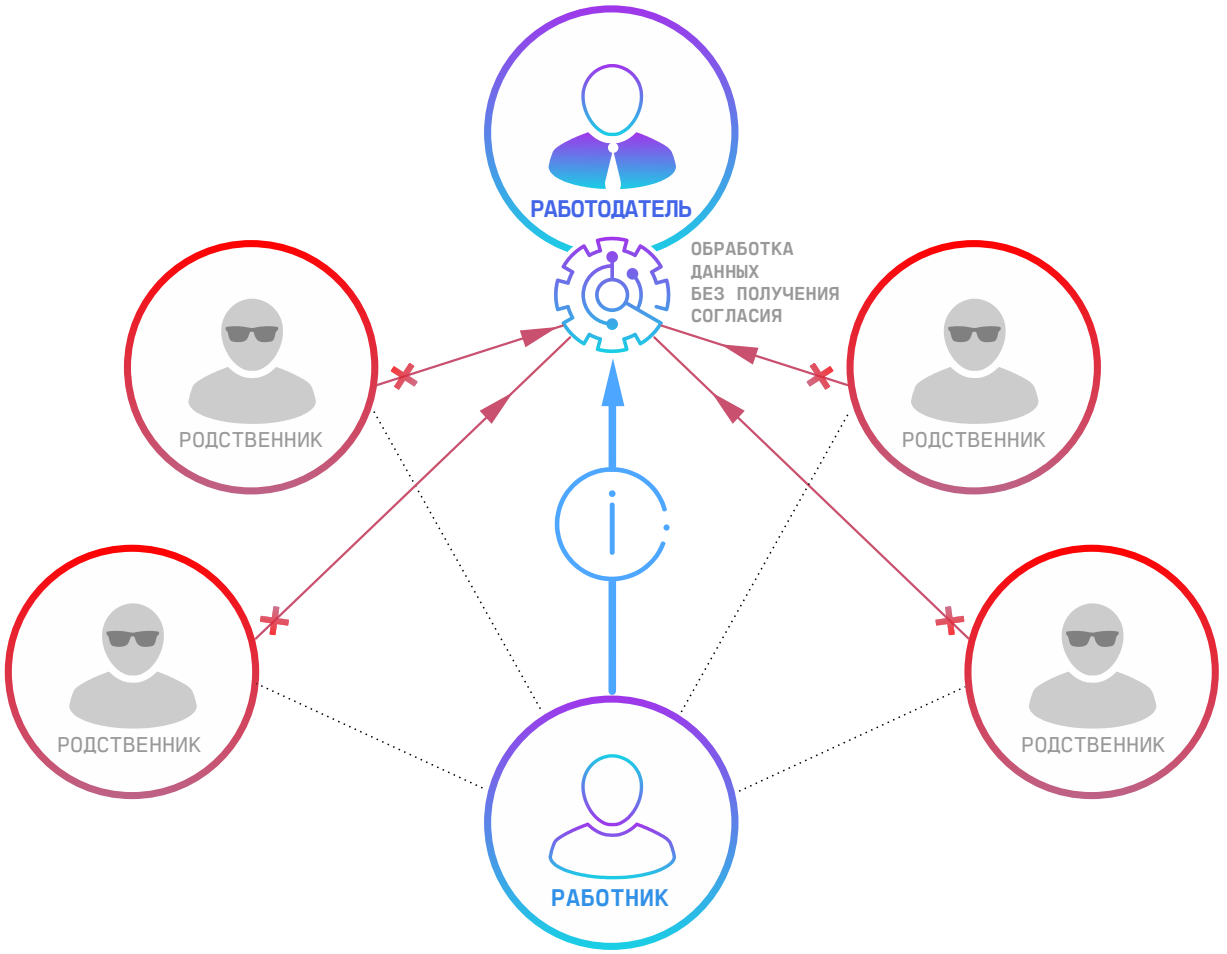
НАПРИМЕР:

При приеме или переводе на новую работу сотрудник указывает сведения о ФИО и трудовой деятельности своих родственников, которая может быть расценена как потенциальный конфликт интересов. Для оценки наличия или отсутствия конфликта интересов работодатель осуществляет проверку, используя полученную информацию, не запрашивая у поименованных родственников согласия на обработку полученных персональных данных

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

РАБОТОДАТЕЛЬ СМОЖЕТ ОЦЕНИТЬ НАЛИЧИЕ КОНФЛИКТА ИНТЕРЕСОВ И ПРИНЯТЬ АДЕКВАТНЫЕ МЕРЫ ПО ИХ ПРЕДОТВРАЩЕНИЮ ИЛИ УРЕГУЛИРОВАНИЮ

РАБОТОДАТЕЛЬ СМОЖЕТ ДОБРОСОВЕСТНО ИСПОЛНИТЬ АНТИКОРРУПЦИОННЫЕ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

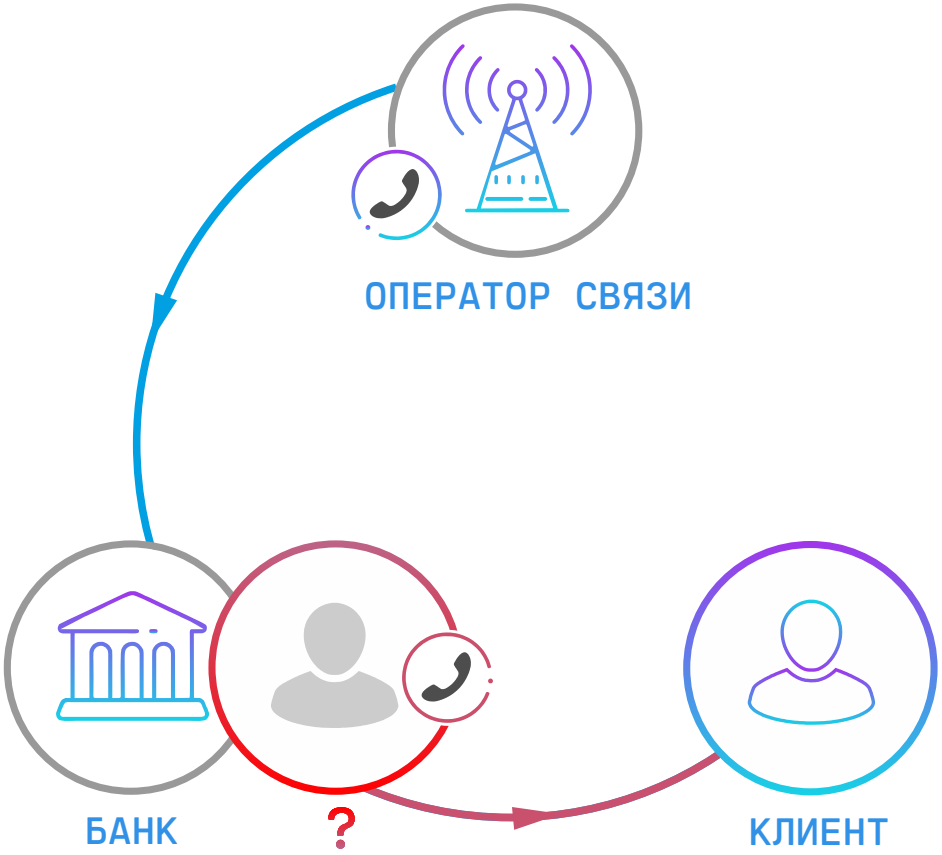


ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ С ЦЕЛЬЮ ЗАЩИТЫ СЧЕТОВ КЛИЕНТОВ

Для противодействия мошенничеству путем имитации входящего звонка от кредитной организации операторы связи в момент поступления такого звонка автоматически связываются с кредитной организацией для подтверждения

НАПРИМЕР:

При заключении договора обслуживания с кредитной организацией клиент/абонент соглашается на передачу своих персональных данных кредитной организацией оператору сотовой связи.
В момент звонка с подозрительного номера абоненту оператор передает эту информацию в кредитную организацию. Если по счетам клиента/абонента производятся сомнительные операции, то кредитная организация их блокирует до момента их подтверждения клиентом/абонентом



ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

ЗАЩИТА КЛИЕНТОВ ОТ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ ТРЕТЬИХ ЛИЦ В УДАЛЕННЫХ КАНАЛАХ, СНИЖЕНИЕ ПОТЕРЬ КЛИЕНТОВ ОТ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

СНИЖЕНИЕ ОПЕРАЦИОННЫХ И РЕПУТАЦИОННЫХ РИСКОВ КРЕДИТНЫХ ОРГАНИЗАЦИЙ, ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ДИСТАНЦИОННЫХ КАНАЛОВ ОБСЛУЖИВАНИЯ

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ С ЦЕЛЬЮ ЗАЩИТЫ СЧЕТОВ КЛИЕНТОВ 2

Для противодействия мошенничеству путем имитации входящего звонка от кредитной организации операторы связи в момент поступления такого звонка автоматически связываются с кредитной организацией для подтверждения

НАПРИМЕР:

При заключении договора обслуживания с кредитной организацией клиент/абонент соглашается на передачу своих персональных данных кредитной организацией оператору сотовой связи.
В момент звонка с подозрительного номера абоненту оператор передает эту информацию в кредитную организацию. Если по счетам клиента/абонента производятся сомнительные операции, то кредитная организация их блокирует до момента их подтверждения клиентом/абонентом

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

ЗАЩИТА КЛИЕНТОВ ОТ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ ТРЕТЬИХ ЛИЦ В УДАЛЕННЫХ КАНАЛАХ, СНИЖЕНИЕ ПОТЕРЬ КЛИЕНТОВ ОТ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

СНИЖЕНИЕ ОПЕРАЦИОННЫХ И РЕПУТАЦИОННЫХ РИСКОВ КРЕДИТНЫХ ОРГАНИЗАЦИЙ, ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ДИСТАНЦИОННЫХ КАНАЛОВ ОБСЛУЖИВАНИЯ

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ НА ФИНАНСОВОМ РЫНКЕ

Прямое взаимодействие кредитных организаций и операторов сотовой связи для получения сведений, связанных с подозрительными событиями (смена SIM карты, переадресация вызова, прекращение договора абонентского обслуживания, смена пользовательского устройства

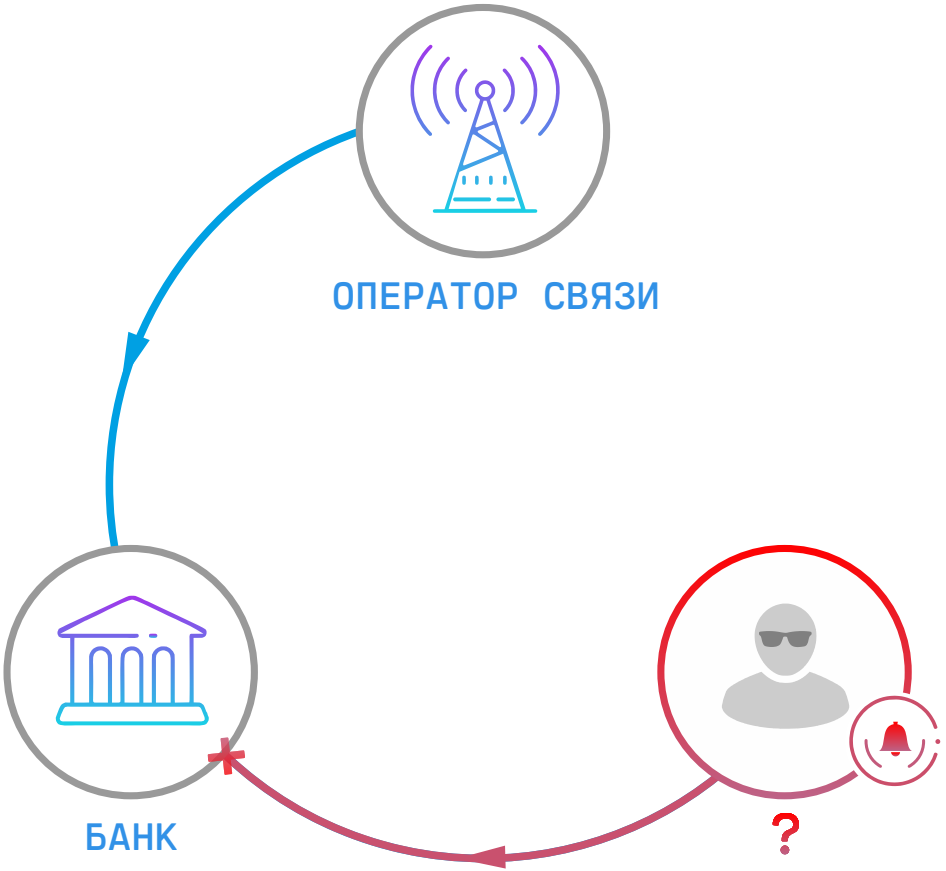
НАПРИМЕР:

При заключении договора обслуживания с кредитной организацией клиент/абонент соглашается на передачу своих данных оператором сотовой связи кредитной организации.
При совершении подозрительного события, например, при смене пользовательского устройства клиента/абонента, оператор отправляет данную информацию в кредитную организацию. Кредитная организация приостанавливает операции по счетам клиента/абонента до момента идентификации лица, их совершающего

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

ЗАЩИТА КЛИЕНТОВ ОТ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ ТРЕТЬИХ ЛИЦ В УДАЛЕННЫХ КАНАЛАХ, СНИЖЕНИЕ ПОТЕРЬ КЛИЕНТОВ ОТ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

СНИЖЕНИЕ ОПЕРАЦИОННЫХ И РЕПУТАЦИОННЫХ РИСКОВ КРЕДИТНЫХ ОРГАНИЗАЦИЙ, ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ДИСТАНЦИОННЫХ КАНАЛОВ ОБСЛУЖИВАНИЯ

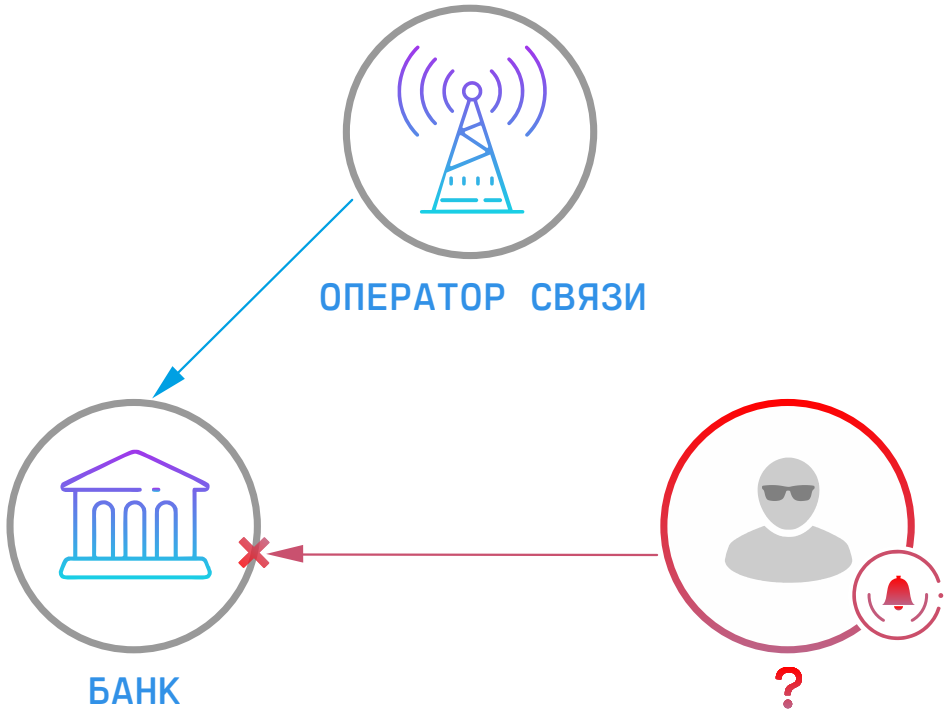


ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ НА ФИНАНСОВОМ РЫНКЕ 2

Прямое взаимодействие кредитных организаций и операторов сотовой связи для получения сведений, связанных с подозрительными событиями (смена SIM карты, переадресация вызова, прекращение договора абонентского обслуживания, смена пользовательского устройства

НАПРИМЕР:

При заключении договора обслуживания с кредитной организацией клиент/абонент соглашается на передачу своих данных оператором сотовой связи кредитной организации.
При совершении подозрительного события, например, при смене пользовательского устройства клиента/абонента, оператор отправляет данную информацию в кредитную организацию. Кредитная организация приостанавливает операции по счетам клиента/абонента до момента идентификации лица, их совершающего



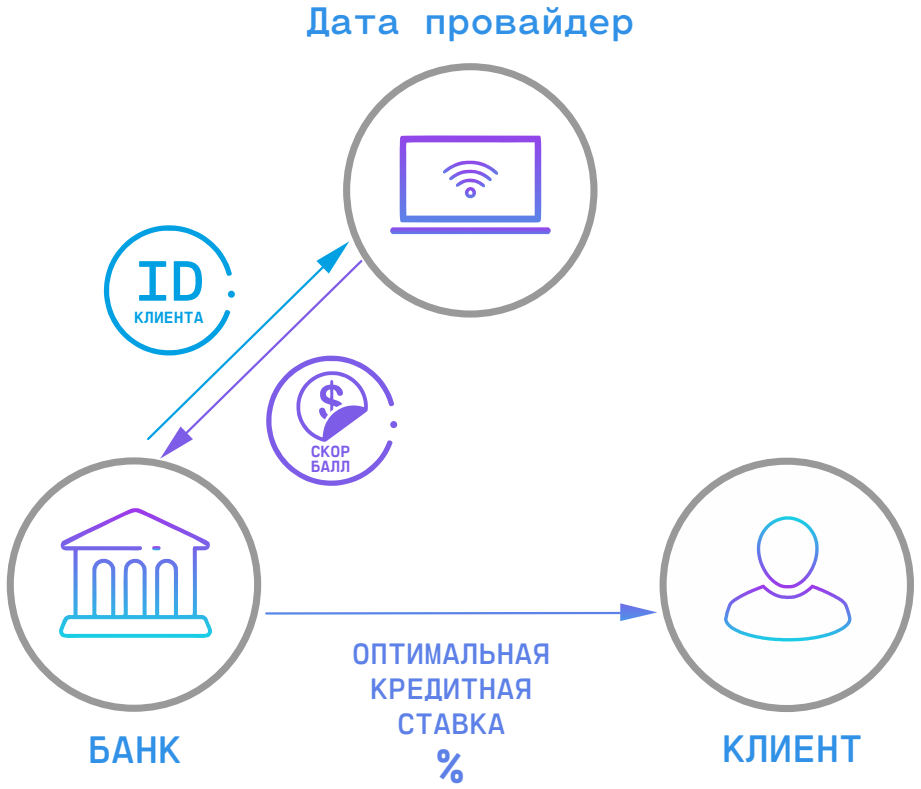
ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

ЗАЩИТА КЛИЕНТОВ ОТ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ ТРЕТЬИХ ЛИЦ В УДАЛЕННЫХ КАНАЛАХ, СНИЖЕНИЕ ПОТЕРЬ КЛИЕНТОВ ОТ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

СНИЖЕНИЕ ОПЕРАЦИОННЫХ И РЕПУТАЦИОННЫХ РИСКОВ КРЕДИТНЫХ ОРГАНИЗАЦИЙ, ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ДИСТАНЦИОННЫХ КАНАЛОВ ОБСЛУЖИВАНИЯ

СКОРИНГ КЛИЕНТОВ ПРИ ОБРАЩЕНИИ ЗА КРЕДИТОМ

При обращении клиента за кредитом кредитная организация, с согласия клиента, вправе обратиться к провайдерам аналитических услуг (например, сотовому оператору) для оценки вероятности возврата кредита данным клиентом. Для идентификации клиента провайдером используется уникальный идентификатор – номер мобильного телефона, адрес электронной почты и др. Провайдер производит оценку вероятности возврата кредита на основании собственных данных и математических моделей. Целью обращения является уточнение собственной оценки банка для предложения клиенту максимально низкой возможной ставки



НАПРИМЕР:

Клиент обращается в кредитную организацию за кредитом, заполняет заявку указывая свои данные, включая номер мобильного телефона и другие идентификаторы. Кредитная организация просит клиента дать согласие на обработку его персональных данных, а также на передачу их 3-му лицу – провайдеру аналитических услуг. Кредитная организация обращается к провайдеру аналитических услуг и просит предоставить вероятность возврата кредита клиентом на основании его идентификатора. Кредитная организация рассчитывает минимально возможную процентную ставку по кредиту для клиента на основании собственной риск политики и рассчитанного провайдером аналитических услуг скор балла

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

УДОБСТВО: В БОЛЬШИНСТВЕ СЛУЧАЕВ КЛИЕНТУ НЕ НУЖНО СОБИРАТЬ БОЛЬШОЙ КОМПЛЕКТ ДОКУМЕНТОВ ДЛЯ ОФОРМЛЕНИЯ КРЕДИТА (СПРАВКА О ДОХОДАХ, КОПИЯ ТРУДОВОЙ КНИЖКИ И ДР.). ПРИ НАЛИЧИИ СОГЛАСИЯ КЛИЕНТА, ВСЮ НЕОБХОДИМУЮ ДЛЯ ПРИНЯТИЯ РЕШЕНИЯ ИНФОРМАЦИЮ КРЕДИТНАЯ ОРГАНИЗАЦИЯ ПОЛУЧИТ У ПРОВАЙДЕРОВ АНАЛИТИЧЕСКИХ УСЛУГ

ВЗВЕШЕННОЕ РЕШЕНИЕ: ПРИ ПРИНЯТИИ РЕШЕНИЯ НА ОСНОВЕ РАЗЛИЧНЫХ СКОРИНГОВ ОЦЕНИВАЕТСЯ ВОЗМОЖНОСТЬ ЗАЕМЩИКА ПО ПОГАШЕНИЮ КРЕДИТА БЕЗ УЩЕРБА ДЛЯ БЮДЖЕТА СЕМЬИ

СКОРОСТЬ: РЕШЕНИЕ ПО КРЕДИТУ, КАК ПРАВИЛО, КЛИЕНТ ПОЛУЧАЕТ ЗА НЕСКОЛЬКО МИНУТ, Т.К.КРЕДИТНАЯ ОРГАНИЗАЦИЯ В ONLINE РЕЖИМЕ ПОЛУЧАЕТ ВСЮ НЕОБХОДИМУЮ ИНФОРМАЦИЮ, ОЦЕНИВАЕТ ЕЕ И ПРИНИМАЕТ РЕШЕНИЕ

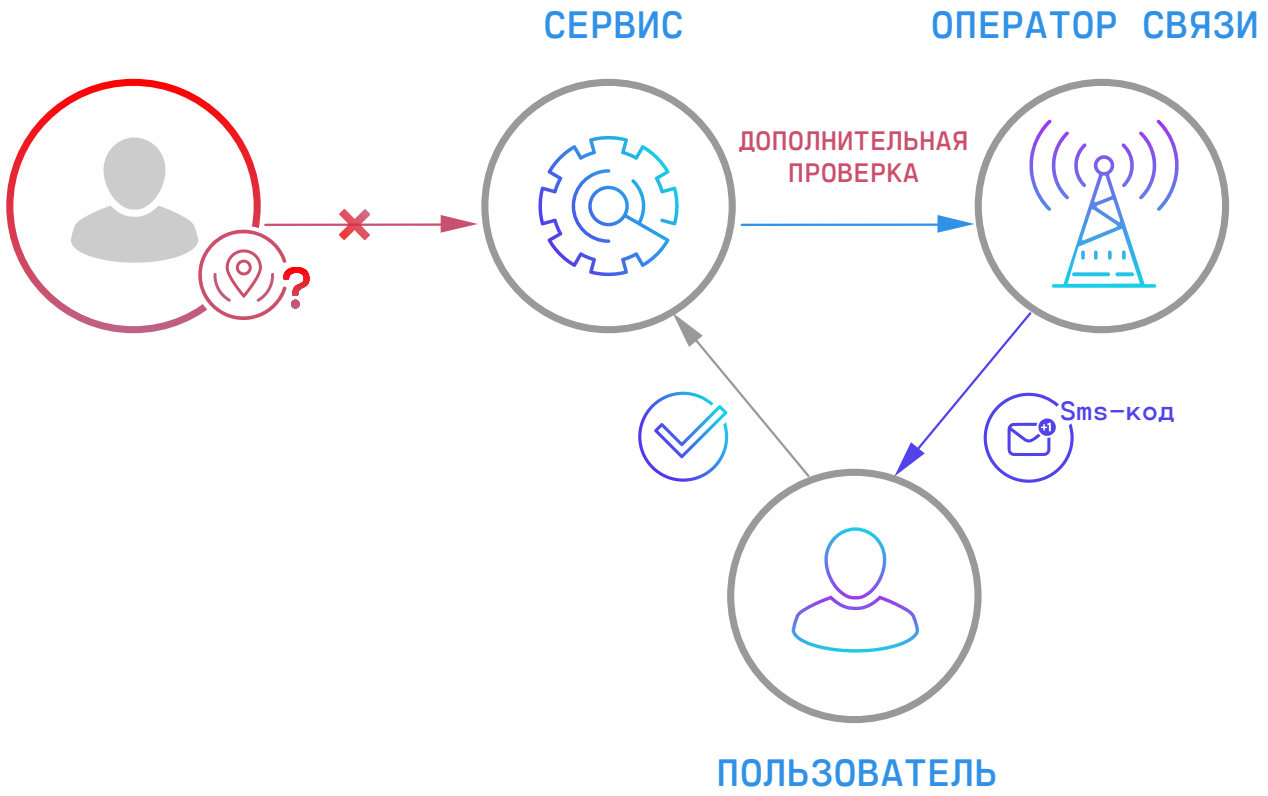
БОЛЕЕ ПРИВЛЕКАТЕЛЬНЫЕ УСЛОВИЯ ПО КРЕДИТУ: ЧЕМ БОЛЬШЕ У КРЕДИТНОЙ ОРГАНИЗАЦИИ ИНФОРМАЦИИ ПО КЛИЕНТУ, ТЕМ ТОЧНЕЕ ОНА МОЖЕТ ОЦЕНИТЬ УРОВЕНЬ РИСКА ПО КРЕДИТУ И ПРЕДЛОЖИТЬ ДЛЯ КЛИЕНТА ВЫГОДНЫЕ УСЛОВИЯ

СИСТЕМА ДОПОЛНИТЕЛЬНОЙ ВЕРИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ С ЦЕЛЬЮ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ

При авторизации из подозрительной локации (новая и/или значительно отдаленная) дополнительно запрашивается ввод кода, который отправляется пользователю по дополнительному каналу связи (например, в СМС-сообщении)

НАПРИМЕР:

При первой авторизации в сервисе сохраняются данные о геолокации пользователя. В дальнейшем, если авторизация происходит из подозрительной локации, то клиенту по дополнительному каналу связи направляется код, который вводится в специальном поле верификации. Допускается использование иных способов верификации добросовестной пользовательской активности. Подозрительная локация – та, которая отличается от первоначального местоположения, где проходила авторизация пользователя (а также находится на большом расстоянии от него – например, в другой области).

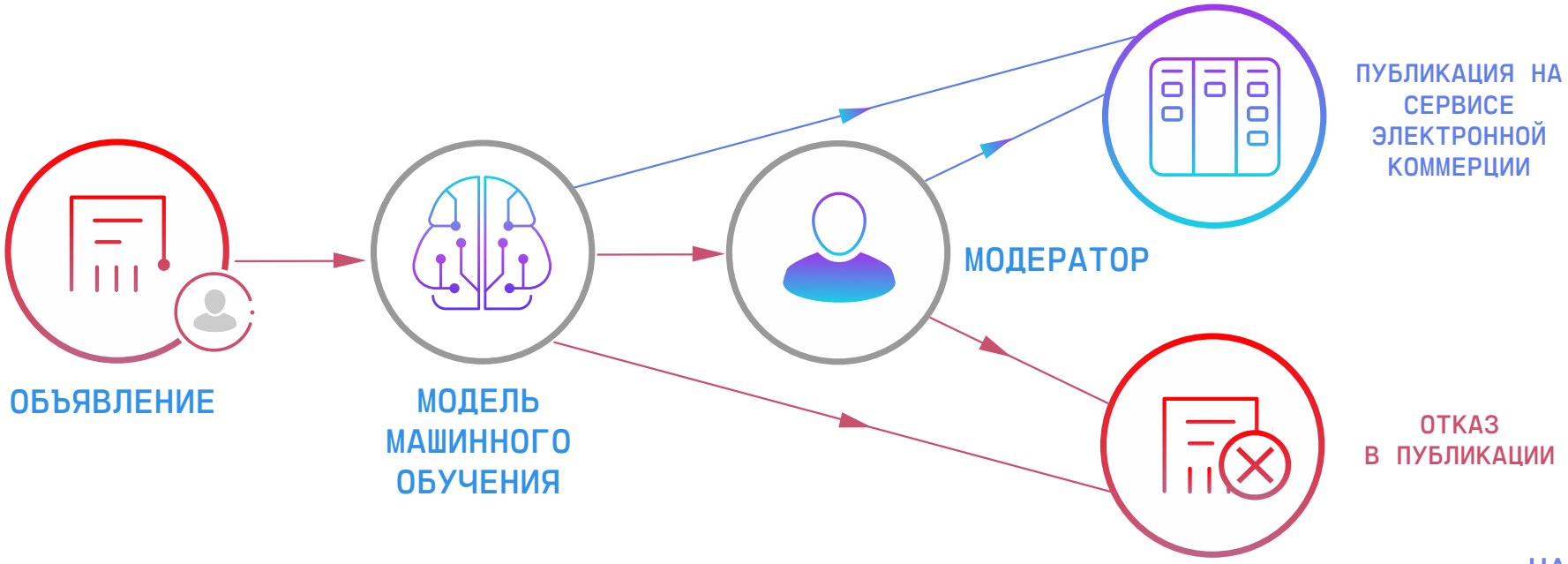


ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ И КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЯ ОТ ВОЗМОЖНОГО ВЗЛОМА СИСТЕМЫ ИЗ-ЗА ДИСКРЕДИТАЦИИ ЛОГИНА И ПАРОЛЯ ПОЛЬЗОВАТЕЛЯ В РЕЗУЛЬТАТЕ ФИШИНГА ИЛИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, ИЛИ ЛЮБОГО ДРУГОГО МЕТОДА ВЗЛОМА

СНИЖЕНИЕ РИСКА ПОЯВЛЕНИЯ НЕДОВОЛЬСТВА И МАТЕРИАЛЬНЫХ ПРЕТЕНЗИЙ К СЕРВИСУ ОТ ПОЛЬЗОВАТЕЛЯ ВЗЛОМАННОГО АККАУНТА

ПРЕДОТВРАЩЕНИЕ РАЗМЕЩЕНИЯ ОБЪЯВЛЕНИЙ С ЗАПРЕЩЕННЫМИ ТОВАРАМИ И УСЛУГАМИ, И ДУБЛИРОВАНИЯ ОБЪЯВЛЕНИЙ



При размещении объявления происходит оценка загруженного контента, в том числе с использованием автоматической обработки данных (текст объявления, хеши ip адресов и cookie, хеши изображений) алгоритмами машинного обучения, затем выносится вердикт о допуске объявления, его отклонении, или необходимости ручной модерации, по результатам

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

- СОДЕЙСТВИЕ СОБЛЮДЕНИЮ ЗАКОНОДАТЕЛЬСТВА. ОГРАНИЧЕНИЕ ТОРГОВЛИ ЗАПРЕЩЕННЫМ ТОВАРОМ
- ЗАЩИТА ПОЛЬЗОВАТЕЛЕЙ ОТ НЕПРИЕМЛЕМОГО КОНТЕНТА
- ПОВЫШЕНИЕ УДОБСТВА СЕРВИСА БЛАГОДАРЯ ФИЛЬТРАЦИИ ДУБЛИРУЮЩИХ ОБЪЯВЛЕНИЙ

НАПРИМЕР:

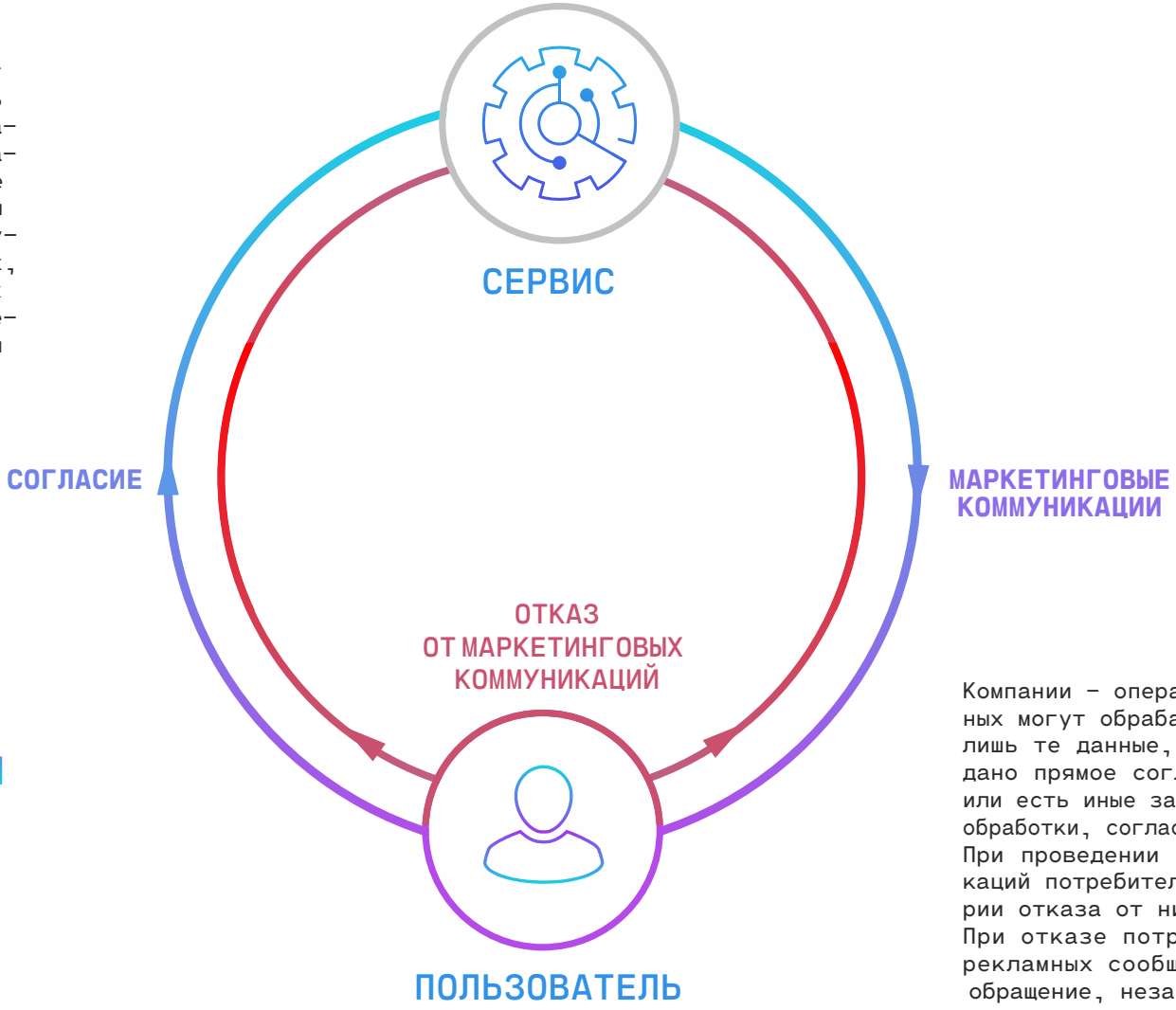
Пользователь электронной доски объявлений размещает объявление с запрещенным товаром или услугой, либо создает дублирующее объявление.

При публикации, многие факторы объявления, в том числе данные пользователя и параметры объявления (хеши ip адресов и cookie, тексты объявлений, а также хеши изображений) проверяются на соответствие законодательству и политике сервиса различными методиками, включая модели машинного обучения, и выносится вердикт соответствия.

По результатам проверки, объявление либо допускается к публикации, либо отклоняется, либо направляется на ручную проверку модератором, если нет достаточной уверенности в корректности автоматизированного вердикта. По результатам ручной модерации проводится обновление модели

МЕХАНИЗМ ПОЛУЧЕНИЯ И ОБРАБОТКИ ОБРАЩЕНИЙ ЛИЦ, ОТКАЗАВШИХСЯ ОТ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ И/ИЛИ ОТ ОБРАБОТКИ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъект персональных данных может потребовать у оператора остановить обработку своих данных таким оператором с использованием его информационных систем и баз данных, после чего незамедлительно прекращается любое использование данных для коммуникации, а также в маркетинговых, аналитических и любых иных целях (за исключением случаев, когда у оператора есть иные законные основания такой обработки)



ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

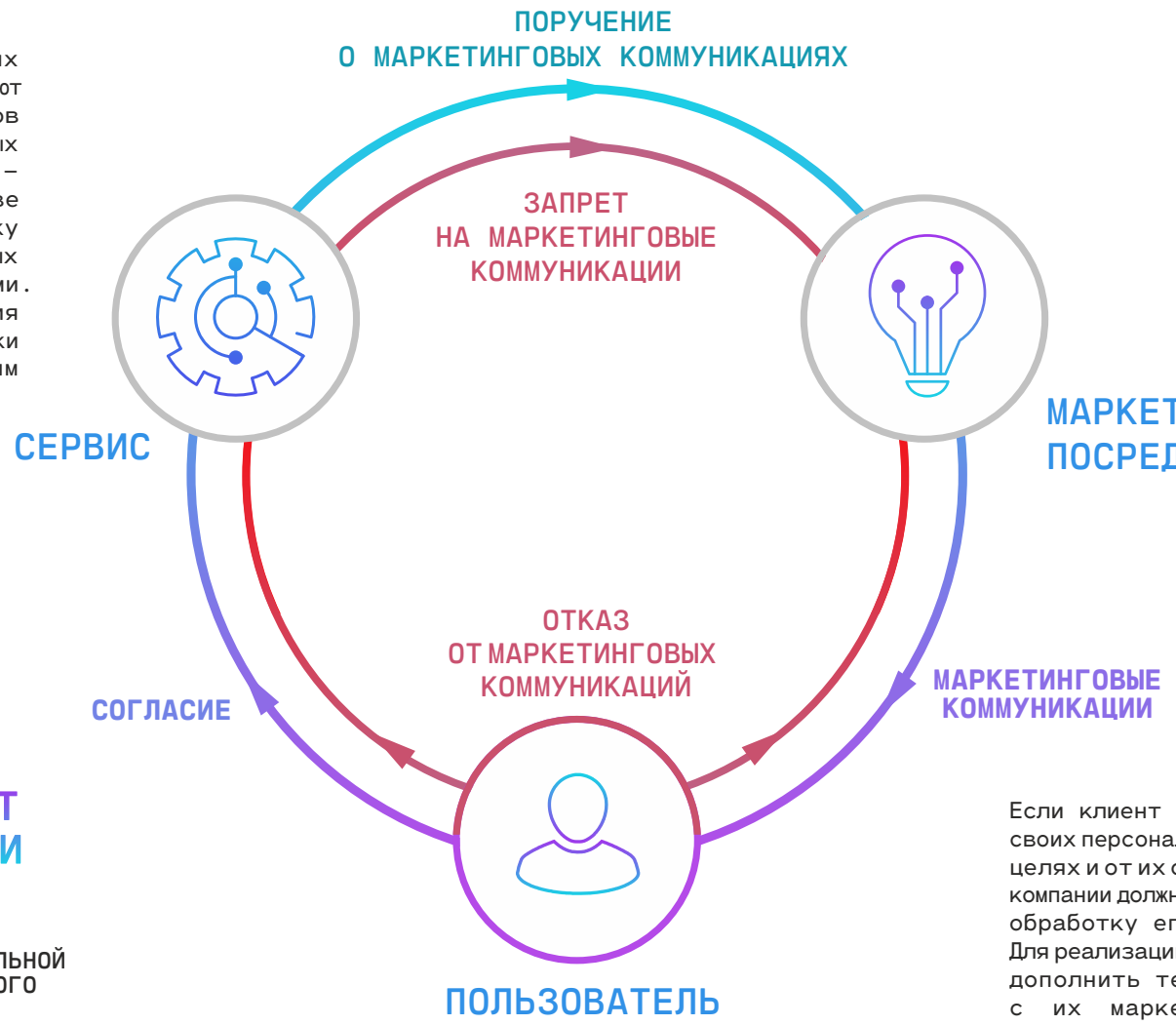
- ЗАЩИТА ГРАЖДАН ОТ НЕЖЕЛАТЕЛЬНОЙ КОММУНИКАЦИИ И НЕЖЕЛАТЕЛЬНОГО ИСПОЛЬЗОВАНИЯ СВОИХ ДАННЫХ
- ПРЕДОТВРАЩЕНИЕ СЛУЧАЕВ ПРИВЛЕЧЕНИЯ К ОТВЕТСТВЕННОСТИ КОМПАНИЙ ВСЛЕДСТВИЕ ДЕЙСТВИЙ МАРКЕТИНГОВЫХ ПОСРЕДНИКОВ
- ФОРМИРОВАНИЕ ПОЗИТИВНОГО ОТНОШЕНИЯ К КОМПАНИИ И ЕЕ ПРОДУКТАМ СО СТОРОНЫ ПОТРЕБИТЕЛЯ

НАПРИМЕР:

Компании – операторы персональных данных могут обрабатывать и использовать лишь те данные, на обработку которых дано прямое согласие субъекта данных или есть иные законные основания такой обработки, согласно законодательству РФ.
При проведении маркетинговых коммуникаций потребителям предлагаются сценарии отказа от них.
При отказе потребителя от получения рекламных сообщений учитывается это обращение, незамедлительно прекращается направление потребителю таких сообщений посредством информационных систем, посредством собственных каналов коммуникации.
При этом, каждой компанией ведется учет лиц, отказавшихся от получения рекламных сообщений

МЕХАНИЗМ ОТКАЗА ПОЛЬЗОВАТЕЛЯ ОТ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ, КОТОРЫЕ РЕАЛИЗУЕТ МАРКЕТИНГОВЫЙ ПОСРЕДНИК

Для осуществления маркетинговых коммуникаций многие компании прибегают к услугам маркетинговых посредников и поручают им обработку персональных данных клиентов. При этом клиент – субъект персональных данных, вправе отозвать свое согласие на обработку персональных данных в маркетинговых целях и на их обработку третьими лицами. При наличии такого возражения компания обязана обеспечить прекращение обработки персональных данных маркетинговым посредником



ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

ЗАЩИТА ГРАЖДАН ОТ НЕЖЕЛАТЕЛЬНОЙ КОММУНИКАЦИИ И НЕЖЕЛАТЕЛЬНОГО ИСПОЛЬЗОВАНИЯ СВОИХ ДАННЫХ

ПРЕДОТВРАЩЕНИЕ СЛУЧАЕВ ПРИВЛЕЧЕНИЯ К ОТВЕТСТВЕННОСТИ КОМПАНИЙ ВСЛЕДСТВИЕ ДЕЙСТВИЙ МАРКЕТИНГОВЫХ ПОСРЕДНИКОВ

НАПРИМЕР:

Если клиент отказывается от обработки своих персональных данных в маркетинговых целях и от их обработки третьими лицами, компании должны незамедлительно прекратить обработку его персональных данных. Для реализации этого механизма необходимо дополнить текущие договоры компаний с их маркетинговыми посредниками следующими положениями:
порядок и сроки передачи отказа клиента, незамедлительное прекращение обработки, а также в перечень операций с данными включить уничтожение персональных данных в отношении данных, согласие на обработку которых субъект давал сервису

ОБЕЗЛИЧИВАНИЕ ДАННЫХ ДЛЯ СИСТЕМ ТЕСТИРОВАНИЯ И ЭКСПЕРИМЕНТАЛЬНЫХ ПРАВОВЫХ РЕЖИМОВ

При наличии согласия клиента на обработку персональных данных в соответствующих целях, компании вправе тестировать свои системы с использованием баз данных, содержащих персональные данные. Для таких случаев многие компании проводят процедуры по удалению (обезличивания) персональных данных. Кроме этого, в рамках экспериментальных правовых режимов, также должны использоваться данные в обезличенном виде

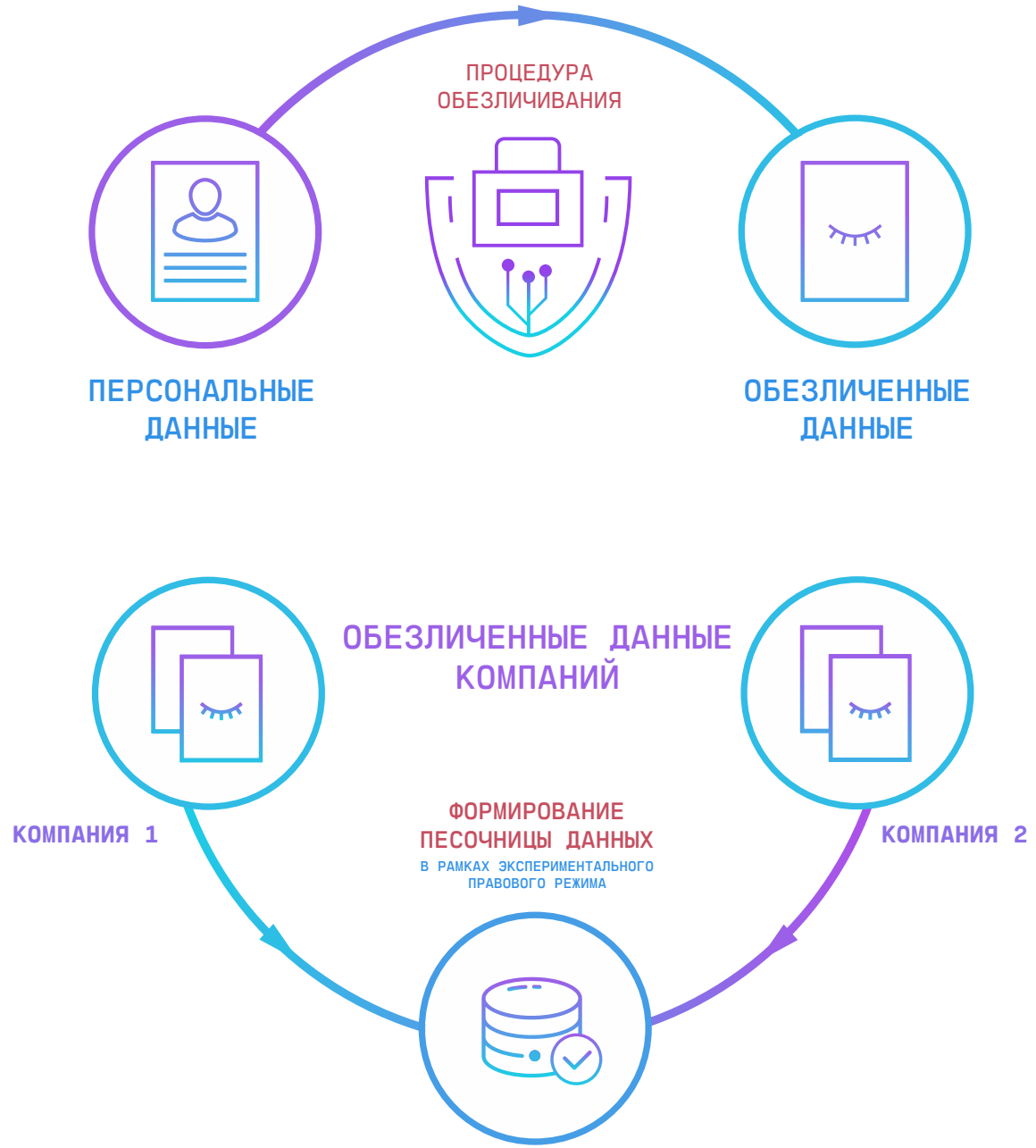
НАПРИМЕР:

При тестировании и экспериментировании с данными организации должны обеспечить отсутствие возможности определить принадлежность персональных данных конкретному человеку путем обезличивания этих данных. Для выбора метода обезличивания, применимого к набору данных (dataset), необходимо определить каким образом будет использоваться конечный (обезличенный) набор данных.Процедура обезличивания возможна как при использовании существующих на рынке инструментов,так и посредством собственного программного обеспечения компаний

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

УМЕНЬШЕНИЕ РИСКОВ И ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА ПРАВ ГРАЖДАН

ВОЗМОЖНОСТЬ ОБЪЕДИНЕНИЯ ОБЕЗЛИЧЕННЫХ ДАННЫХ РАЗЛИЧНЫХ КОМПАНИЙ ДЛЯ ТЕСТОВЫХ ПРОЕКТОВ В РАМКАХ ЭКСПЕРИМЕНТАЛЬНЫХ ПРАВОВЫХ РЕЖИМОВ



ПРЯМЫЕ МАРКЕТИНГОВЫЕ КОММУНИКАЦИИ С ЦЕЛЬЮ ПОВЫШЕНИЯ КОЛИЧЕСТВА ПРОДУКТОВ НА ОДНОГО КЛИЕНТА

Действующее законодательство Российской Федерации предусматривает возможность осуществления прямых рекламных коммуникаций с существующим клиентом (потребителем) с помощью средств связи, только при наличии его предварительного согласия.

То есть любая реклама посредством телефонной связи без предварительного согласия потребителя запрещена.
Вместе с тем законом не определяется порядок и форма получения такого предварительного согласия потребителя.
Следовательно, согласие потребителя может быть выражено в любой форме, достаточной для подтверждения его волеизъявления на взаимодействие с конкретной целью – получение рекламы.

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

- ОТВЕЧАЕТ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА И СЛОЖИВШЕЙСЯ СУДЕБНОЙ ПРАКТИКЕ
- НЕ ДОПУСКАЕТ ВВЕДЕНИЕ ПОТРЕБИТЕЛЯ В ЗАБЛУЖДЕНИЕ
- ФОРМИРОВАНИЕ ПОЗИТИВНОГО ОТНОШЕНИЯ К КОМПАНИИ И ЕЕ ПРОДУКТАМ СО СТОРОНЫ ПОТРЕБИТЕЛЯ

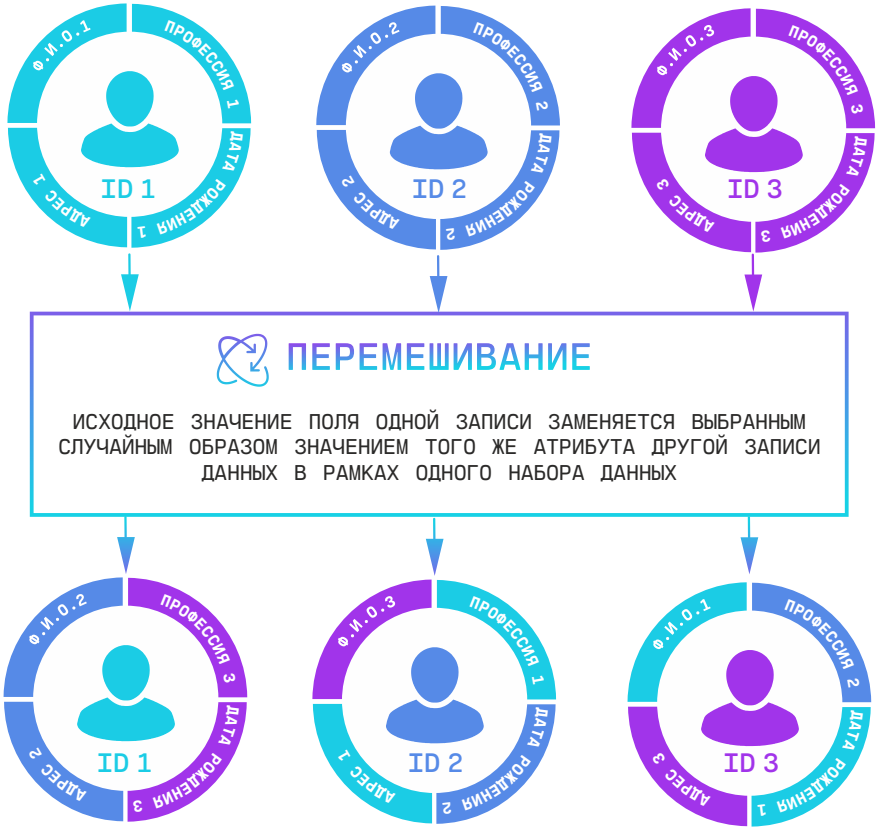
КОММУНИКАЦИИ ПО УЖЕ ПРЕДОСТАВЛЯЕМЫМ УСЛУГАМ

НАПРИМЕР:

При отсутствии у компании предварительного согласия абонента на осуществление рекламных коммуникаций, полученного до непосредственного совершения звонка, считаем одним из примеров допустимой практики сообщение потребителю рекламной информации во время осуществления прямых контактов по иным уже предоставляемым услугам при условии явно выраженного предварительного согласия на получение такой информации в ходе звонка.

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ МЕТОДОМ ПЕРЕМЕШИВАНИЯ (ШАФЛ)

В любой компании возникает необходимость разработки нового и улучшения существующего программного обеспечения, что обусловлено широким использованием технологий в повседневной жизни, повышением ожиданий пользователей от программного обеспечения и иными факторами. Малейшая ошибка в программном обеспечении может повлечь колоссальные расходы, а также репутационные издержки. В связи с этим компании проводят различные виды тестирования систем и программного обеспечения (наиболее распространенные – нагрузочное и функциональное).
Обычной практикой является развертывание систем тестирования путем клонирования промышленной системы: таким образом если в промышленной системе есть персональные данные, то в системах тестирования к ним получат доступ специалисты по тестированию. Если задачами тестирования не является испытания методов обработки персональной информации, то целесообразно обезличивать данные в системах тестирования в целях обеспечения дополнительной защиты.



ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

НАХОЖДЕНИЕ ДАННЫХ В ОДНОЙ СИСТЕМЕ/ БАЗЕ ДАННЫХ/ТАБЛИЦЕ

СОХРАНЕНИЕ ВНУТРЕННИХ ИДЕНТИФИКАТОРОВ ДЛЯ СВЯЗИ С ДАННЫМИ ДРУГИХ СИСТЕМ/ БАЗ ДАННЫХ/ТАБЛИЦ

ВЫСОКАЯ СКОРОСТЬ РАБОТЫ

ПРОСТОТА РЕАЛИЗАЦИИ АЛГОРИТМА ОБЕЗЛИЧИВАНИЯ

СЛОЖНОСТЬ ВОССТАНОВЛЕНИЯ ИСХОДНЫХ ДАННЫХ ОПЕРАТОРОМ ПРОПОРЦИОНАЛЬНА КОЛИЧЕСТВУ ЗАПИСЕЙ И КОЛОНОК

ПОЛНОЕ СОХРАНЕНИЕ ДАННЫХ ПО ОТДЕЛЬНЫМ КОЛОНКАМ, ЧТО ДЕЛАЕТ ИХ ОГРАНИЧЕННО ПРИГОДНЫМИ ДЛЯ СТАТИСТИЧЕСКОГО АНАЛИЗА

НАПРИМЕР:

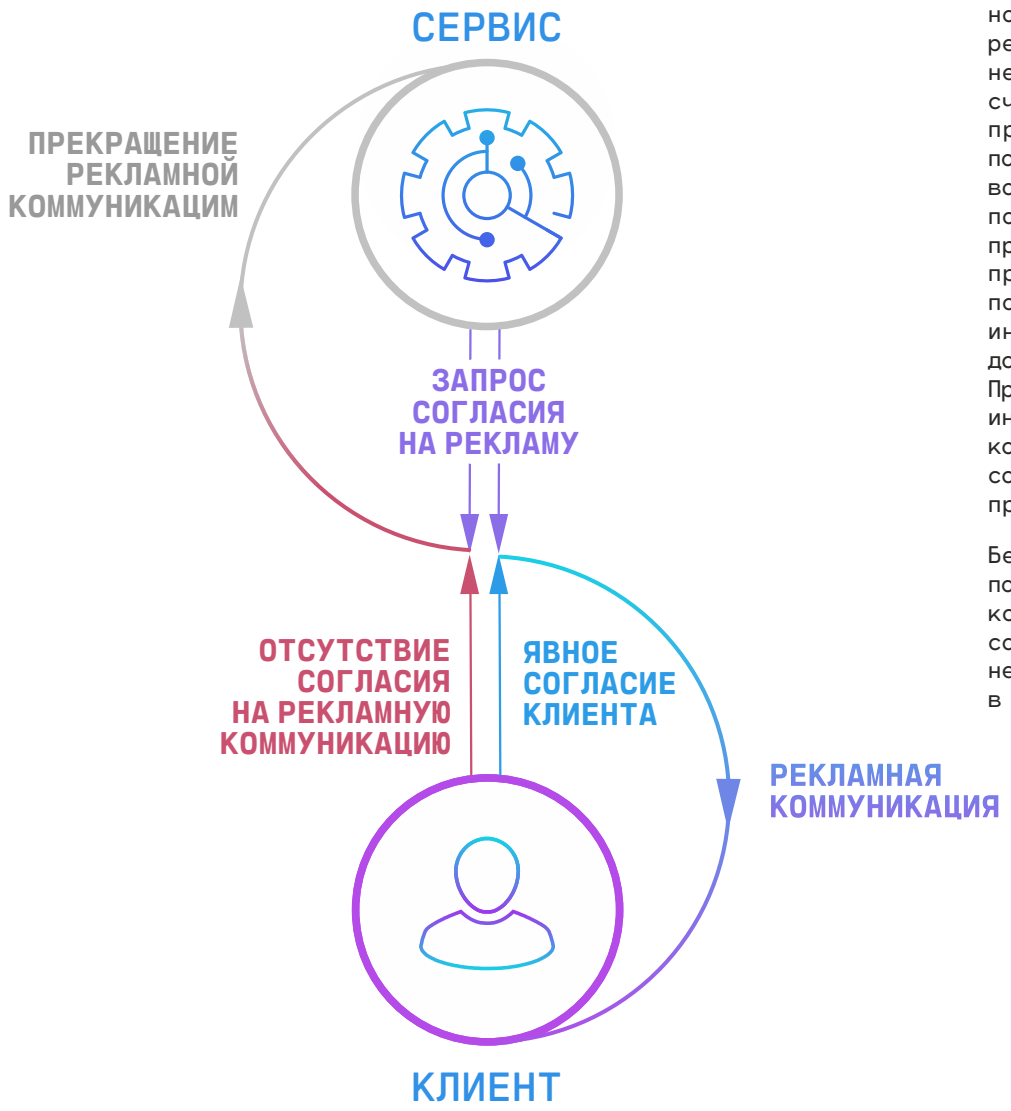
Считаем одним из примеров рекомендованной практики обезличивание персональных данных для внутреннего использования компанией, например, для тестирования систем, методом перемешивания (шафл), согласно которому исходное значение поля одной записи заменяется выбранным случайным образом значением того же атрибута другой записи данных в рамках одного набора данных (базы данных).
Данный метод используется, когда важно сохранить уникальные (хотя скорректированные) записи, например, с целью сохранения бизнес-логики и работоспособности приложений в случае необходимости модификации ключевых полей, значения которых не представляют ценности без связи со значениями других полей записи.
По завершении использования тестовой среды, содержащей обезличенные по настоящей методике данные, подобная тестовая Среда подлежит уничтожению со всеми содержащимися в ней данными.
Рекомендуется применять практику в качестве одного из шагов развертывания систем тестирования совместно с другими техническими и организационными методами защиты данных в организациях.
Применение данного метода может не приводить к окончательной анонимизации или псевдоанонимизации данных, однако приведенный метод обезличивания в комбинации с другими методами, такими как замена чувствительных к идентификации атрибутов на квази-идентификаторы, может применятся для псевдоанонимизации и анонимизации набора данных.

ПРЯМЫЕ МАРКЕТИНГОВЫЕ КОММУНИКАЦИИ С ЦЕЛЬЮ ПОВЫШЕНИЯ КОЛИЧЕСТВА ПРОДУКТОВ НА ОДНОГО КЛИЕНТА

КОММУНИКАЦИИ ПО УЖЕ ПРЕДОСТАВЛЯЕМЫМ УСЛУГАМ

Действующее законодательство Российской Федерации предусматривает возможность осуществления прямых рекламных коммуникаций с существующим клиентом (потребителем) с помощью средств связи, только при наличии его предварительного согласия.

То есть любая реклама посредством телефонной связи без предварительного согласия потребителя запрещена.
Вместе с тем законом не определяется порядок и форма получения такого предварительного согласия потребителя.
Следовательно, согласие потребителя может быть выражено в любой форме, достаточной для подтверждения его волеизъявления на взаимодействие с конкретной целью – получение рекламы.



НАПРИМЕР:

При отсутствии у компании предварительного согласия абонента на осуществление рекламных коммуникаций, полученного до непосредственного совершения звонка, считаем одним из примеров допустимой практики сообщение существующему потребителю компании рекламной информации во время осуществления прямых контактов по иным уже предоставляемым услугам при условии получения явно выраженного предварительного согласия такого потребителя на получение рекламной информации в ходе звонка, позволяющего достоверно установить его волеизъявление.
При этом, учитывая необходимость получения информированного согласия, представитель компании до запроса у потребителя данного согласия должен представиться и озвучить представляемую им компанию.

Без получения явно выраженного согласия потребителя на осуществление маркетинговой коммуникации или в случае получения соответствующего отказа, компания должна незамедлительно прекратить коммуникацию в указанных целях

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

ПРЕДЛОЖЕННАЯ ПРАКТИКА ПОЗВОЛЯЕТ НЕ ДОПУСТИТЬ ВВЕДЕНИЕ ПОТРЕБИТЕЛЯ В ЗАБЛУЖДЕНИЕ ОТНОСИТЕЛЬНО ДЕЙСТВИТЕЛЬНОЙ ЦЕЛИ КОММУНИКАЦИИ

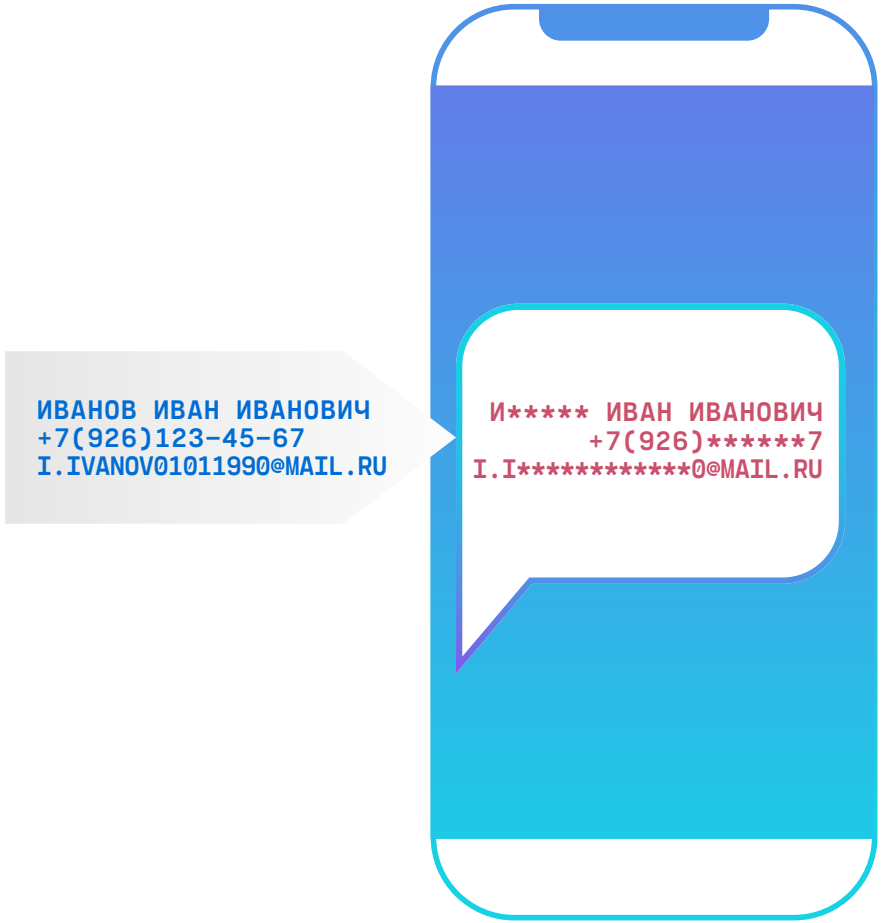
ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ МЕТОДОМ МАСКИРОВАНИЯ

Интернет-сервисы для обеспечения защиты аккаунтов пользователей и их персональных данных предоставляют доступ к аккаунту исключительно его владельцу при успешной авторизации на портале.

С точки зрения безопасности аккаунта наиболее важным этапом авторизации является аутентификация.

В ряде случаев, с целью повышения уровня безопасности и обеспечения дополнительной защиты персональных данных интернет-сервисами используется двухфакторная аутентификация пользователя – метод, при котором пользователю для получения доступа необходимо предоставить два разных типа аутентификационных данных, например, пароль и код, который пользователь получает в СМС-сообщении по номеру телефона или электронном сообщении по адресу электронной почты, привязанные пользователем к своему аккаунту.

В таком случае интернет-сервисом пользователю направляется уведомление с указанием соответствующего номера телефона или адреса электронной почты, на которые направлен данный код.



НАПРИМЕР:

Считаем одним из примеров рекомендованной практики в уведомлении, направляемом интернет-сервисом пользователю в рамках осуществления процедуры аутентификации, обезличивать содержащиеся в нем персональные данные, например, посредством использования метода маскирования.

Метод маскирования заключается в наложении маски (например, удаление/скрытие) на каждую ячейку, ранее содержащую однозначные идентификаторы.

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

НИВЕЛИРОВАНИЕ СЛУЧАЕВ ПРЕДОСТАВЛЕНИЯ ТРЕТЬИМ ЛИЦАМ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ ПОЛЬЗОВАТЕЛЯ. ПРИ ЭТОМ САМ ПОЛЬЗОВАТЕЛЬ, ПОЛУЧАЯ УВЕДОМЛЕНИЕ, СОДЕРЖАЩЕЕ ТАКИМ ОБРАЗОМ ОБЕЗЛИЧЕННЫЕ ДАННЫЕ, МОЖЕТ БЕСПРЕПЯТСТВЕННО ИДЕНТИФИЦИРОВАТЬ НОМЕР ТЕЛЕФОНА ИЛИ АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ, НА КОТОРЫЕ НАПРАВЛЕН КОД, НЕОБХОДИМЫЙ ДЛЯ ПРОХОЖДЕНИЯ ПРОЦЕДУРЫ АУТЕНТИФИКАЦИИ.

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ МЕТОДОМ ИСПОЛЬЗОВАНИЯ СИНТЕТИЧЕСКИХ ИДЕНТИФИКАТОРОВ В ЦЕЛЯХ РАЗРАБОТКИ И ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Любая современная организация использует различные приложения для автоматизации бизнес-процессов. За время работы она накапливает большие массивы информации в виде баз данных. Наиболее чувствительны, как правило, клиентские, платежные, финансовые и другие виды конфиденциальных данных.

При этом для целей тестирования и внедрения программного обеспечения возникает необходимость подготовки данных максимально похожих на реальные, хранящиеся в продуктивных базах.

В целях обеспечения защиты, конфиденциальные данные, содержащиеся в базах данных, используемых разработчиками и тестировщиками, целесообразно обезличивать.

ВОЗРАСТ	ПОЛ	СНИЛС	МЕСЯЦ	МЕСЯЧНЫЙ ДОХОД	МЕСЯЧНЫЙ РАСХОД
23	М	123-456-789-01	Январь	80 000	20 000
35	Ж	749-423-789-02	Январь	150 000	60 000
64	М	749-623-777-03	Январь	35 000	10 000
23	М	123-456-789-01	Февраль	70 000	30 000
35	Ж	749-423-789-02	Февраль	160 000	50 000
64	М	749-623-777-03	Февраль	45 000	15 000

ПОСЛЕ ИСПОЛЬЗОВАНИЯ СИНТЕТИЧЕСКИХ ИДЕНТИФИКАТОРОВ
ПО АТРИБУТУ «СНИЛС»
МОЖНО ДОБИТЬСЯ ДЕПЕРСОНАЛИЗАЦИИ
ПРИ СОХРАНЕНИИ ИНДИВИДУАЛЬНОСТИ ЗАПИСЕЙ

ВОЗРАСТ	ПОЛ	СНИЛС	МЕСЯЦ	МЕСЯЧНЫЙ ДОХОД	МЕСЯЧНЫЙ РАСХОД
23	М	349-404-255-82	Январь	80 000	20 000
35	Ж	898-330-120-38	Январь	150 000	60 000
64	М	217-285-342-65	Январь	35 000	10 000
23	М	349-404-255-82	Февраль	70 000	30 000
35	Ж	898-330-120-38	Февраль	160 000	50 000
64	М	898-330-120-38	Февраль	45 000	15 000

НАПРИМЕР:

Считаем одним из примеров рекомендованной практики обезличивание персональных данных для целей разработки и тестирования программного обеспечения посредством использования синтетических идентификаторов. При использовании данного метода значения идентифицирующих и косвенно идентифицирующих атрибутов заменяются на другие значения по алгоритму, неизвестному третьей стороне. Синтетические идентификаторы генерируются случайным образом, однако, с целью сохранения бизнес-логики создается справочник соответствия синтетических идентификаторов исходным данным.

После проведения обезличивания каждому идентифицирующему атрибуту соответствует свой синтетический идентификатор. Для обеспечения защиты данных доступ к справочнику соответствия синтетических идентификаторов исходным данным должно иметь ограниченное число лиц, изначально имеющих доступ к исходным данным. Также в указанных целях на лиц, которым передан обезличенный набор данных, рекомендуется возложить обязанность использовать указанные данные исключительно для целей разработки и тестирования программного обеспечения, а также не предпринимать какие-либо меры для восстановления исходных данных.

По завершении использования тестовой среды, содержащей обезличенные по настоящей методике данные, подобная тестовая среда подлежит уничтожению со всеми содержащимися в ней данными. Применение данного метода может не приводить к окончательной анонимизации или псевдоанонимизации данных. Для указанных целей приведенный метод обезличивания может применяться в комбинации с иными методами.

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

ИДЕНТИФИЦИРУЮЩИЕ АТРИБУТЫ НЕ УДАЛЯЮТСЯ, А ПЕРЕНОСЯТСЯ В СПРАВОЧНИК СООТВЕТСТВИЯ

КАЖДОМУ ИДЕНТИФИЦИРУЮЩЕМУ АТРИБУТУ СООТВЕТСТВУЕТ СВОЙ СИНТЕТИЧЕСКИЙ ИДЕНТИФИКАТОР

ДЕОБЕЗЛИЧИВАНИЕ ДАННЫХ ВОЗМОЖНО ТОЛЬКО ЛИЦОМ, ИМЕЮЩИМ ДОСТУП К ИСХОДНЫМ ДАННЫМ

ПРИ УНИЧТОЖЕНИИ СПРАВОЧНИКА СООТВЕТСТВИЯ, ОТСУТСТВУЕТ ВОЗМОЖНОСТЬ ДЕОБЕЗЛИЧИВАНИЯ

ВОЗМОЖНОСТЬ ЗАМЕНЫ ИДЕНТИФИЦИРУЮЩИХ АТРИБУТОВ ВО ВСЕХ СИСТЕМАХ ТЕСТИРОВАНИЯ НА ЕДИНЫЕ СООТВЕТСТВУЮЩИЕ ДАННЫМ АТРИБУТАМ СИНТЕТИЧЕСКИЕ ИДЕНТИФИКАТОРЫ, ЧТО ПОЗВОЛЯЕТ СОХРАНИТЬ БИЗНЕС-ЛОГИКУ В ОТСУТСТВИЕ ВОЗМОЖНОСТИ ИДЕНТИФИКАЦИИ КОНКРЕТНОГО ЛИЦА

ПРЕВЕНТИВНАЯ ДЕЯТЕЛЬНОСТЬ КОМПАНИИ, НАПРАВЛЕННАЯ НА НЕДОПУЩЕНИЕ УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ

Уровень категоризации данных является важнейшим в процессе обеспечения безопасной обработки персональных данных.

В настоящее время отсутствуют нормативные правовые акты, предписывающие автоматизировать данный процесс. В тоже время причинами большинства инцидентов в сфере информационной безопасности, связанных с персональными данными, являются действия инсайдеров, а не хакерские атаки.

Сохранение копий на рабочем столе, выгрузка записей из баз данных, хранение в папках общего доступа, скриншоты при доступе через браузер и прочее – все это типичные ситуации для любой компании.

Минимизировать эти риски можно, выявив нерегламентированный доступ, небезопасное сохранение копий персональных данных или хранение конфиденциальных данных в местах, не подходящих для этого.

НАПРИМЕР:

Считаем одним из примеров рекомендованной практики, позволяющей обеспечить защиту персональных и (или) конфиденциальных данных от несанкционированного доступа, реализацию в компании инструментов аудита не только цифровой инфраструктуры, где такие данные должны храниться, но и всех информационных объектов компании, где потенциально может осуществляться хранение или обработка данных.

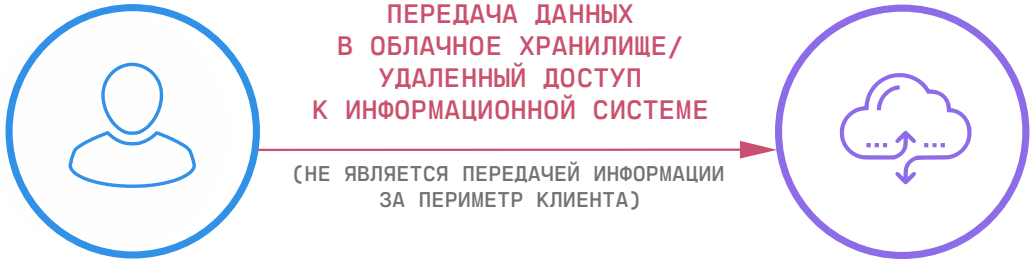
В настоящее время на рынке существует много вариантов как коммерческих, так и свободно распространяемых средств для сканирования информации в сетевых папках, базах данных, локальных компьютерах, сетевых хранилищах и облачных сервисах хранения. Потому выявление и тегирование информации конфиденциального характера, фиксация истории действий с файлами, истории изменения уровней доступа, а также выявление нарушений регламентов обработки информации доступны практически любому оператору персональных данных.

ПОЛОЖИТЕЛЬНЫЙ ЭФФЕКТ ОТ ВНЕДРЕНИЯ ПРАКТИКИ

- ВЫРАБОТКА МЕТОДИК ЗАЩИТЫ ДАННЫХ С УЧЕТОМ РЕАЛЬНЫХ РИСКОВ
- ОБЪЕКТИВНАЯ ОЦЕНКА РЕГЛАМЕНТОВ ДОСТУПА К ДАННЫМ

ПЕРЕДАЧА ДАННЫХ В ОБЛАЧНОЕ ХРАНИЛИЩЕ

Облачные сервисы – сервисы, предоставляющие возможность хранить свои файлы на удаленных серверах, а также получать к ним доступ из любой точки мира, где есть доступ в информационно-телекоммуникацию сеть «Интернет». В условиях стремительно растущих объемов хранимой и передаваемой информации данные сервисы стали популярны и востребованы пользователями.
Так, одно лицо («Облачный провайдер») предоставляет другому лицу («Клиенту») удалённый доступ через информационно-телекоммуникационную сеть к информационной системе («Облачная система») для размещения (записи) информации, определяемой Клиентом («Информация клиента»).
При этом возможна ситуация, в которой Информация клиента содержит персональные данные третьих лиц. В таком случае оператором персональных данных, помещаемых в Облачную систему, является Клиент, который сам определил цель обработки персональных данных и самостоятельно принял решение о хранении.



КЛИЕНТ–ОПЕРАТОР ПЕРСОНАЛЬНЫХ ДАННЫХ

- ОПРЕДЕЛЯЕТ ЦЕЛЬ ОБРАБОТКИ ДАННЫХ
- ПРОВОДИТ ОЦЕНКУ СООТВЕТСТВИЯ СПОСОБОВ ЗАЩИТЫ ИНФОРМАЦИИ И ПАРАМЕТРОВ ДОСТУПА ТРЕТЬИХ ЛИЦ
- САМОСТОЯТЕЛЬНО ПРИНИМАЕТ РЕШЕНИЕ О ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЛАЧНОМ ХРАНИЛИЩЕ

ОБЛАЧНЫЙ ПРОВАЙДЕР
(НЕ ЯВЛЯЕТСЯ ОПЕРАТОРОМ ПЕРСОНАЛЬНЫХ ДАННЫХ)

- ПРЕДОСТАВЛЯЕТ КЛИЕНТУ МЕСТО ДЛЯ ХРАНЕНИЯ ДАННЫХ
- ИСПОЛЬЗУЕТ СРЕДСТВА ЗАЩИТЫ ДАННЫХ
- УВЕДОМЛЯЕТ ИЛИ ПРЕДОСТАВЛЯЕТ ПО ЗАПРОСУ КЛИЕНТА ИНФОРМАЦИЮ О КОНКРЕТНЫХ СПОСОБАХ И СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАЧНОМ СЕРВИСЕ И СВЕДЕНИЙ О МЕСТЕ(СТРАНЕ) РАЗМЕЩЕНИЯ СЕРВЕРНОГО ОБОРУДОВАНИЯ

НАПРИМЕР:

Если облачный провайдер не инициирует размещение персональных данных в Облачной системе, не определяет цели их обработки, а также не выполняет поручение Клиента обработать такие персональные данные, а лишь предоставляет Клиенту место для самостоятельного хранения информации, то:
– такое размещение не считается передачей информации за периметр Клиента. Провайдер облачной системы не осуществляет обработку персональных данных Клиента, в том числе способом «хранения», и на него не распространяются требования закона ФЗ «О персональных данных» в части, предъявляемым к условиям обработки персональных данных Клиента.

Добросовестным признается поведение оператора персональных данных, при котором – в случае размещения в Облачной системе обрабатываемых им персональных данных – такое размещение происходит исходя из его оценки соответствия применяемых Облачным провайдером способов защиты информации и параметров доступа третьих лиц требованиям к хранению определенной категории персональных данных.

Облачная система может использоваться Клиентом для самостоятельного хранения в нём обрабатываемых им персональных данных, если по оценке самого Клиента, применяемые Облачным провайдером средства защиты и параметры доступа третьих лиц соответствуют требованиям, предъявляемым законом к обработки той категории персональных данных, которые пользователь планирует разместить в Облачной системе.

При этом примером рекомендованной практики добросовестного поведения считаем уведомление Облачным провайдером или предоставление по запросу Клиента информации о конкретных способах и средствах защиты информации в Облачном сервисе, сведений о месте (стране) размещения серверного оборудования для целей оказания услуг и условия предоставления доступа к информации третьих лиц

КОДЕКС ЭТИКИ
ИСПОЛЬЗОВАНИЯ
ДАННЫХ

БЕЛАЯ КНИГА | ПРИЛОЖЕНИЕ 1

1010
0101
1010

УДАЛЕННАЯ ИДЕНТИФИКАЦИЯ

Для обеспечения большей достоверности на практике используются многофакторные модели аутентификации. Лицо считается установленным, если получен положительный результат сопоставления предоставленных субъектом идентификаторов с факторами аутентификации, которыми обладает или может получить из доверенного источника (информационные системы банков, операторов связи, ГИС, «цифровой профиль гражданина» и пр.) идентифицирующее лицо.

Целесообразно использование принципа технологической нейтральности: способы идентификации должны быть равнозначными и влечь равные правовые последствия. Во-первых, в законодательстве не существует каких-либо устоявшихся и обоснованных критериев, по которым использование идентификатора может быть привязано к конкретным правоотношениям. Во-вторых, в соответствии с принципом диспозитивности и свободы участников гражданско-правовых отношений нельзя ограничивать стороны последних в использовании тех или иных идентификаторов, которые они посчитают возможным.

Цифровые способы идентификации могут использоваться в любых правоотношениях, если иное не запрещено законом или соглашением сторон.

В случаях, предусмотренных федеральными законами или принятыми в соответствии с ними иными нормативными правовыми актами, либо соглашением сторон, при дистанционном выражении воли физическим или юридическим лицом с помощью электронных или иных аналогичных средств такое физическое или юридическое лицо может быть установлено путем применения одного из идентификаторов.

Не допускается сбор избыточных персональных данных под видом идентификации, а также навязывание процедуры идентификации в сервисах, реализующих услуги/товары, необходимость в проведении которой, ввиду специфики самого сервиса и/или требований закона, отсутствует.

ОБРАБОТКА ДАННЫХ РОДСТВЕННИКОВ

Ряд федеральных законов (например, федеральный закон «О противодействии коррупции»), содержит требования о предоставлении гражданами персональных данных своих родственников в целях предотвращения коррупции, обеспечения достоверности отчетности и пр. Таким образом, информация поступает ее получателю не от самого родственника, а от третьего лица – потенциального кандидата на должность и пр.

Добросовестной практикой целесообразно считать обработку персональных данных организацией-получателем этих данных и лицом, предоставляющим сведения о родственниках, с связи с обработкой таких данных в силу исполнения ими обязанностей, предусмотренных законодательством РФ, а также в связи с обработкой персональных данных, подлежащих обязательному раскрытию или опубликованию,или обработкой персональных данных в общественном интересе.

На основании п. п. 2, 7, 11 ч. 1 ст. 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» ДОПУСТИМО не требовать от работников и иных лиц предоставления согласия субъекта персональных данных при направлении в организацию сообщений, уведомлений и т.п., содержащих данные третьих лиц, в рамках противодействия коррупции и управления конфликтом интересов.

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ С ЦЕЛЬЮ ЗАЩИТЫ СЧЕТОВ КЛИЕНТОВ

Подробное описание практики

Операторами связи разработан системный подход по предотвращению данного вида мошенничества с подменой номеров кредитных организаций. Универсальное технологическое решение предполагает интеграцию кредитных организаций по API и предоставление перечня номеров клиентов, по которым необходима нотификация по различным событиям.

Перечень событий может быть индивидуально согласован с кредитной организацией, например, нотификация по вызовам, совершенным с официальных номеров банка, вызовам с номеров, визуально похожих на номера банка, вызовам с номеров, используемых мошенниками для обзвона клиентов банка.

Операторы связи на своей стороне проводят аналитику и определяют перечень номеров, с которых совершаются мошеннические вызовы.

Дополнительно перечень номеров, требующих уведомления со стороны оператора связи, может быть предоставлен кредитной организацией.

Кредитные организацию получают в режиме реального времени (в момент вызова) по техническим каналам связи информацию о совершении звонка с номера, включенного в перечень событий.

Основываясь на полученной информации, кредитная организация по своему усмотрению принимает необходимые меры к недопущению мошеннических операций.

Использование антифрод-платформы по информированию кредитных организаций о совершении вызовов с номеров телефонов, внесенных в черный список, позволит в значительной степени снизить количество случаев мошенничества с помощью методов социальной инженерии

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ НА ФИНАНСОВОМ РЫНКЕ

Подробное описание практики

Считаем примером рекомендованной практики взаимодействие кредитных организаций и сотовых операторов в рамках прямых договоров для оперативного получения сведений, связанных с антифродовыми событиями (смена сим карты, переадресация вызова, прекращение договора абонентского обслуживания, смена пользовательского устройства и пр.).

С учетом предлагаемого в настоящее время создания единой информационной системы проверки сведений об абонентах считаем необходимым также закрепить возможность использования прямых договоров между сотовыми операторами и кредитными организациями для получения сведений по списку антифродовых событий в режиме мониторинга телефонных номеров.

Это сложившаяся практика взаимодействия банков и сотовых операторов, которую необходимо признать добросовестной. Это позволит:

1. Вывести сотовых операторов из «серой» зоны с точки зрения предоставления сведений банкам по соответствующим событиям, что позволит однозначно трактовать такое взаимодействие со стороны контрольно-надзорных органов.

2. Обеспечит банкам возможность оперативно получать сведения по номерам телефонов своих клиентов и осуществлять своевременную их защиту в случае мошеннических операций в удаленных каналах обслуживания (банковские мобильные приложения).

МЕХАНИЗМ ПОЛУЧЕНИЯ И ОБРАБОТКИ ОБРАЩЕНИЙ ЛИЦ, ОТКАЗАВШИХСЯ ОТ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ И/ИЛИ ОТ ОБРАБОТКИ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Подробное описание практики

В соответствии с законодательством Российской Федерации о рекламе продвижение товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем, допускается только при условии предварительного согласия потребителя рекламы.

Таким образом потребитель на законодательном уровне ограждается от контактов с теми компаниями на которые он предварительно не соглашался.

При этом, в ряде случаев, для осуществления прямых контактов с потребителем различные компании могут собирать и обрабатывать персональные данные такого потребителя. В этой ситуации потребитель может быть дополнительно защищен положениями законодательства Российской Федерации о персональных данных: так, по требованию субъекта персональных данных обработка оператором персональных данных должна быть немедленно прекращена.

В свою очередь, несмотря на наличие прямого возражения потребителя, в ряде случаев компании продолжают осуществлять прямые контакты с потребителем, что может, в зависимости от обстоятельств, приводить к нарушению законодательства о рекламе, а также законодательства о персональных данных.

Подобные ситуации возникают зачастую ввиду отсутствия у компании действенного механизма для получения и обработки требованийпотребителя о запрете направления ему рекламы или о прекращении обработки его персональных данных.

Считаем примером рекомендованной практики наличие у каждой компании действующего механизма получения и обработки заявлений и обращений потребителей, отказавшихся от получения рекламы или от обработки его персональных данных. В зависимости от технических и финансовых возможностей компании, такой механизм может быть реализован через соответствующее программное обеспечение, через ведение различного рода реестров (blacklists), позволяющих вести учет отказов, а также путем предоставления потребителям различных сценариев взаимодействия, упрощающих предоставление отказа (формы отказа от рассылки в самом по себе рекламном сообщении и т.п.).

Наличие такого механизма у компании позволит, во-первых, сократить случаи нарушения законодательства и прав граждан, а во-вторых,будет способствовать формированию позитивного отношения к компании и ее продуктам со стороны потребителя.

ПРЕВЕНТИВНАЯ ДЕЯТЕЛЬНОСТЬ КОМПАНИИ, НАПРАВЛЕННАЯ НА НЕДОПУЩЕНИЕ УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ (ПРИМЕРЫ РЕШЕНИЙ)

СУЩЕСТВУЕТ ДВА ПРИНЦИПИАЛЬНО РАЗНЫХ ПО СВОЕЙ СУТИ ТИПА РЕШЕНИЙ:

Ediscovery

РЕДКО СУЩЕСТВУЮТ ИЗОЛИРОВАННО ОТ DLP-СИСТЕМ,
ЯВЛЯЯСЬ ИХ СОСТАВНОЙ ЧАСТЬЮ.
ОНИ ПОЗВОЛЯЮТ СКАНИРОВАТЬ ЛОКАЛЬНЫЕ ПЕРСОНАЛЬНЫЕ
КОМПЬЮТЕРЫ ИЛИ СЕТЕВЫЕ ПАПКИ И ВЫЯВЛЯТЬ ХРАНЕНИЕ
КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В МЕСТАХ,
ДЛЯ ЭТОГО НЕ ПРЕДНАЗНАЧЕННЫХ.

DCAP-системы

ПОЗВОЛЯЮТ ПРОВОДИТЬ ПОЛНОЦЕННЫЕ РАССЛЕДОВАНИЯ
(ОТКУДА ИНФОРМАЦИЯ ПОЯВИЛАСЬ,
КЕМ РЕДАКТИРОВАЛАСЬ, КАК ИМЕННО ИЗМЕНЯЛАСЬ,
КТО СЕЙЧАС ИМЕЕТ К НЕЙ ДОСТУП И КТО
ИЗ АДМИНИСТРАТОРОВ ЕГО ПРЕДОСТАВИЛ),
МОГУТ ИМЕТЬ БЛОКИРУЮЩИЕ ФУНКЦИИ
(ИЗМЕНИТЬ УРОВЕНЬ ДОСТУПА, УДАЛИТЬ,
ЗАШИФРОВАТЬ КОНФИДЕНЦИАЛЬНОЕ СОДЕРЖИМОЕ)
И ДАЖЕ ПРОАКТИВНЫЕ ФУНКЦИИ
(ПОЗВОЛЯЮТ МОДЕЛИРОВАТЬ ПОТЕНЦИАЛЬНЫЕ
УГРОЗЫ ДЛЯ ТОЙ ИЛИ ИНОЙ НАСТРОЙКИ ДОСТУПА)
ОДНАКО DCAP-СИСТЕМЫ ЗАЧАСТУЮ ПРОИГРЫВАЮТ
ПО КАЧЕСТВУ КОНТЕНТНОГО АНАЛИЗА СИСТЕМАМ EDISCOVERY

ТАКИМ ОБРАЗОМ, К ВЫБОРУ ПРИКЛАДНЫХ ИНСТРУМЕНТОВ СТОИТ ПОДХОДИТЬ ОТВЕТСТВЕННО,
ЗАРАНЕЕ ОПРЕДЕЛИВ КРИТИЧНЫЙ ПУЛ ЗАДАЧ КОМПАНИИ И ОТТАЛКИВАТЬСЯ
ИМЕННО ОТ НИХ, А НЕ ОТ ВОЗМОЖНОСТЕЙ ПРЕДЛАГАЕМЫХ РЕШЕНИЙ

КОДЕКС ЭТИКИ
ИСПОЛЬЗОВАНИЯ
ДАННЫХ

БЕЛАЯ КНИГА

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ДЛЯ КЕЙСА ПО УДАЛЕННОЙ ИДЕНТИФИКАЦИИ

1010
0101
1010

БАНКОВСКИЙ ID

В настоящее время есть потребность в использовании банковской идентификации с использованием банковского идентификатора гражданина (Банк ID) и предоставление сведений о нем, полученных банком в результате ранее проведенной идентификации в соответствии с ФЗ-115 (ПОД/ФТ), третьему лицу с согласия гражданина. В частности, в ряде банков существует сервис идентификации Банк ID, который может быть использован третьими лицами (компаниями) на основе коммерческих соглашений между банком и этими лицами для идентификации физических лиц, являющихся клиентами банка.

В качестве рекомендованной практики предлагаем рассмотреть в первую очередь возможность использования банковского идентификатора (Банк ID) для удаленной идентификации физических лиц в компаниях, не являющихся субъектами ФЗ-115 (ПОД/ФТ), в рамках коммерческих соглашений между компаниями и банками.

В результате такой идентификации компания, использующая сервис банковской идентификации, будет получать идентификационные сведения о физическом лице – клиенте банка (ФИО, паспортные данные, дата рождения, СНИЛС, ИНН, телефон), предоставленные банком с согласия этого клиента, выраженного банку.

В рамках реализации этой практики необходимо обеспечить актуализацию соответствующих сведений о физическом лице в банке с учетом их возможного изменения. Актуализация сведений возможна с использованием ЕСИА как государственного источника достоверных и актуальных данных о гражданине с учетом реализации концепции «цифрового профиля», предполагающей автоматическое обновление данных гражданина из соответствующих ГИСов.

В развитие – дополнительно к сервису удаленной идентификации, предоставляемой банками, может быть использована биометрическая идентификация клиента, если банк, предоставляющий такой сервис (использование Банк ID для удаленной идентификации), имеет и хранит биометрические эталоны по своим клиентам.

МОБИЛЬНЫЙ ID

1. Мобильный ID – сервис быстрого входа и регистрации, работающий на базе технологии SIM-пушей. Он позволяет пользователю гибко управлять собственными данными и самостоятельно определять, какую информацию предоставлять интернет-компаниям. Каждая авторизация подкрепляется разъяснениями о составе передаваемых данных и подтверждается согласием пользователя. Личный кабинет Мобильного ID при этом хранит статистику выданных согласий и состав переданных данных.

2. На наш взгляд, сервис Мобильный ID позволяет операторам персональных данных в полной мере исполнить обязанность обеспечить точность, достаточность, актуальность персональных данных следующим образом. Мобильный ID позволяет пользователям создавать цифровые профили.
Пользователь может перенести свои абонентские данные в цифровой профиль, предоставив соответствующее поручение сервису. Также пользователь может давать сервису Мобильный ID поручение на предоставление данных из цифрового профиля определённому сервис-провайдеру (владельцу интернет-сайта, приложения для смартфона, видеоигры и т.д.), а в случае, если пользователь обнаруживает некорректные или неактуальные данные, он может заменить их в ручном режиме. В случае такого изменения все сервис-провайдеры, которые ранее предоставляли услуги пользователю Мобильного ID, могут быть уведомлены о таких изменениях.

3. На наш взгляд, получение подтверждения в сервисе Мобильный ID является достаточным для подтверждения получения согласия и для установления факта предоставления доступа неограниченному кругу лиц к персональным данным самим субъектом. Сервис Мобильный ID предоставляет сервис-провайдерам возможность получить авторизованное пользователем подтверждение совершения каких-либо действий в его сервисе. Для этого сервис-провайдер инициирует направление пользователю push-сообщения посредством сервиса, в момент совершения пользователем юридически значимых действий, например, выражения согласия с политикой обработки персональных данных. Информация о том, какие действия подтверждал пользователь, сохраняется у сервис-провайдера посредством log-файлов, информация о факте подтверждения пользователем своих действий или операции сохраняется сервисом Мобильный ID и передаётся сервис-провайдеру. Т.к. использование сервиса Мобильный ID неразрывно связано с услугами связи, то личность каждого пользователя ранее была установлена оператором связи в установленном законом порядке. Сервис Мобильный ID может сравнить данные, предоставленные оператору связи об абоненте-владельце номера и данные, предоставленные пользователем сервис-провайдеру при наличии согласия пользователя на обработку его персональных данных в целях такой верификации.

МОБИЛЬНЫЙ ID

4. Информация о соответствии (или о несоответствии) личности пользователя и реального субъекта персональных данных передаётся сервис-провайдеру и в случае необходимости может быть использована им в подтверждение правомерности обработки данных без необходимости запрашивать и получать дополнительные документы у субъекта персональных данных.

5. Технология Mobile ID как один из видов цифровых идентификаторов используется за рубежом. Цифровой идентификатор Mobile ID может применяться в следующих целях:

– упрощение процедуры совершения платежей в электронной форме (электронная коммерция), так как предполагает быстроту входа в сервис и автоматическое заполнение необходимых форм регистрации;

– подтверждение и обеспечение безопасности электронных транзакций в банках и платежных системах: вход в мобильный банк, подтверждение транзакций, анти-фрод (защита учетной записи, идентификация личности);

– обеспечение безопасности и быстрота использования ряда электронных сервисов, в частности, при покупке электронных билетов и регистрации в схемах лояльности транспортных компаний;

– взаимодействие лиц с государственными органами: вход на интернет-порталы государственных услуг, коммуникация с пользователями, обмен документами, здравоохранение и проч.

Мобильный телефон и SIM-карты также могут быть использованы при совершении авторизованных юридически значимых действий (мобильная электронная подпись).

ДВУХФАКТОРНАЯ ИДЕНТИФИКАЦИЯ (АУТЕНТИФИКАЦИЯ)

Этап 1 (Рассмотрение заявки на заключение договора)

Физическое лицо имеет возможность отправить на рассмотрение заявку на заключение договора с указанием своих паспортных данных и иной информации исключительно после предоставления соответствующих согласий:

- согласие на обработку ПД для рассмотрения его заявки;
- согласие на применение АСП (Аналога собственноручной подписи).

Согласие подписывается с помощью SMS (клиент на свой абонентский номер получает уникальный код, вводя который в форму сайта, совершает подписание согласия).

Этап 2 (Заключение кредитного договора)

Договор подписывается с помощью SMS (клиент на свой абонентский номер получает уникальный код, вводя который в формусайта, совершает подписание согласия).

Этап 3 – Опциональный (Обмен бумажными документами)