Концепция информационной безопасности

1. Цель Политики

ПАО «Совкомбанк» (далее по тексту – Банк, Совкомбанк) для целей осуществления своих основных видов деятельности и поддержания своих бизнес-процессов на регулярной основе обрабатывает информацию ограниченного доступа, содержащую сведения, относящиеся к банковской тайне, коммерческой тайне, персональным данным и к платежной информации. Банк обязуется сохранять конфиденциальность, целостность и доступность обрабатываемой информации.

Настоящая Концепция информационной безопасности (далее по тексту – Концепция) является политикой, которая отражает систему взглядов на цели, задачи, принципы и основные механизмы обеспечения информационной безопасности в Банке.

Концепция является общедоступным документом и размещена в открытом доступе на веб-сайте sovcombank.ru.

2. Область применения

Концепция применяется при использовании информации, информационных систем, электронно-вычислительных устройств, приложений и сетевых сервисов (далее по тексту – информационные активы), используемых для ведения банковского бизнеса.

Действие настоящей Концепции распространяется на деятельность всех сотрудников Банка.

Концепция рекомендована для соблюдения компаниями, входящими в Банковскую группу ПАО «Совкомбанк» (далее – Группа) в части, не противоречащей требованиям применимого законодательства. Компаниям Группы рекомендовано утвердить свои Концепции информационной безопасности или руководствоваться положениями настоящей Концепции.

3. Ответственность

Подразделение информационной безопасности отвечает за разработку и поддержание Концепции в актуальном состоянии.

Подразделение информационной безопасности несет ответственность за реализацию настоящей Концепции и вправе привлекать другие структурные подразделения и руководство Банка в целях надлежащей реализации Концепции.

Наблюдательный совет Банка осуществляет контроль за реализацией Концепции.

4. Соблюдение

Соблюдение положений Концепции обязательно для сотрудников Совкомбанка. Нарушение требований настоящей Концепции может повлечь дисциплинарную, административную и/или уголовную ответственность в соответствии с действующим законодательством Российской Федерации и локальными нормативными документами банка.

5. Цели информационной безопасности

Целями Банка в области обеспечения информационной безопасности являются:

- поддержание стратегии развития Банка посредством защиты банковской тайны, персональных данных и коммерческой тайны;
- соблюдение требований российского законодательства и нормативных документов, регламентирующих порядок обработки и защиты банковской тайны, персональных данных и коммерческой тайны;
- создание процесса управления рисками информационной безопасности;
- управление выявленными рисками информационной безопасности на приемлемом уровне посредством разработки и внедрения планов минимизации рисков;
- повышение уровня осведомленности всего персонала по вопросам обеспечения информационной безопасности;
- установление ответственности за обеспечение и управление информационной безопасности в Банке.

6. Обеспечение информационной безопасности

Организация информационной безопасности

В Банке разработаны, поддерживаются и внедряются политики, процедуры и стандарты обеспечения информационной безопасности для защиты конфиденциальности, целостности и доступности своих информационных активов.

Управление доступом

Доступ к информационным системам Банка контролируется на протяжении всего жизненного цикла учетной записи: от первоначальной идентификации и аутентификации пользователя до предоставления, изменения и блокировки прав доступа. Права доступа для учетных записей пользователей в информационных системах предоставляются с использованием принципа минимальных привилегий и периодически пересматриваются. Пароли соответствуют требованиям политики Банка к их сложности и периодически меняются.

Для аутентификации пользователей с привилегированными правами доступа применяются механизмы двухфакторной аутентификации.

Управление активами

В Банке определена схема классификации информационных систем для реализации последовательного подхода к управлению рисками информационной безопасности, обеспечению непрерывности бизнеса и аварийному восстановлению информационных активов.

Непрерывность бизнеса и аварийное восстановление

Банк защищает критически важные информационные активы от последствий серьезных сбоев или аварий путем разработки и реализации планов обеспечения непрерывности и восстановления деятельности. Мы обеспечиваем резервное копирование критически важных данных и стремимся к предотвращению сбоев, обеспечению своевременного восстановления критичных данных после сбоев, а также к поддержанию выполнения критически важных бизнес-процессов во время сбоев, сохраняя при этом конфиденциальность информации.

Управление коммуникациями и сетевой безопасностью

Для обеспечения эффективного управления коммуникациями и сетевой безопасностью в Банке внедрены различные системы и сервисы защиты сетевой инфраструктуры, такие как: межсетевые экраны, системы предотвращения и обнаружения вторжения, системы и сервисы защиты от атак типа отказа в обслуживании (DDoS) и средства контроля и защиты доступа к беспроводным сетям и в сеть Интернет, а также реализована сегментация сети для того, чтобы Банк защищал свои информационные активы от их компрометации как со стороны внешних, так и со стороны внутренних нарушителей.

Системы предотвращения и обнаружения вторжения

Системы предотвращения и обнаружения вторжения развернуты в Банке на уровне сетевой инфраструктуры и на уровне конечных пользовательских устройств. Безопасность сетевой инфраструктуры находится под круглосуточным мониторингом.

Защита инфраструктуры беспроводных сетей

Инфраструктура беспроводных сетей в наших офисах защищена с помощью механизмов контроля доступа, аутентификации, шифрования и контроля появления несанкционированных точек доступа.

Защита от атак типа отказа в обслуживании

Защита от DDoS-атак строится в Банке по принципу эшелонированной защиты:

•

- защита от атак типа DDoS на пограничных устройствах поставщика услуг Интернет;
- использование внешних провайдеров защиты от DDoS-атак;
- использование внутренних систем предотвращения DDoS-атак в Банке.

Защита доступа в Интернет

Сотрудникам Банка предоставляется доступ в Интернет только для исполнения своих должностных обязанностей. Фильтрация доступа осуществляется в соответствии с установленными в Банке правилами. Дополнительные доступы предоставляются только по согласованию с руководством и подразделением информационной безопасности.

Безопасность рабочих станций и ноутбуков

Безопасность корпоративных рабочих станции и ноутбуки сотрудников в Банке обеспечивается, но не ограничивается, за счет применения следующих средств защиты:
- средства антивирусной защиты, встроенного в рабочие сборки операционных систем по умолчанию и настроенного на регулярное сканирование и получение актуальных обновлений антивирусных баз;
- средств шифрования дисков на корпоративных ноутбуках сотрудников;
- средств блокировки записи данных на съемные носители информации;
- средств удаленного подключения сотрудников к корпоративной сети с многофакторной аутентификацией.

Соблюдение нормативных требований

Банк соблюдает применимые требования российского законодательства по информационной безопасности, а также следует рекомендациям совета безопасности индустрии платежных карт PCI Security Standards Council.

Криптографическое управление

В Банке применяются криптографические средства защиты информации для поддержания конфиденциальности информации, обеспечения проверки целостности и электронных подписей. Требования к алгоритмам шифрования и длине ключей при хранении, передаче по каналам связи и использовании информации, определены в порядке криптографической защите информации.

Управление инцидентами информационной безопасности

В рамках управления инцидентами информационной безопасности Банк проводит следующие работы:
- осуществляет координирование инцидентов информационной безопасности;
- осуществляет своевременное расследование инцидентов информационной безопасности;
-

- оценивает риск, связанный с инцидентом информационной безопасности;
- внедряет корректирующие защитные меры в целях минимизации риска от инцидента информационной безопасности;
- обеспечивает заполнение внутренних уведомлений и отчетов.

Управление рисками информационной безопасности

Банк управляет рисками информационной безопасности по всем процессам обеспечения защиты информации. Оценка рисков проводится на регулярной основе и для различных активов: процессы, технологии, информационные системы, люди, информация. Регулярный процесс оценки рисков информационной безопасности проводится для решения следующих задач:
- идентификация всех информационных, программных и физических активов;
- выявление угроз и уязвимостей информационной безопасности;
- количественная оценка риска информационной безопасности;
- обработка риска информационной безопасности для выделения средств на минимизацию факторов, представляющих наибольший риск;
- внедрение средств и технологий защиты информации в областях, обеспечивающих максимальное снижение рисков для персональных данных, банковской и коммерческой тайны клиентов.

Регистрация и мониторинг событий

В банке внедрены требования к регистрации событий, процессу мониторинга и анализу активностей сотрудников в инфраструктуре и информационных системах банка. Совкомбанк соблюдает все применимые требования к регистрации и мониторингу событий.

Управление изменениями

Все изменения в информационной инфраструктуре банка производятся в соответствии с внедренными процессами управления изменениями, управления конфигурациями, а также процессами управления техническими ресурсами.

Физическая безопасность и безопасность окружающей среды

Совкомбанк применяет защитные меры для предотвращения несанкционированного доступа в свои офисы, а также обеспечивает физическую защиту информационных активов от возможных природных стихийных угроз.

Меры, применяемые Банком, включают, но не ограничиваются:
- системы контроля доступа;
- системы видеонаблюдения;
- системы охранной и пожарной сигнализации;
- сейфы и специализированные шкафы.

Безопасное управление жизненным циклом прикладных систем

Совкомбанк разрабатывает и внедряет стандарты безопасной разработки и настройки прикладных систем, а также проводит анализ защищенности исходных кодов и прикладных систем на всех этапах их жизненного цикла, чтобы гарантировать выявление и своевременное устранение и/или минимизацию рисков информационной безопасности.

Управление уязвимостями и обновлениями

На регулярной основе Банк проводит анализ уязвимостей своей информационной инфраструктуры и обеспечивает установку обновлений безопасности программного обеспечения. Управление и контроль исправления уязвимостей в инфраструктуре Банка осуществляется за счет регулярного (еженедельного) взаимодействия между бизнес-подразделениями, подразделениями информационных технологий и информационной безопасности Банка. Еженедельный статус установки обновлений безопасности программного обеспечения измеряется и контролируется.

Защита от утечек информации

Предотвращение утечек информации осуществляется за счет регулярного мониторинга каналов утечки информации, применения технических средств контроля, организационных мер защиты и обучения работников Банка.

Каналы контроля включают в себя, но не ограничиваются:
- исходящую электронную почту;
- передачу и загрузку файлов в Интернет;
- корпоративные мессенджеры;
- печать документов.

Банк контролирует утечку данных, чтобы предотвратить риски кражи, а также случайной передачи или преднамеренного раскрытия банковской тайны и/или персональных данных клиентов.

Обучение сотрудников и тренинги

В Банке внедрена программа повышения осведомленности сотрудников по вопросам информационной безопасности. Для достижения наиболее эффективного результата Банк использует такие каналы повышения осведомленности сотрудников как: курсы и анимированные ролики на корпоративном портале, вводное обучение новых сотрудников и ежегодное обязательное обучение по вопросам информационной безопасности для всех сотрудников Банка.

Анализ защищенности

Внутренний и внешний анализ защищенности инфраструктуры Банка проводиться на регулярной основе нашей собственной командой.

Кроме того, может быть заказан внешний анализ защищенности инфраструктуры банка специалистами вендора для обеспечения дополнительной уверенности в эффективности применяемых методов и средств защиты информации.

Информационная безопасность вендоров/партнеров.

В Банке выстроен процесс для проведения первоначальной и постоянной комплексной проверки вендоров/партнеров, которые заключают официальные деловые соглашения с Банком. Каждый вендор/партнер, которому планируется предоставить доступ к защищаемой информации, подписывает с Банком соглашение о неразглашении и/или соглашение о конфиденциальности.

7. Куда обращаться?

По вопросам и жалобам в области информационной безопасности следует обращаться в службу технической поддержки или отдел информационной безопасности (e-mail: oib@sovcombank.ru).

Необходимо также сообщить по вышеперечисленным каналам в случае, если:

- пароль сотрудника стал известен другим лицам;
- сотрудник получил подозрительное сообщение по электронной почте;
- компьютер странно работает.

2021