ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АКБ «Tenge Bank»

Ташкент 2022

Ташкент 2022

Глава 1. Введение

1. Настоящая Политика информационной безопасности АКБ «Tenge Bank» (далее – Политика) определяет цели и принципы обеспечения информационной безопасности, излагает основные направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих внутренних документов АКБ «Tenge Bank» (далее – Банк).

2. Нормативно-правовую основу Политики составляют положения законодательства Республики Узбекистан по вопросам использования информационных систем и информационной безопасности, а также требования международных стандартов управления информационной безопасностью.

3. Положения Политики обязательны для исполнения всеми работниками Банка, а также должны доводиться до сведения клиентов и иных третьих лиц, имеющих доступ к информационным системам и документам Банка, в той их части, которая непосредственно взаимосвязана с Банком и их деятельностью.

4. Политика охватывает все информационные системы и документы, владельцем и пользователем которых является Банк. Банк обеспечивает создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления Банка, предназначенной для управления процессом обеспечения информационной безопасности. Обеспечение информационной безопасности – одно из условий для успешного осуществления коммерческой деятельности Банка. Информация, циркулирующая в Банке, является одним из важнейших банковских активов.

5. Информационная безопасность (далее – ИБ) Банка – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, которые могут привести к материальному ущербу, нанести ущерб репутации Банка или повлечь нанесение иного ущерба Банку, его акционерам, работникам или клиентам.

6. Являясь элементом общей политики руководства Банка, ИБ основывается на требованиях бизнеса, разрабатывается и реализуется в соответствии с общими правилами управления рисками в Банке. Нарушения в данной области могут привести к серьезным последствиям, включая потерю доверия со стороны клиентов и снижению конкурентоспособности.

7. Обеспечение ИБ включает в себя применение всех доступных средств и инструментов в рамках компетенций работников Банка, направленных на защиту информации и поддерживающей ее инфраструктуры.

8. Неотъемлемой частью организации ИБ является непрерывный контроль эффективности предпринимаемых мер, определение для работников перечня недопустимых действий (бездействия), возможных последствий и ответственности.Настоящая Политика согласована с Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан (письмо № 01-19-01/191 от 01.02.2021 года)

9. Настоящая Политика согласована с Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан
(письмо № 01-19-01/191 от 01.02.2021 года)

Глава 2. Нормативные ссылки

10.Политика и система ИБ в целом основываются на следующих нормативно-правовых актах и международных стандартах (в данном разделе указаны основные нормативные акты, непосредственно влияющие на процесс создания системы ИБ Банка в целом, в то же время существует ряд документов, который либо описывает стратегические аспекты развития ИБ на государственном уровне, либо регламентирует правила по информационной защите отдельных направлений деятельности):

- Закон Республики Узбекистан от 11 декабря 2003 г., № 560-II «Об информатизации»;
- Закон Республики Узбекистан от 11 декабря 2003 года № 562–II «Об электронной цифровой подписи»;
- Закон Республики Узбекистан от 29 апреля 2004 года № 611-II «Об электронном документообороте»;
- Закон Республики Узбекистан от 30 августа 2003 г. № 530-II «О банковской тайне»;
- Закон Республики Узбекистан от 04 апреля 2006 года № ЗРУ-30 «О защите информации в автоматизированной банковской системе»;
- Закон Республики Узбекистан от 11 сентября 2014 года №374 «О коммерческой тайне»;
- Закон Республики Узбекистан от 02 июля 2019 года № №ЗРУ-547 «О персональных данных»;
- Постановление Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан»;
- Постановление Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов»;
- Постановление Кабинета Министров Республики Узбекистан от 22 ноября 2005 года № 256 «О совершенствовании нормативно-правовой базы в сфере информатизации»;

- Постановление Кабинета Министров Республики Узбекистан от 4 мая 2011 года № 126 «О мерах по внедрению и использованию единой защищенной электронной почты и системы электронного документооборота в исполнительном аппарате Кабинета Министров, органах государственного и хозяйственного управления, государственной власти на местах»;
- Постановление Кабинета Министров Республики Узбекистан от 14 июня 2013 года №170 «О дополнительных мерах по реализации Постановления Президента Республики Узбекистан от 8 июля 2011 года № ПП–1572 «О дополнительных мерах по защите национальных информационных ресурсов»;
- Постановление Кабинета Министров Республики Узбекистан от 16 октября 2015 года №295 «Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан»;
- Постановление Правления Центрального Банка Республики Узбекистан от 25 января 2020 года № 2/4 Об утверждении Положения о защите информации в автоматизированных банковских системах коммерческих банков Республики Узбекистан;
- O'z DSt ISO/IEC 13335-1:2009 Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий. (Часть1). Концепции и модели управления безопасностью информационно-коммуникационных технологий;
- O'z DSt ISO/IEC 15408-1:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
- O'z DSt ISO/IEC 15408-2:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности;
- O‘z DSt ISO/IEC 15408-3:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности;
- O‘z DSt ISO/IEC 27000:2014 «Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь»;
- O‘z DSt ISO/IEC 27001:2016 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования»;
- O‘z DSt ISO/IEC 27002:2016 «Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасности»;
- O‘z DSt ISO/IEC 27003:2014 «Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью»;
- O‘z DSt ISO/IEC 27005:2013 «Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности»;
- O‘z DSt 3388:2019 Информационная технология. Методы обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем управления информационной безопасности;

- O‘z DSt ISO/IEC 27007:2015 Информационная технология. Методы обеспечения безопасности. Руководящие указания по аудиту систем управления информационной безопасностью;
- O‘z DSt ISO/IEC 27010:2015 Информационная технология. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью при коммуникациях между отраслями и организациями;
- O‘z DSt ISO/IEC 27011:2014 «Информационная технология. Методы обеспечения безопасности. Руководящие указания по управлению информационной безопасностью в организациях телекоммуникаций»;
- O‘z DSt 3386:2019 Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы менеджмента инцидентов;
- O‘z DSt 3387:2019 Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2. Руководящие указания по планированию и подготовке к реагированию на инциденты;
- O‘z DSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации»;
- O‘z DSt 2815:2014 «Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации»;
- O‘z DSt 2816:2014 «Информационная технология. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия не декларированных возможностей»;
- O‘z DSt 2817:2014 «Информационная технология. Средства вычислительной техники. Классификация по уровню защищенности от несанкционированного доступа к информации»;
- O‘z DSt 2927:2015 «Информационная технология. Информационная безопасность. Термины и определения»;
- O‘z DSt 1047:2018 «Информационная технология. Термины и определения»;
- Методические пособия по разработке политики информационной безопасности на территории Республики Узбекистан (Приложение №10 к протоколу Республиканской комиссии по координации реализации Комплексной программы развития Национальной информационно-коммуникационной системы Республики Узбекистан на 2013-2020 годы от 23 февраля 2016 года № 7);
- «Регламент взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по реагированию и расследованию и предотвращению инцидентов информационной безопасности» (Приложение №1 и №2 к протоколу Технического совета по вопросам информационно коммуникационной безопасности Республики Узбекистан №7 от 17.11.2017 г.);
- «Требования обеспечения информационной безопасности органов государственного и хозяйственного управления, государственной власти на местах» (Приложение № 2 к протоколу Республиканской комиссии по координации реализации Комплексной программы развития национальной информационно-коммуникационной системы Республики Узбекистан на 2013- 2020 годы от 11 ноября 2017 года № 7);

Глава 3. Область применения

11. Политика ИБ распространяется на всех сотрудников Банка, включая практикантов, контрактников и внешних посетителей (клиенты, технический обслуживающий персонал и т.п.), которые по тем или иным причинам имеют легитимный доступ к ИР Банка, его клиентов и корреспондентов. Также она применяется в отношении к АРМ персонала банка, оргтехнике и другим ресурсам информационной структуры Банка.

12. Политика, информационной безопасности не распространяется на информационные системы и объекты информатизации, предназначенные для передачи, обработки, хранения сведений, содержащих государственные секреты. Защита информации, содержащая государственные секреты, обеспечивается в соответствии с Законодательством Республики Узбекистан.

Глава 4. Цели и задачи

13.Основной целью, на достижение которой направлены все положения Политики, является минимизация ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму.

14.Процесс создания надежной информационной защиты является непрерывным. В целях обеспечения достаточно надежной системы ИБ необходима постоянная регулировка ее параметров, адаптация для отражения новых угроз, исходящих из внешней и внутренней среды. Не должно существовать каких-либо препятствий при внесении изменений в стандарты, процедуры или Политику по мере возникновения такой необходимости.

В соответствии с данным положением определяются следующие этапы цикла управления ИБ (модель PDCA: Plan-Do-Check-Act):

1) Plan – Планирование (разработка) – анализ рисков, определение Политики, целей, задач, процессов, процедур, программно-аппаратных средств, относящихся к управлению рисками и совершенствованию ИБ для получения результатов в соответствии с общей стратегией и целями Банка;

2) Do – Реализация (внедрение и эксплуатация) – внедрение и эксплуатация Политики, механизмов контроля, процессов, процедур, программно-аппаратных средств;

3) Check – Проверка (мониторинг и анализ) – оценка, и там, где это применимо – измерение характеристик исполнения процессов в соответствии с Политикой, целями и практическим опытом, анализ изменения внешних и внутренних факторов, влияющих на защищенность информационных ресурсов, предоставление отчетов руководству для анализа;

4) Act – Корректировка (сопровождение и совершенствование) – принятие корректирующих и превентивных мер, основанных на результатах внутренних и внешних проверок состояния ИБ, требований со стороны руководства, иных факторов в целях обеспечения непрерывного совершенствования системы управления ИБ.

15.Построение системы управления ИБ Банка и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

1) законность – любые действия, предпринимаемые для обеспечения ИБ, осуществляются на основе действующего законодательства с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Банка;

2) ориентированность на бизнес – ИБ рассматривается как процесс поддержки основной деятельности Банка. Любые меры по обеспечению ИБ не должны повлечь за собой серьезных препятствий деятельности Банка;

3) непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Банка должны осуществляться без прерывания или остановки текущих бизнес-процессов Банка;

4) комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла на всех технологических этапах их использования во всех режимах функционирования;

5) обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем ИБ должна быть меньше размера возможного ущерба от любых видов риска;

6) приоритетность – категорирование (ранжирование) всех информационных ресурсов Банка по степени важности при оценке реальных, а также потенциальных угроз ИБ;

7) необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

8) специализация – эксплуатация технических средств и реализация мер ИБ должны осуществляться профессионально подготовленными специалистами Банка;

9) информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях ИБ и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер ИБ;

10) взаимодействие и координация – меры ИБ осуществляются на основе взаимосвязи соответствующих структурных подразделений Банка, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

11) подтверждаемость – важная документация и все записи – документы, подтверждающие исполнение требований по ИБ и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

Глава 5. Основные положения

16. ИБ состоит из трех основных компонентов:

- конфиденциальность: свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;

- целостность: свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);

- доступность: свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия.

17.Политика ИБ предусматривает обеспечение ИБ на основе использования совокупности организационных, режимных, технических, программных и других методов и средств защиты информации, а также осуществления всестороннего непрерывного контроля эффективности реализованных мер по обеспечению ИБ.

18.В процессе реализации Политики ИБ в неё могут вноситься изменения и дополнения.

Глава 6. Объекты защиты

19.Основными объектами обеспечения ИБ в Банке признаются следующие элементы:

1) информационные ресурсы банка, его клиентов и корреспондентов, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Банка к банковской и коммерческой тайне, персональным данным, финансовой информации, и любой иной информации, необходимой для обеспечения нормального функционирования Банка (далее – защищаемая информация);

2) средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;

3) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы Банка, с помощью которых производится обработка защищаемой информации;

4) процессы Банка, связанные с управлением и использованием информационных ресурсов;

5) помещения, в которых расположены средства обработки защищаемой информации;

6) рабочие помещения и кабинеты работников Банка, помещения Банка, предназначенные для ведения закрытых переговоров и совещаний;

7) персонал Банка, имеющий доступ к защищаемой информации;

8) технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

20.Список пользователей информационных систем Банка, их права и приоритеты на доступ к информации, заведен в матрицы доступов, полномочия к программным и техническим средствам предоставляются в соответствии с матрицами доступов подразделений Банка, процессы регламентированы Правилами допустимого использования информационных ресурсов Банка и Правилами управления логическим доступом к информационным ресурсам Банка.

21.Подлежащая защите информация может:

1) размещаться на бумажных носителях;

2) существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);

3) передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;

4) присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.

Глава 7. Риск и модель угроз информационной безопасности

I.Риски информационной безопасности

22. Риск ИБ – это потенциальная возможность использования уязвимостей актива или группы активов с конкретной угрозой для причинения ущерба Банку. Для управления рисками ИБ необходимы соответствующие методы определения и обработки рисков, которые могут включать расчет затрат и экономического эффекта, требования законодательных актов, интересы заинтересованных сторон и другие соответствующие данные.

23. Процесс определения рисков, принятый в Банке, включает идентификацию, сравнительную оценку риска, и назначение им приоритетов в соответствии с критериями принятия риска и важностью целей для Банка. Результаты определения рисков ИБ помогут руководству принять решения относительно управления рисками ИБ, назначения приоритетов при управлении рисками ИБ и внедрения соответствующих средств управления безопасностью для защиты от этих рисков.

24. Для оценки риска, процесс определения рисков включает систематический метод оценки величины риска (анализ риска) и процесс сравнения предполагаемого риска с соответствующими критериями риска. Определение риска должно выполняться периодически, это позволит своевременно учитывать изменения требований ИБ и возникновение рискованных ситуаций, а также произошедшие существенные изменения. Для определения риска следует использовать методы, обеспечивающие сопоставимые и воспроизводимые результаты.

25. Для эффективного определения риска ИБ четко определяется область его действия. Определение риска ИБ будет взаимосвязано с определениями рисков для других областей деятельности (при необходимости). До начала обработки рисков устанавливается критерии принятия рисков. Риск принимается, если определено, что его уровень низкий или стоимость его обработки для Банка экономически невыгодна, эти критерии документируются.

26. После определения риска для каждого идентифицированного риска должно быть принято решение об его обработке. К возможным опциям обработки рисков относятся:

- применение соответствующих средств управления для снижения рисков;
- осознанное и объективное принятие рисков, если они однозначно удовлетворяют требованиям и критериям принятия рисков Банка;
- разделение совместных рисков с другими сторонами, например, страховщиками или поставщиками.

27. После принятия решения об обработке рисков используются соответствующие средства управления, которые прежде были выбраны и внедрены. При случаях доступа сторонних организаций к информационным активам Банка и средствам обработки информации необходимого по производственным причинам, а также, в случае получения товаров и услуг от сторонних организаций, проводится анализ рисков для определения возможных последствий для безопасности информации и требований к средствам управления. Такие мероприятия следует согласовывать и определять в договорах со сторонней организацией.

28. Все действия по определению, обработке и принятию рисков, обмену информацией относительно рисков, мониторингу рисков, должны выполняться в соответствии со стандартом O'z DSt ISO/IEC 27005:2013.

II.Угрозы информационной безопасности

29. Под угрозами ИБ понимается совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности.

30. Угрозы ИБ подразделяются на:

1) случайные – стихийные бедствия (природные источники угроз – землетрясение, пожары, осадки, наводнения и т.д.), непреднамеренные ошибочные действия со стороны работников Банка, ошибки аппаратных и программных средств и т.д.;

2) преднамеренные, т.е. умышленная фальсификация или уничтожение данных, неправомерное использование данных, компьютерные преступления и т.д.

31. К числу угроз ИБ относятся (но не ограничены ими):

1) утрата информации, составляющей банковскую тайну, коммерческую тайну Банка и иную охраняемую законом информацию;

2) искажение (несанкционированная модификация, подделка) защищаемой информации;

3) утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);

4) несанкционированное использование информационных ресурсов (злоупотребления, мошенничества и т.п.);

5) недоступность информации в результате ее блокирования, отказа и сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, активного сетевого оборудования, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств, и злонамеренных действий.

32. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние ИБ Банка и его нормальное функционирование:

1) финансовые потери, связанные с утечкой, разглашением, или несанкционированной модификацией защищаемой информации;

2) финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;

3) финансовые потери, связанные с несанкционированными действиями в информационных ресурсах Банка;

4) ущерб от дезорганизации деятельности Банка, финансовые и репутационные потери, связанные с невозможностью выполнения им своих обязательств;

5) ущерб от принятия управленческих решений на основе необъективной информации;

6) ущерб от отсутствия у руководства Банка объективной информации;

7) ущерб, нанесенный репутации Банка;

8) иной вид ущерба.

Глава 8. Модель нарушителя информационной безопасности

33. Нарушители ИБ классифицируются следующим образом:

1) внутренние нарушители – работники Банка, неосознанно либо злонамеренно нарушающие режим ИБ;

2) внешние нарушители – лица, не связанные с Банком трудовыми отношениями (в том числе стажеры и практиканты), из хулиганских или корыстных побуждений предпринимающие действия, способные нанести ущерб информационным ресурсам Банка.

34.Опасность нарушителя во многом определяется количеством и степенью важности доступных ему информационных ресурсов. Исходя из этого, наиболее рисковыми категориями следует считать менеджеров высшего и среднего звена, администраторов информационных ресурсов и лиц, работающих с большими объемами клиентской и финансовой информации.

35. Основные типы внутренних нарушителей:

1) «необученный/халатный работник» – работник Банка, по незнанию или по собственной халатности допускающий нарушение, не несущее в себе злого умысла;

2) «конкурирующий работник» – работник Банка, по личной неприязни либо по иным причинам пытающийся нанести ущерб другому работнику. В результате его действий может пострадать не только его «цель», но и в целом Банк;

3) «заинтересованный нарушитель» – работник Банка, который заинтересован в неправомерных действиях по отношению к Банку третьей стороной либо собственной выгодой. Как правило, заинтересован в дальнейшем сохранении с Банком трудовых отношений и не будет предпринимать действий, прямо его компрометирующих. Наиболее вероятное нарушение – утечка информации (в случае заинтересованности собственной выгодой – финансовые мошенничества);

4) «внедренный злоумышленник» – работник Банка, поступивший на работу с целью совершения противоправных действий в интересах третьих лиц. Практически не заинтересован в дальнейших трудовых отношениях с Банком;

5) «увольняющийся работник» – работник, прекращающий с Банком трудовые отношения без взаимных претензий. Наиболее вероятна утечка информации, к которой он имел непосредственный доступ;

6) «обиженный работник» – работник Банка, неудовлетворенный условиями трудовой деятельности, либо, как вариант, руководство Банка явно недовольно деятельностью работника. Возможны любые, даже самые нелогичные нарушения, особенно в момент расторжения трудовых отношений.

36. Основные типы внешних нарушителей (в данном разделе используется терминология, принятая на настоящий момент в сообществе специалистов по ИБ):

1)«Script Kiddie», или «Начинающий» – лицо, интересующееся взломом любого информационного ресурса, имеющего общеизвестные уязвимости. Не нацелен на взлом информационных ресурсов именно Банка, легко прекращает атаку в случае обнаружения серьезных средств защиты. Как правило, использует широко распространенные методы взлома, не разрабатывает собственных средств;

2)«Black hat» – «Черный хакер» – в отличие от «Script Kiddie» более упорен во взломе конкретного ресурса, обход систем защиты считает «делом чести», может разрабатывать простые атакующие средства. Действует с целью самоутверждения или для извлечения личной выгоды, может продавать свои услуги криминальным структурам;

3)«Elite hacker», или «Гуру» – высококлассный специалист по взлому информационных систем. Как правило, работает «под заказ» криминальных структур либо конкурирующих организаций. В первом случае будет нацелен на проведение финансового мошенничества, во втором – либо на утечку информации, либо на недоступность серверов и компрометацию Банка в глазах клиентов. В арсенале имеет полный спектр специального программно-технического обеспечения, а также использует методы социальной инженерии;

4)«Партнер» – работник организации-партнера, имеющих доступ к информационным системам Банка. Можно определить любым типом внутреннего нарушителя, но он, как правило, менее управляем и менее осведомлен о требованиях ИБ, принятых в Банке;

5)«Консультант» – работник сервисной компании, который имеет доступ к информационным ресурсам. Возможны разные сценарии проявления несанкционированной деятельности, как правило, в рамках обслуживаемой информационной системы;

6)«Стажер/практикант» – как правило, ограничен в доступе к информации и информационным системам, однако постоянно находится на территории Банка и может получать информацию косвенно либо методами социальной инженерии. Может нанести серьезный ущерб только при халатном отношении к своим обязанностям работника Банка, курирующего данного стажера/практиканта;

7)«Клиент» – клиент Банка, имеющий доступ к его сервисам дистанционного банковского обслуживания. Может нанести урон при неправильном использовании данных сервисов, утере идентификационных данных либо действовать как первые три типа внешних нарушителей, имея – пусть и ограниченный – доступ к информационным банковским ресурсам.

Глава 9. Меры информационной безопасности

37. Основными мерами по обеспечению ИБ Банка являются:

1) административно-правовые и организационные меры;

2) меры физической безопасности;

3) программно-технические меры.

38. Административно-правовые и организационные меры включают (но не ограничены ими):

1) контроль исполнения требований законодательства РУз и внутренних документов;

2) разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;

3) контроль соответствия бизнес-процессов требованиям Политики;

4) информирование и обучение работников Банка работе с информационными ресурсами и требованиям ИБ;

5) реагирование на инциденты, локализацию и минимизацию последствий;

6) анализ новых рисков ИБ;

7) отслеживание и улучшение морально-делового климата в коллективе;

8) определение действий при возникновении чрезвычайных ситуаций;

9) проведение профилактических мер при приеме на работу и увольнении работников Банка;

10) организация и обеспечение системой поддержания заданных параметров температуры и влажности;

11) обеспечение системой видеонаблюдения;

12) морально-этические (психологические) меры.

39. Меры физической безопасности включают (но не ограничены ими):

1) организацию пропускного и внутриобъектового режимов;

2) построение периметра безопасности защищаемых объектов;

3) организацию круглосуточной охраны режимных объектов, в том числе с использованием технических средств безопасности;

4) организацию противопожарной безопасности охраняемых объектов;

5) контроль доступа работников Банка в помещения ограниченного доступа.

40. Программно-технические меры включают (но не ограничены ими):

1) использование лицензионного программного обеспечения и сертифицированных средств защиты информации;

2) использование средств защиты периметра (firewall, Intrusion Prevention System (IPS) и т.п.);

3) применение комплексной антивирусной защиты;

4) использование средств ИБ, встроенных в информационные системы;

5) использование специальных комплексов ИБ (как защита электронных информационных ресурсов, так и защита от утечки по электромагнитным и акустическим каналам);

6) обеспечение регулярного резервного копирования информации;

7) контроль за правами и действиями пользователей, в первую очередь привилегированных;

8) применение систем криптографической защиты информации;

9) обеспечение безотказной работы аппаратных средств;

10) мониторинг состояния критичных элементов информационной системы.

Благодарим Вас за ознакомление с Политикой информационной безопасности АКБ «Tenge Bank»