indeed id

Система централизованного управления учетными данными и доступом пользователей

Обзор

« Сокращение риска несанкционированного доступа к информационным ресурсам кредитной организации с помощью управления доступом и учетными данными »

Подготовлено специалистами Компании Индид

2012

Введение

Деятельность современного банка во многом сводится к управлению финансовой информацией: движение денег и обязательств на счетах, расчёты между кредитными организациями, торговля на валютном и других финансовых рынках.

Эта финансовая информация создаётся, хранится, изменяется и контролируется со всё более нарастающим участием информационных систем.

Однако новые технологии, при всей их неоспоримой полезности, приносят в банковскую деятельность и новые риски. А в ряде случаев происходит трансформация старых рисков в новые, иногда более масштабные. Таким новым риском является несанкционированный доступ (НСД) к информационным системам и информации [1]принадлежащей кредитной организации.

Наше исследование посвящено анализу данного риска и роли систем централизованного управления учетными данными и доступом (IAM[2]) в его минимизации.

Несанкционированный доступ и несанкционированные действия

Основная часть рисков, при использовании информационных систем, для кредитной организации возникает вследствие несанкционированных действий с финансовой информацией банка, данные действия являются в первую очередь следствием получения лицом проводящим такие операции несанкционированного доступа к информационным ресурсам и системам.

Несанкционированными действиями чаще всего являются проведение законченных банковских операций[3], а также хищение информации или изменение ее в нужную злоумышленнику сторону.

Хотя речь идёт, в первую очередь, о рисках связанных с преднамеренными действиями, не стоит упускать из вида и непреднамеренные ошибки в работе сотрудников. Такие действия также могут привести к несанкционированному изменению информации, а следовательно причинить ущерб[4] крединой организации.

Таким образом, необходимо построить систему информационной безопасности банка (СИБ[5]) так, чтобы минимизировать возможность несанкционированного доступа тем самым сократить вероятность несанкционированных действий как со стороны злоумышленников так и со стороны сотрудников организации совершающих непреднамеренные, опасные для информационной безопасности действия.

Вопрос *"Как сократить риск несанкционированного доступа?"* является ключевым в данном исследовании. Для ответа на него, мы во первых, рассмотрим типовые ситуации, в которых происходит несанкционированный доступ, и защитные меры[6] для его пресечения. После этого, мы опишем существующие инструменты реализующие указанные защитные меры. Далее последует детальный анализ роли каждого инструмента в снижении риска и механизма его работы.

Сценарий угрозы	Защитная мера
Лицо использует для несанкционированного доступа и действий права, которыми обладает другое лицо.	Недопущение проникновения в информационную систему банка лиц, выдающих себя за правомочных пользователей. Применение мер препятствующих передаче аутентификаторов от одного пользователя к другому. Быстрый отзыв скомпрометированных аутентификаторов.
Лицо использует для несанкционированного доступа и действий права, которыми оно не должно обладать. *Например, сотрудник уже уволен, но его пароль всё ещё действует. Или сотрудник переведён в другой отдел, но у него всё ещё остались права с прежнего рабочего места.*	Увеличение степени соответствия между тем, что правомочному пользователю разрешено делать в информационной системе банка, и тем, что он реально может там делать в данный момент. Рассогласование между первым и вторым может возникать, как в случае изменения позиции сотрудника, так и в случае изменений в самой инфосфере банка: — Любые изменения в позиции сотрудника, влекущие изменения в его правах, должны как можно быстрее отражаться на его реальных правах в компьютерной системе. — Внедрение новых информационных систем, а также изменение старых, может приводить к необходимости серьёзной перестройки прав пользователей, что без должной централизации и контроля, ухудшает указанное соответствие. Для достижения этого соответствия у IT-подразделения банка должны быть инструменты, позволяющие изменять права сотрудников быстро и при этом контролируемо. Повышение производительности этого процесса важно ещё и с другой стороны: крайне желательно свести к минимуму количество IT-администраторов, имеющих права изменять права сотрудников. Всё это касается и аутентификаторов, выдаваемых пользователю, как впервые, так и взамен скомпрометированных. Также упрощение данных процедур позволяет производить выдачу прав не только IT-специалистам, а, например, сотруднику из отдела кадров или отдела безопасности, что, в свою очередь, ещё больше усилит указанное в данном пункте соответствие.
Лицо использует для несанкционированнного доступа и действий свои настоящие права.	Более тонкая настройка прав пользователей. В том числе введение новых прав, изначально не предусмотренных информационной системой (приложением и т.п.). Расширенный аудит и возможность быстрого отзыва прав. То есть минимизация ущёрба за счёт быстрого выяснения и пресечения несанкционированных действий.
Несанкционированное действие уже случилось или длится.	Расширенный аудит и возможность быстрого отзыва прав. То есть минимизация ущёрба за счёт быстрого выяснения и пресечения несанкционированных действий.

Роль систем централизованного управления доступом пользователей к информационным ресурсам и их учетными данными

Для реализации указанных мер противодействия несанкционированному доступу и действиям в арсенале систем класса IAM существуют и используются следующие инструменты:

- Современная многофакторная аутентификация пользователя, значительно снижающая вероятность доступа в информационную систему неправомочного лица, а также затрудняющая передачу аутентификаторов другим лицам.
- Система по управлению учётными записями пользователей (IdM[7]), упрощающая и ускоряющая выдачу и отзыв прав пользователя, повышающая контроль над ними, а также за счёт большей автоматизации позволяющая без ущерба для эффективности более тонкую настройку прав пользователя.
- Единая точка доступа (SSO[8]) во все информационные системы, к которым подключён пользователь, консолидирующая контроль действий пользователя, упрощающая процедуры аутентификации для пользователя, а также в целом снижающая возможность компрометации аутентификаторов пользователя.
- Введение новых прав, изначально не предусмотренных информационной системой. Например, когда сумма операции превышает некое пороговое значение, пользователю необходимо пройти повторную или дополнительную аутентификацию. Другими словами, два пользователя могут иметь одинаковое право создавать платёжные поручения, но только один из них сможет создавать платёжные поручения больше некоторой суммы.
- Расширенный аудит, повышающий отслеживаемость несанкционированных действий, как в реальном времени, так и пост-фактум. Это достигается за счёт централизации контроля действий пользователя, а также более подробного описания этих действий (вплоть до имени IT-администратора, выдавшего данные права данному сотруднику). То есть осуществляется не только аудит доступа (использования прав), но и аудит выдачи и изменения прав.

Далее мы рассмотрим данные инструменты более подробно, отдельно отмечая влияние каждого инструмента и практики на снижение операционных рисков в деятельности финансового института.

Аутентификация[9]

Для доказательства своей личности пользователь использует один или несколько аутентификаторов. Наиболее известный аутентификатор - это пароль. Также, это может быть карта доступа, отпечаток пальца и многое другое. Всего в отрасли активно используется более двадцати видов аутентификаторов.

Одним из важных элементов усиления системы аутентификации является так называемая многофакторная аутентификация, позволяющая значительно снизить вероятность прохождения аутентификации лицом, не являющимся настоящим пользователем.

Многофакторной аутентификацией является одновременное использование аутентификаторов из разных, групп аутентификаторов:

- то что пользователь знает (например, пароль, пин-код)
- то чем пользователь владеет (например, банковская карта, карта доступа)
- то что является неотемлемой характеристикой пользователя (например, отпечаток пальца)
- то где пользователь находится (используя, например, данные из СКУД[10])

Подходы к аутентификации	Как это снижает риски?
Многофакторная аутентификация. *Например, пароль и карта, или пароль и отпечаток пальца.*	Увеличивает для злоумышленника сложность прохождения процедуры аутентификации, так как необходимо провести атаку на разнородные системы аутентификации.
Сокращение количества аутентификаторов, которые необходимо знать/обладать пользователю. *Достигается путём применения SSO.* *Также стоит рассмотреть и вариант введения единой карты доступа, как для СКУД, так и для доступа в компьютерную систему.*	Снижает риск компрометации аутентификаторов. *Например, пользователь может запомнить один пароль, или следить за сохранностью одной карты доступа. Если паролей много, то пользователь будет просто вынужден куда-то их записать, тем самым увеличивая вероятность их компрометации.*
Упрощение процедуры аутентификации для пользователя. *Достигается с помощью SSO.* *Также, например, приложить палец к сканеру проще, чем ввести пароль. Кроме того, пароль надо ещё помнить, а карту доступа хранить.*	Упрощает для пользователя следование политикам безопасности. Снижает вероятность их нарушения.
Быстрый отзыв и перевыпуск аутентификаторов в случае компрометации.	Быстрое пресечение несанкционированного доступа.

Система управления учетными записями (IdM)

Сотрудник банка может иметь доступ одновременно к нескольким информационным системам банка (приложения, базы данных, веб-сайты и т.д.). IdM позволяет с помощью коннекторов к этим системам автоматически создавать и изменять учётные записи в них из центральной консоли, а также изменять права пользователя в них. Это минимизирует операционные риски следующим образом:

Что делает IdM?	Как это снижает риски?
Ускорение создания, изменения и удаления учётных записей пользователя, а также изменения прав пользователя.	Повышение степени соответствия между реальными правами пользователя и теми, которыми он должен обладать.
Упрощение создания, изменения и удаления учётных записей пользователя, а также изменения прав пользователя.	Возможность более точной настройки прав пользователя. Уменьшение количества IT-сотрудников, имеющих права изменять права пользователей. Возможность сотрудникам, например, из отдела кадров или отдела безопасности, не являющихся IT-специалистами, создавать учётные записи, изменять права пользователей, а также контролировать данный процесс.
Централизация создания, изменения и удаления учётных записей пользователя, а также изменения прав пользователя.	Повышение эффективности контроля за учётными записями, правами пользователей и их изменениями.
Быстрый отзыв прав пользователя вплоть до удаления его учётной записи.	Быстрое пресечение несанкционированного действия.

Единая точка доступа (SSO)

Если IdM централизирует и автоматизирует управления учётными записями и правами пользователей, то SSO добавляет к этому централизацию доступа пользователей ко всем информационным системам.

Таким образом доступ пользователей к приложениям проходит не напрямую в конкретное приложение, а через агента SSO. Пользователь аутентифицируется один раз в агенте SSO, после чего агент SSO сам аутентифицирует пользователя в необходимых информационных системах. Причём пользователь знает только свой аутентификатор в агенте SSO (например, пароль), но не знает свои пароли в конкретных информационных системах, к которым он получает доступ через агента SSO.

Что делает SSO?	Как это снижает риски?
Доступ к любой информационной системе проходит через сервер SSO и регистрируется в его журнале. Дополнительная, аутентификация критичных действий пользователей в информационных системах.	Повышает уровень контроля за действиями пользователей, как в реальном времени, так и пост-фактум.
Централизация выдачи, отзыва и перевыпуска в случае компрометации аутентификаторов.	Быстрое пресечение несанкционированного доступа. Быстрый перевыпуск аутентификаторов.
Аутентификация проводится один раз.	Пользователю достаточно безопасно хранить один аутентификатор. Например, один пароль проще запомнить, чем десять. То есть это снижает вероятность компрометации аутентификатора.
Автоматическое, регулярное изменение паролей пользователя в целевых системах.	Гарантирует исполнение регламентов информационной безопасности в части регулярного изменения паролей.
Применение надежных методов шифрования аутентификационной информации, интеграция с PKI	Обеспечивает защищенность хранимой информации. В случае использования PKI, доступ гарантируется только обладателю закрытого ключа владельца данных.
Стандартизация процедуры аутентификации.	Возможность поддержания единой корпоративной политики по отношению к аутентификации, например, единые требования к сложности пароля, или введение единой карты доступа. Пользователь привыкает к единой стандартной процедуре аутентификации, и любые отклонения от неё (например, в случае попытки фишинга со стороны злоумышленника) вызывают у пользователя обоснованные подозрения.

Расширенный аудит

Инструменты из арсенала IAM, которые мы описали выше, значительно расширяют возможности аудита, как действий пользователя, так и изменений его прав.[11] Это в значительной степени упрощает осуществление контроля за соблюдением принципов управления операционными рисками и выявлением факторов такого риска в части организации работы информационных систем кредитных организаций.

В отдельных случаях, подробное журналирование действий пользователей компонентами IAM может использоваться не только для целей аудита и предотвращения возможных утечек информации, но и как доказательная база при проведении расследований инцидентов связанных с инцидентами в области информационной безопасности.

Инструмент IAM	Как это расширяет аудит?
Система по управлению учётными записями (IdM).	Создание, изменение и удаление учётных записей пользователя, а также изменения прав пользователя, регистрируются в едином журнале. Также в нём регистрируется, кто и когда осуществлял создание, изменение и удаление учётных записей, а также менял права пользователей.
Единая точка доступа (SSO).	Доступ к любой информационной системе проходит через сервер SSO и также регистрируется в едином журнале.
Аутентификация.	Интеграция со СКУД позволяет регистрировать в едином журнале дополнительный фактор – местоположение сотрудника.
IAM в целом.	Наличие центральной консоли и единого журнала позволяет сотрудникам, не являющихся IT-специалистами, например, из отдела безопасности, оперативно анализировать текущую ситуацию.

Заключение

Как видно из детального рассмотрения инструментов и практик IAM, выполненного нами выше, использование этих инструментов и практик, ключевыми из которых являются:

- многофакторная и строгая аутентификациия пользователей,
- использование единой точки доступа к информационным системам,
- управления учетными данными пользователей,

в значительной степени снижают возможность несанкционированного доступа и несанкционированных действий при использовании информационных систем, тем самым повышают общий уровень информационной безопасности кредитной организации.

В связи с этим можно сделать вывод о том что:

- внедряя инструменты и практики IAM, финансовая организация добивается значительного сокращения рисков возникновения ущерба от инцидентов информационной безопасности;[12]
- инструменты IAM являются важной частью инфраструктуры обеспечивающей информационную безопасность современного банка.[13] [14] [15]

Перечисленные нами в обзоре инструменты IAM дополняют и усиливают друг друга, и применение их в комплексе приносит наибольший положительный эффект. Однако, практика внедрения и эксплуатации подобных систем показала, что путь поэтапного внедрения является оптимальным.

Так же стоит отметить, что реализацию каждого этапа внедрения инструментов IAM следует проводить имея выработанную стратегию действий, а одной из первых задач является сокращение источников учетных записей пользователей используемых организаций до минимума и аудит всех существующих учетных записей.

При подготовке обзора использовались следующие документы:

"Рекомендации по организации управления операционным риском в кредитных организациях" - Приложение к письму Банка России от 24 мая 2005 г. № 76-Т "Об организации управления операционным риском в кредитных организациях".

Стандарт Банка России СТО БР ИББС-1.0-2010 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения".

Sound Practices for the Management and Supervision of Operational Risk. February 2003. Basel Committee on Banking Supervision.

Minimizing the Risk of Internal Fraud in Challenging Times. May 2009. Datamonitor.

Magic Quadrant for Enterprise Single Sign-On. September 2009. Gregg Kreizman. Gartner Research.

Identity Management Market Forecast 2007 To 2014. Andras Cser and Jonathan Penn. February 2008. Forrester research.

Enterprise Single Sign-On: The Fast Lane To Identity And Access Management. Andras Cser. November, 2010. Forrester research.

Комментарии

[1] Информационный актив (в терминах СТО БР ИББС): Информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации банковской системы Российской Федерации; находящаяся в распоряжении организации банковской системы Российской Федерации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

[2] Identity and Access Management

[3] Главной целью злоумышленника является получение контроля над информационными активами на уровне бизнес процессов. Прямое нападение на уровне бизнес–процессов, например, путем раскрытия конфиденциальной банковской аналитической информации, более эффективно для злоумышленника и опаснее для собственника, чем нападение, осуществляемое через нижние уровни, требующее специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективное по соотношению "затраты / получаемый результат" (СТО БР ИББС, пункт 6.4)

[4] Ущерб: Утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации банковской системы Российской Федерации, наступивший в результате реализации угроз ИБ через уязвимости ИБ. (СТО БР ИББС, пункт 3.45.)

[5] Система информационной безопасности (в терминах СТО БР ИББС): Совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

[6] Защитная мера: Сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ организации банковской системы Российской Федерации. (СТО БР ИББС, пункт 3.42.)

[7] Identity Management

[8] Single Sign-On

[9] Аутентификация (в терминах СТО БР ИББС): Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

[10] Система контроля и управления физическим доступом

[11] Должны быть документально определены и выполняться процедуры сбора и хранения информации о действиях работников организации БС РФ, событиях и параметрах, имеющих отношение к функционированию защитных мер. (СТО БР ИББС, пункт 8.12.3.)

[12] Инцидент информационной безопасности; инцидент ИБ (в терминах СТО БР ИББС): Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

Угроза информационной безопасности; угроза ИБ (в терминах СТО БР ИББС): Угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организации банковской системы Российской Федерации.

[13] В составе АБС должны применяться встроенные защитные меры, а также рекомендуются к использованию сертифицированные или разрешенные руководством организации БС РФ к применению средства защиты информации от НСД и НРД. (СТО БР ИББС, пункт 7.4.2.)

[14] В организации БС РФ должны быть документально определены и утверждены руководством, выполняться и контролироваться процедуры идентификации, аутентификации, авторизации; управления доступом; контроля целостности; регистрации событий и действий. (СТО БР ИББС, пункт 7.4.3.)

[15] В организации БС РФ должны применяться защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и (или) авторизации клиентов и работников организации БС РФ. Все попытки НСД и НРД к такой информации должны регистрироваться. При увольнении или изменении должностных обязанностей работников организации БС РФ, имевших доступ к указанной информации, необходимо выполнить документированные процедуры соответствующего пересмотра прав доступа. (СТО БР ИББС, пункт 7.4.11.)