Политика информационной безопасности Дочерней организации Акционерного общества Банк ВТБ (Казахстан)

В Дочерней организации Акционерное общество Банк ВТБ (Казахстан) (далее – Банк) разработана и утверждена Советом директоров Банка Политика информационной безопасности (далее – Политика), которая определяет подходы, принципы, правила в построении эффективной системы управления информационной безопасностью (далее – ИБ) в Банке, а также определяет органы и подразделения Банка, ответственные за реализацию положений Политики.

Политика разработана в соответствии с действующим законодательством Республики Казахстан, требованиями Агентства Республики Казахстан по регулированию и развитию финансового рынка и Национального Банка Республики Казахстан, а также внутренними документами Банка.

Политика определяет:

1) цели, задачи и основные принципы построения системы управления ИБ;
2) область действия системы управления ИБ;
3) требования к управлению доступом к создаваемой, хранимой и обрабатываемой информации в информационных активах Банка;
4) требования к осуществлению мониторинга деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ;
5) требования к осуществлению сбора, консолидации и хранения информации об инцидентах ИБ;
6) требования к проведению анализа информации об инцидентах ИБ;
7) ответственность работников Банка за обеспечение ИБ при исполнении возложенных на них функциональных обязанностей.

Цели, задачи и основные принципы построения системы управления ИБ

Основными целями управления ИБ в Банке являются построение эффективной системы управления ИБ (далее – СУИБ), соответствующей внешней операционной среде, стратегии Банка, организационной структуре Банка, объему активов, характеру и уровню сложности операций Банка, направленной на минимизацию рисков ИБ, а также цели, предусмотренным Политикой.

Основной задачей СУИБ является минимизация рисков ИБ, которым подвержены технологии и автоматизированная информационная система (далее – АИС), используемые Банком для достижения бизнес-целей, а также обеспечение эффективности мероприятий по ликвидации неблагоприятных последствий реализации угроз ИБ и потенциальных инцидентов.

В целях обеспечения надлежащего уровня СУИБ, ее развития и улучшения, Банком достигается ряд основных целей:

1) реализация мер по защите информационных активов от угроз ИБ;
2) оптимизация стоимости владения средствами защиты информации;

3) предотвращение и/или снижение до приемлемого уровня ущерба от реализации актуальных угроз ИБ;
4) соблюдение законодательных, нормативных и договорных требований в области ИБ;
5) повышение стабильности функционирования Банка в условиях возможной реализации угроз ИБ;
6) контроль состояния СУИБ Банка и постоянное ее совершенствование;
7) непрерывный мониторинг и реагирование на инциденты ИБ, включая процесс киберразведки;
8) обучение и повышение квалификации работников для оперативного реагирования на инциденты ИБ;
9) участие в проведении единой стратегии развития участников Группы ВТБ в части ИБ, внедрение прозрачных унифицированных процессов контроля, обеспечения и управления ИБ;
10) повышение эффективности и качества взаимодействия с Головным банком по вопросам ИБ.

Основополагающие принципы построения системы управления ИБ

В целях достижения максимальной эффективности СУИБ Банк руководствуется следующими основными принципами:

1) **Неотъемлемость** - безопасность АИС является их неотъемлемым свойством (характеристикой), а не дополнительным сервисом;

2) **Комплексность** - необходимо согласованное применение разнородных средств при построении целостной системы защиты информации, перекрывающей все каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;

3) **Системность** - деятельность по защите информации должна быть строго и всесторонне регламентирована;

4) **Непрерывность** - защита информации не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем Банка, начиная с самых ранних стадий их проектирования, а не только на этапе эксплуатации;

5) **Адекватность** - применяемые методы и средства защиты информации должны быть адекватны угрозам ее уничтожения, утечке или искажения;

6) **Идентификация и оценка активов** - реализация принципа «Адекватность» должна основываться на идентификации всех информационных активов и определении их ценности для целей и задач Банка;

7) **Гибкость и управляемость** - системы защиты должны обеспечивать возможность варьировать уровень защищенности АИС;

8) **Своевременность** - разработка подсистем ИБ должна вестись одновременно с разработкой защищаемой системы;

9) **Упреждение** - акцент в работе системы обеспечения ИБ должен ставится на предотвращении (предупредительных мерах) событий ИБ, которые могут повлиять на целостность, доступность и конфиденциальность информации;

10) **Контролируемость** - обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации;

11) **Законность** - деятельность по защите информации должна осуществляться в строгом соответствии с действующим законодательством, требованиями надзорных и контролирующих органов, нормативными актами в области защиты информации;

12) **Следование лучшим практикам** - при реализации мер по обеспечению ИБ рекомендуется учитывать требования Группы ВТБ, отечественных и международных стандартов в области ИБ как лучших практик;

13) **Анализ и совершенствование** - необходима постоянная работа по оценке эффективности и совершенствованию мер и средств защиты информации на основе анализа функционирования информационных систем, изменений в методах и средствах перехвата информации и воздействия на компоненты систем, изменений нормативных требований по защите, отечественного и зарубежного опыта в области защиты информации;

14) **Минимизация полномочий** - предоставление пользователям прав доступа определяется исключительно производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, в каком это необходимо работнику и третьим лицам для выполнения его должностных/договорных обязанностей;

15) **Разделение функций -** при определении состава ролей, использующихся для распределения прав доступа, запрещается совмещение в рамках одной роли такого состава функций (концентрации полномочий), которое позволило бы одному работнику единолично осуществлять выполнение критичных операций или получать полный и неконтролируемый доступ к какой-либо системе Банка;

16) **Персонификация** - действия всех работников Банка должны осуществляться от имени персонифицированной учетной записи. Наличие учетных записей, не закрепленных за конкретным работником, не допустимо;

17) **Запрещено все, что не разрешено** - доступ к любому объекту информационной системы должен предоставляться только при наличии соответствующего разрешения (правила), зафиксированного в проектной документации, регламенте бизнес-процесса и настройках средств защиты информации. Любой, неразрешенный явно, доступ должен быть запрещен;

18) **Простота применения защитных мер и средств** - используемые средства защиты должны быть интуитивно понятны и просты в использовании. Их применение не должно быть связано со значительными дополнительными трудозатратами при обычной работе пользователей (работники и клиенты) информационных систем;

19) **Стойкость средств защиты** - уровень стойкости применяемых средств и эффективность мер защиты информации должны определяться ценностью защищаемого объекта и требовать от злоумышленника неадекватно больших затрат времени и вычислительных мощностей на их преодоление;

20) **Эшелонированность средств защиты** - нельзя полагаться на единственный защитный рубеж, каким бы надежным он не считался. Помимо средств защиты периметра должны использоваться системы защиты внутренней сети, серверов, рабочих станций, баз данных и т.д.;

21) **Разнообразие средств защиты** - в целях снижения зависимости уровня безопасности в целом от поставщиков, провайдеров, компаний-партнеров, а также сбоев и отказов отдельных систем, целесообразно использовать средства различных производителей. Обязательным является использование антивирусных средств различных производителей на рабочих станциях, серверах и средствах межсетевого экранирования;

22) **Специализация и профессионализм** - к работам по разработке, внедрению, сопровождению средств и реализации мер защиты информации необходимо привлекать специализированные организации, наиболее подготовленные к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы, необходимые лицензии на право оказания услуг в этой области, обладающие партнерскими статусами компаний-вендоров внедряемых решений и имеющие в своем штате высококвалифицированных работников;

23) **Осведомленность** - осведомленность работников и клиентов в вопросах ИБ является обязательным условием безопасного функционирования систем;

24) **Персональная ответственность** - ответственность за обеспечение безопасности информации и систем ее обработки возлагается не только на Подразделение по информационной безопасности, но и на каждого работника Банка в пределах его полномочий;

25) **Лояльность персонала** - создание такой благоприятной атмосферы в коллективах всех подразделений Банка, при которой выполнение требований ИБ не воспринималось бы работниками как дополнительная нагрузка, от которой желательно избавиться, а как осознанная необходимость и неотъемлемая часть корпоративной этики;

26) **Вовлеченность руководства** - осознание руководством Банка необходимости обеспечения ИБ, непосредственное участие в принятии стратегических решений по вопросам функционирования системы обеспечения ИБ, включая вопросы принятия рисков ИБ;

27) **Взаимодействие и координация** - эффективное обеспечение ИБ достигается на основе взаимодействия и координации со всеми иными заинтересованными подразделениями Банка, подразделением ИБ Головного Банка и другими профильными министерствами, ведомствами, организациями и объединениями;

28) **Технологическая независимость -** при выборе программных и программно-аппаратных средств, в том числе средств защиты информации, учитывается наличие ограничений на возможность их применения со стороны разработчиков (производителей) или иных лиц. Средства защиты информации, должны быть обеспечены гарантийной и (или) технической поддержкой на весь период их эксплуатации.

Политика распространяется на всех работников Банка и описывает концептуальные основы и требования к организации деятельности по обеспечению ИБ, а также задаёт основные векторы их реализации по следующим направлениям:

1) идентификация информационных активов, категорирование защищаемой информации;
2) построение сетевой безопасности, включая противодействие атакам;
3) построение механизмов антифрода;
4) обеспечение контроля доступа к АИС Банка и информационным ресурсам;
5) обеспечение защиты серверов, центров обработки данных, серверных помещений;
6) обеспечение антивирусной защиты информационной инфраструктуры в порядке, определяемом Банком;
7) обеспечение защиты автоматизированных рабочих мест;
8) обеспечение ИБ на стадиях жизненного цикла прикладного программного обеспечения/ АИС Банка;
9) обеспечение ИБ при осуществлении деятельности в виртуальной среде;
10) обеспечение защиты систем управления базами данных;
11) обеспечение/осуществление контентного контроля при использовании интернета и электронной почты;
12) обеспечение защиты от воздействия вредоносного кода;
13) обеспечение криптографической защиты информации;
14) осуществление резервного копирования и хранения резервных копий;
15) повышение осведомленности работников по вопросам ИБ;
16) мониторинг ИБ и управление событиями и инцидентами ИБ;
17) управление ИБ.

Область действия СУИБ охватывает:

1) все бизнес-процессы Банка;
2) все структурные подразделения Банка;
3) все здания головного офиса и филиалов Банка.

Требования к управлению доступом к создаваемой, хранимой и обрабатываемой информации в информационных активах Банка

Требования к управлению доступом к создаваемой, хранимой и обрабатываемой информации в информационных активах Банка охватывают все стадии жизненного цикла пользовательского доступа от начальной регистрации новых пользователей до конечного снятия с регистрации пользователей, которым больше не требуется доступ к АИС и сервисам.

Работник наделяется ролью (перечнем ролей) на основании документально оформленной заявки, подписанной руководителем его структурного подразделения Банка и согласованной с владельцем бизнес-процесса.

Пользователю должны предоставляться минимально необходимые для выполнения функциональных обязанностей полномочия и при изменении должностных обязанностей или увольнении работника Банка все права должны отзываться.

Третьим лицам, которым требуется предоставление доступа к АИС Банка в соответствии с условиями договора / соглашения (техническое сопровождение оборудования, сопровождение внедрения информационных систем) должно заключаться соглашение о конфиденциальности (в том числе с партнерами).

В случае передачи третьим лицам информационных активов (размещение серверных мощностей Банка в сторонних центрах обработки данных, использование внешних сервисов обработки и/или хранения данных) Банком предпринимаются следующие меры обеспечения ИБ:

1) отражение в соответствующем соглашении / договоре с третьим лицом требований по защите информационных активов Банка и права проверки Банком исполнения таких требований, а также условий о возмещении ущерба, возникшего вследствие нарушения ИБ и работоспособности АИС;
2) исключение возможности доступа третьих лиц к информации, передача которой третьим лицам не допускается в соответствии с гражданским, банковским законодательством РК, законодательством РК о персональных данных и их защите.

Требования к осуществлению мониторинга деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ

Порядок реагирования на инциденты ИБ состоит из следующих этапов, включая, но не ограничиваясь ими:

1) мониторинг событий ИБ и выявление инцидентов ИБ (далее – этап мониторинга и выявления);
2) локализация и противодействие инциденту ИБ (далее – этап реагирования);
3) внутреннее расследование инцидента ИБ (далее – этап внутреннего расследования).

На этапе мониторинга деятельности по обеспечению ИБ осуществляются следующие мероприятия подразделением по ИБ:

1) мониторинг и анализ событий ИБ;
2) отнесение событий ИБ к инциденту ИБ в соответствии с разработанным порядком отнесения событий ИБ к инцидентам ИБ;
3) классификацию и приоритизацию инцидентов ИБ;
4) передачу информации об инциденте ИБ на этап реагирования.

На этапе реагирования на инциденты ИБ применяются стандартные процедуры реагирования, а в случаях низкой эффективности применения стандартных процедур реагирования, принимаются оперативные меры реагирования на инциденты ИБ, включающие следующие меры, но не ограничиваясь ими:

1) информирование и привлечение к процессу реагирования работников Банка, а также при необходимости третьих лиц в целях обеспечения процесса эффективного противодействия инциденту ИБ;
2) по согласованию с владельцами бизнес-процесса применение дополнительных мер контроля по частичной или полной остановке бизнес-процесса в Банке;
3) сбор данных с программно-технических средств, вовлеченных в инцидент ИБ;
4) анализ инцидента ИБ, его сдерживание и устранение его последствий;
5) ретроспективный анализ событий ИБ;
6) определение индикаторов компрометации и уязвимостей, выявленных в ходе реагирования на инциденты ИБ, и реализация корректирующих мер, направленных на недопущение аналогичного инцидента ИБ в дальнейшем;
7) принятие решения о необходимости проведения внутреннего расследования инцидента ИБ.

На этапе внутреннего расследования инцидента ИБ Банком обеспечивается:

1) привлечение к внутреннему расследованию инцидента ИБ ответственных работников и (или) подразделений Банка, вовлеченных в процесс реагирования на инциденты ИБ, а также третьих лиц;
2) сбор и анализ материалов, необходимых для проведения внутреннего расследования инцидента ИБ;
3) установление причин возникновения инцидента ИБ и порядка реализации инцидента ИБ;
4) оценка масштаба воздействия и ущерба от реализации инцидента ИБ;
5) анализ эффективности принятых мер реагирования на расследуемый инцидент ИБ;
6) подготовка заключения о результатах расследования инцидента ИБ, в котором отражается информация об инциденте ИБ, а также рекомендации по принятию корректирующих мер в целях снижения вероятности и возможного ущерба от повторной реализации инцидента ИБ.

Требования к проведению анализа информации об инцидентах ИБ

Основными целями анализа информации об инцидентах ИБ являются:

1) обеспечение полноты и точности информации об инциденте ИБ;
2) определение последствий и нанесенного ущерба;
3) определение методов атаки и контролей, способных предотвратить повторные инциденты ИБ;
4) определение действий, которые можно предпринять для полного устранения угрозы ИБ;
5) установление основной причины инцидента ИБ.

Политика обязательна к исполнению всеми работниками Банка, третьими лицами, а также доводится до сведения поставщиков сервисов, имеющих доступ к информационным активам и внутренним документам Банка, в той части, которая непосредственно взаимосвязана с Банком и их деятельностью.

Политика подлежит пересмотру в случае изменения/дополнения законодательства Республики Казахстан и/или внутренних документов Банка.