ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «ПИРЕУС БАНК МКБ»

2021

Содержание

1. Политика информационной безопасности

1.1. Вступление

Политика информационной безопасности АО ПИРЕУС БАНК МКБ (далее – "Политика") является нормативным документом, который формулирует и отоб позицию АО «ПИРЕУС БАНК МКБ» (далее – Банк) в области информационной безопасности. Политика описывает основные принципы, описанные Руководством Банка, определяющие построение структуры информационной безопасности.

Банковская информация является важным активом Банка. Вся банковская информация подлежит защите в соответствии с ее ценностью, и в способ, который укреепляет доверие клиентов, обеспечивает соответствие регулятивным нормам и защищает конкурентоспособность Банка.

В этом документе описываются общие векторы развития информационной безопасности и принципы, описанные Руководством, которые используются для управления информационной безопасностью Банка для достижения целей бизнес-стратегии Банка. Другие более специфические политики, процедуры, стандарты, инструкции, регламенты и т.д. разрабатываются с учетом требований данной Политики.

1.2. Область применения

Требования Политики информационной безопасности распространяются на процессы Банка, его информационные системы, инфраструктуру и являются обязательными для выполнения всеми работниками Банка, а также распространяются на взаимоотношения с поставщиками, провайдерами и партнерами, услуги которых связаны с использованием, обработкой или доступом к информации или информационным активам Банка, обрабатывающих или использующих банковскую информацию в своей деятельности.

Любые случаи несоблюдения Политики информационной безопасности подлежат расследованию. В случае выявления нарушений к виновным применяются меры в соответсвии с трабованиями действующего законодательства Украины.

1.3. Термины и определения

Банк – АО «ПИРЕУС БАНК МКБ»

Банковская (корпоративная) информация – совокупность информации (в электронной, письменной или устной форме), которая обрабатывается в Банке, а также используется для поддержки процессов Банка. Информация, которая создается третьими лицами от имени Банка и информация, на которую Банк владаеет авторскими правами, также относится к банковской информации.

Информационная система – комбинация аппаратного, программного обеспечения и данных, обеспечивающая функционирование процессов Банка.

Владелец информации – подразделение Банка, которое отвечает за процесс, в котором производится обработка информации. Владелец информации несет ответственность за соблюдение

требований информационной безопасности и определяет порядок использования информации в процессе.

Информационная безопасность (ИБ) – совокупность процессов и мер, направленных на обеспечение целостности, конфиденциальности, доступности и наблюдательности информации.

Доступность – свойство доступности информации или информационного актива, которая определяет возможность использования информации или информационной системы по требованию авторизованного объекта в минимально необходимом объеме.

Конфиденциальность – свойство информации (или информационного актива), которая заключается в том, что доступ к ней не может быть получен неавторизованным лицом, объектом и/или процессом, вследствие административных/правовых ограничений, наложенных его владельцем.

Целостность – свойство информации (или информационного актива), которая заключается в невозможности ее модификации несанкционированно, без разрешения/известия ее владельца.

Наблюдательность – свойство системы, позволяющей фиксировать деятельность пользователей и процессов, а также однозначно устанавливать идентификаторы причастных к определенным событиям пользователей и процессов с целью предотвращения нарушения политики безопасности и/или обеспечения ответственности за определенные действия.

Система управления информационной безопасностью (СУИБ) – часть общей системы управления Банка, основанная на подходе оценки рисков, предназначенная для создания, внедрения, эксплуатации, контроля, анализа, поддержки и улучшения информационной безопасности Банка.

Критические информационные активы (критическая информация) – совокупность информации, в письменном или электронном виде, которая представляет ценность для Банка и/или его клиентов, а также несанкционированное или неконтролируемое разглашение или потеря которой может нанести ущерб Банку или клиентам. Критичность информации определяется исходя из уровней ее классификации относительно конфиденциальности, целостности и доступности.

Руководство Банка (руководство) – Председатель и Члены Правления Банка, Председатель и Члены Наблюдательного Совета.

1.4. Нормативные ссылки

Данная Политика разработана с учетом требований:

- Национальных стандартов Украины по ИБ:
  - ДСТУ ISO/IEC 27000:2015 “Информационные технологии. Методы защиты. Система управления информационной сохранностью. Обзор и словарь”;
  - ДСТУ ISO/IEC 27001:2015 “Информационные технологии. Методы защиты. Системы управления информационной сохранностью. Требования”;
  - ДСТУ ISO/IEC 27002:2015 “Информационные технологии. Методы защиты. Свод практик по мерам информационной безопасности”;
- Постановления Правления НБУ №95 от 28.09.2017 года «Об утверждении Положения об организации мероприятий по обеспечению информационной безопасности в банковской системе Украины»;
- Постановления Правления НБУ №4 от 16.01.2021 г. «Об утверждении Положения об осуществлении контроля за соблюдением банками требований законодательства по

вопросам информационной безопасности, киберзащиты и электронных доверительных услуг»;

- Рекомендации и правила, принятые в рамках Группы ПИРЕУС.

1.5. Цели, задачи и направления

Цель Политики это внедрение, поддержка и постоянное совершенствование СУИБ, которая должна обеспечивать необходимый уровень информационной безопасности в условиях штатного функционирования и в условиях реализации угроз, защиту информации и ресурсов Банка от внешних и внутренних угроз и угроз, связанных с умышленными и непреднамеренными действиями работников Банка. Также общей целью Банка является защищенность информации.

Цели, задачи и направления Политики информационной безопасности Банка :

- Поддержка задач Банка посредством обеспечения конфиденциальности, целостности и доступности банковской информации и информационных систем/инфраструктуры;
- Уменьшение риска нарушения конфиденциальности, целостности и доступности банковской информации путем определения правил использования банковской информации и информационных систем;
- Распространение информации об общих правилах информационной безопасности среди персонала Банка и представителей третьих лиц, которая определяет обязанности, ответственность и роль каждого работника;
- Обеспечение соответствия нормам регулятора и контрактным обязательствам;
- Обеспечение защиты деловой репутации и имиджа Банка;
- Обеспечение масштабирования процессов Банка и укрепление доверия клиентов к продуктам и услугам Банка, создавая таким путем конкурентные преимущества;
- Управление информационной безопасностью, в частности определение ролей и обязанностей в области ИБ;
- Классификация информационных активов;
- Проведение оценки рисков ИБ;
- Обеспечение безопасности информационных активов в соответствии с категорией их классификации и оценкой рисков;
- Мониторинг событий ИБ и управление инцидентами ИБ;
- Обеспечение непрерывности деятельности Банка в части, касающейся ИБ;
- Организация и контроль обеспечения безопасного управления жизненным циклом информационных систем Банка.

1.6. Основные требования, правила, принципы, роли и ответственность обеспечения ИБ.

Принципы и правила:

- Публичные сервисы и внутренние сети Банка должны отвечать требованиям стандартов ИБ;

- Для уменьшения рисков возникновения инцидентов ИБ руководство Банка должно создать всем работникам Банка условия для систематического обучения нормам и мерам ИБ;
- В Банке создаются, действуют, систематически тестируются и обновляются Планы бесперебойного функционирования деятельности Банка на случай непредвиденных (критических) ситуаций;
- Работники Банка и представители третьих лиц, которые имеют доступ к информации и/или инфраструктуре Банка, принимают участие в поддержании соответствующего уровня ИБ в пределах своих должностных обязанностей и полномочий и несут ответственность за его нарушения в пределах, установленных действующим законодательством Украины и внутренними нормативными документами Банка

Банк применяет следующие меры по обеспечению ИБ:

- Определен перечень критических процессов, информационных ресурсов (активов), обеспечивающих их функционирование, и мер, необходимых для их надлежащей защиты;
- Создан и утвержден перечень сведений, составляющих банковскую тайну;
- Проведена оценка критичности информационных активов;
- Определены правила доступа к информационным ресурсам и программно-техническим комплексам;
- Организован контроль физического и логического доступа ко всем имеющимся ресурсам;
- Реализована антивирусная защита информационных ресурсов;
- Обеспечена защита сети и защита удаленного доступа к ресурсам сети (локальной, ссетям других организацийОрганизована идентификация и аутентификация всех определенных ресурсов;
- Реализована криптографическая защита информации;
- Банк разрабатывает требования по информационной безопасности для третьих сторон, предоставляющих Банку услуги по аутсорсингу, разработке, внедрению, аудиту информационных систем и ресурсов, а также получают от Банка информацию с ограниченным доступом. Эти требования, ответственность и контроль за их выполнением вышеупомянутыми третьими сторонами определяются в соглашениях (договорах) с этими сторонами.

Роли и ответственность:

- Эффективность ИБ Банка достигается путем полноценного участия работников всех подразделений на всех этапах деятельности;
- Каждый работник Банка или третьей стороны, который имеет доступ к информации и/или инфраструктуре Банка, обеспечивает поддержание соответствующего уровняь информационной безопасности;
- В пределах своих функциональных обязанностей и полномочий работники выполняют и отвечают за выполнение требований Политики, законодательных, регуляторных и внутрибанковских норм и несут ответственность за их нарушение согласно действующему законодательству Украины и внутрибанковским нормативным документам;

- В Банке создан и постоянно работает специальный Руководящий орган по вопросам внедрения и функционирования СУИБ (далее – "Руководящий орган СУИБ"), решения и наставления которого обязательны для выполнения всеми работниками Банка;
- Руководящий орган СУИБ обеспечивает процесс разработки, внедрения, функционирования, мониторинга, пересмотра, поддержки и совершенствования СУИБ;
- На руководящий орган СУИБ возложены задачи по определению задач информационной безопасности, их соответствия требованиям действующего законодательства Украины, в частности, нормативно-правовым актам Национального банка Украины, нормативным документам Банка, а также их интегрированности в процессы и банковские продукты;
- Руководящий орган СУИБ утверждает и пересматривает Политику ИБ, анализирует эффективность ее реализации и осуществляет контроль за деятельностью любого подразделения Главного офиса и отделений Банка по выполнению требований нормативно-правовых актов НБУ и нормативных документов Банка по вопросам информационной безопасности путем инициирования перед Председателем Правления Банка проведение проверок подразделений Главного офиса и отделений Банка по внедрению и функционированию СУИБ, выполнению решений Руководящего органа СУИБ. Постоянный контроль внедрения, выполнения, усовершенствования и поддержки Политики в актуальном состоянии возложен на Руководящий орган СУИБ;
- Для уменьшения рисков возникновения инцидентов информационной безопасности Руководство Банка создает работникам условия для систематического обучения нормам и мерам информационной безопасности.

2. Общие положения информационной безопасности.

Следование требованиям Руководства Банка к управлению информационной безопасностью очевидны и понятны всем работникам Банка. Стратегия развития информационной безопасности отражает цель Руководства Банка по построению надежной системы информационной безопасности. С этой целью Руководство Банка утверждает политики безопасности, процедуры, стандарты и нормы и обеспечивает их соблюдение.

Этот документ определяет роль Руководства Банка в соттвествиим стребваниями информационной безопасности. Общие принципы информационной безопасности определяют основные необходимые действия и мероприятия, выполнение которых является обязательным условием построения защищенного рабочего процесса. Такие принципы – это краткие характеристики положений Политики информационной безопасности, которые обязательно соблюдаются всеми работниками Банка, а также другими лицами, которые имеют доступ к банковской информации или информационным системам.

Общие положения возникают из потребностей информационной безопасности Банка, определяемых путем оценки рисков в информационных системах, изучением международных стандартов по вопросам информационной безопасности и национальных регулятивных норм.

Общие положения устанавливают минимальный уровень безопасности, определенный Руководством Банка, который относится ко всем работникам Банка и третьим лицам, имеющим

доступ к банковской информации или информационным системам. Общие положения свидетельствуют о важности и необходимости защиты банковской информации.

Все решения в соотвествии с требованиями информационной безопасности и безопасности информационных систем принимаются с учетом положений, описанных в настоящем документе, как минимальные требования к информационной безопасности.

Общие положения информационной безопасности, применяемые в каждой организации, делятся на базовые и функциональные положения.

2.1. Базовые положения

Базовые положения представляют собой общие директивы, которые используются для установления и поддержания приемлемого уровня информационной безопасности Банка в общем. Базовые положения являются основой определения функциональных принципов.

2.1.1. Ответственным лицом за информационную безопасность Банка (Chief information security officer, CISO) является Председатель Правления Банка (или лицо, исполняющее его полномочия) и обеспечивает:

- стратегическое руководство по вопросам информационной безопасности Банка;
- определение направлений развития информационной безопасности Банка, их соответствие стратегии развития Банка;
- соответствие мер безопасности информации потребностям процессов/банковских продуктов;
- контроль за внедрением мер безопасности информации в Банке.

2.1.2. Подчиненность и/или подотчетность дает возможность проверки действий сторон, привлеченных к обработке информации, и обеспечивает, что действия пользователя (работника или работника третьей стороны) однозначно могут определять такого пользователя. Роли и ответственность определяются в соответствии с критичностью информации.

2.1.3. Ответственность за контроль выполнения требований Политики и своевременной осведомленности по вопросам информационной безопасности подчиненных работников, несут их руководители по соответствующему направлению работы. Каждый работник обязан обеспечивать поддержание соответствующего уровня информационной сохранности. В пределах своих функциональных обязанностей и полномочий работники должны выполнять и отвечать за выполнение требований Политики и нормативных документов, утвержденных в Банке.

2.1.4. Все правила и методы, применяемые для обеспечения приемлемого уровня информационной безопасности в Банке, не противоречат установленным социально-этическим нормам.

2.1.5. Уровень информационной безопасности достигается благодаря общим действиям владельцев информации, пользователей информационных систем, администраторов информационных систем и специалистов по информационной безопасности. Решения принимаются

после детального рассмотрения и обсуждения и оценки всех задействованных подразделений Банка для достижения наивысшего уровня информационной безопасности.

2.1.6. Механизмы безопасности и контроля, применяемые к каждому информационному активу, пропорциональны ценности такого актива, угрозам, которые могут повлиять на этот актив и потерям, которые могут быть получены в случае нарушения информационной безопасности этого актива.

2.1.7. Внедрение принципа целостности – применение механизмов, внедрение политик, процедур и стандартов как целостной системы информационной безопасности помогает достичь более эффективной безопасности, а также снижение стоимости и сложности системы.

2.1.8. Создание порядка реагирования на инциденты. При возникновении инцидента по информационной безопасности персонал Банка своевременно и скоординированно реагирует в соответствии с утвержденными процедурами обработки инцидентов информационной безопасности. Уменьшение или предупреждение будущих угроз достигается за счет своевременного использования соответствующих административных и технических средств безопасности.

2.1.9. В связи с развитием информационных технологий и потребностей бизнеса в Банке растет количество угроз и уязвимостей информации и информационных систем, что требует периодической переоценки положения. Переоценка помогает определить отклонения в отношении внедренных механизмов и средств безопасности и контроля, а также избыточный риск. Управление рисками является достаточно важной задачей для Банка так же, как и вопрос принятия решений о принятии риска или снижение уровня риска до приемлемого.

2.1.10. Политика информационной безопасности и контроль безопасности, используемые в Банке, учитывают и не нарушают права сторон, задействованных в обработке информации.

2.2. Функциональные принципы

Функциональные принципы производны и определяются из базовых положений. Они покрывают специфические тематические области (политики, процедуры, стандарты, инструкции и т.п. по информационной безопасности) и определяют области применения системы управления информационной безопасностью Банка.

2.2.1. Соблюдение Политики информационной безопасности

Все работники Банка должны понимать необходимость защиты банковской информации, информационных систем и инфраструктуры и соблюдают все требования, определенные в политиках, процедурах, технических стандартах и методиках по информационной безопасности. Персонал Банка и представители третьих сторон, которые имеют доступ к банковской информации или информационным системам, должны быть ознакомлены с Политикой информационной безопасности.

2.2.2. Назначение владельца информации

Для всех видов банковской информации должен быть определен ее владелец, который несет ответственность за ее функции. Владелец информации также ответственен за защиту информации, даже если ответственность за обработку информации была передана другой, более специализированной стороне или если владелец разрешил предоставление доступа к информации третьей стороне.

2.2.3. Классификация и защита информации

Вся банковская информация должна быть классифицирована в соответствии с установленной схемой классификации. Отнесение информации к определенному классу осуществляется владельцем информации в соответствии с ее конфиденциальностью, целостностью и доступностью. Более того, информация защищается соответствующим образом при ее хранении, обработке и передаче. Классификация информации подразумевает, что информация используется и защищается должным образом.

2.2.4. Организационная структура системы информационной безопасности

Для достижения приемлемого уровня безопасности необходимо тесное взаимодействие всех подразделений Банка. С этой целью, задачи безопасности (роли, задачи, ответственности), равно как и критические процедуры, должны четко определяться для всего Банка для достижения однозначности и взаимопонимания при выборе и применении административных и технических механизмов безопасности.

Для решения вопросов управления системой информационной безопасности в Банке создан Руководящий орган по вопросам ИБ, в состав которого входят представители подразделений, которые являются собственниками и участниками критических процессов, специалисты по информационной безопасности и, по необходимости представители других подразделений Банка.

Банк имеет в составе подразделение по информационной безопасности, непосредственно подчиняющееся ответственному лицу за информационную безопасность Банка. Подразделение по информационной безопасности контролирует и координирует назначенных лиц по применению Политики информационной безопасности Банка (Группы Пиреус) в различных сферах, внедрение соответствующей защиты и механизмов контроля и эффективное выполнение задач по информационной безопасности. Сотрудникам подразделения по информационной безопасности запрещено разрабатывать, внедрять, сопровождать или эксплуатировать информационные системы Банка, которые не используются для обеспечения безопасности информации.

2.2.5. Эффективность административных и технических средств контроля информационной безопасности

Для соблюдения соответствующего уровня информационной безопасности в Банке необходимо внедрение и пересмотр эффективности административных и технических средств безопасности (контролей). Административные и технические средства безопасности (контроли) важны, поскольку они взаимосвязаны между собой и формируют единую систему управления информационной безопасностью.

Административные и технические средства безопасности (контроли), которые используются в Банке, проверяются на соответствие существующим политикам, процедурам и стандартам, а также

проводится их переоценка эффективности предотвращения существующих угроз и актуализация в соответствии с требованиями информационной безопасности.

2.2.6. Ответственность за соблюдением работниками требований по информационной безопасности

Директора департаментов и руководители самостоятельных структурных подразделений Банка должны принимать все необходимые меры для соблюдения политик, процедур, стандартов, инструкций, регламентов и методических рекомендаций информационной безопасности в их подразделениях. Ответственность по общему уровню информационной безопасности, соблюдению Политики информационной безопасности в Банке возложена на Руководство Банка и распространяется на всех работников на всех уровнях Банковской организационной структуры (top-down approach).

2.2.7. Аудит Политики информационной безопасности

Проверка соблюдения политик, процедур, стандартов, инструкций, регламентов и методических рекомендаций информационной безопасности работниками Банка и третьими лицами осуществляется периодическими и непосредственными аудиторскими проверками.

2.2.8. Соответствие нормам информационной безопасности

Контроли и средства, внедренные для защиты банковской информации, определены и избраны на основе существующих регулятивных норм и контрактных обязательств Банка, обеспечивающих свободный обмен идеями, свободный информационный поток, конфиденциальность информации и коммуникаций, защиту персональных данных и прозрачность процесса.

В соответствии с требованиями действующего законодательства Председатель Правления Банка (или заменяющее его лицо) организовывает проведение внешнего аудита (с целью получения Банком оценки информационной безопасности) в соответствии с законодательством в сфере защиты информации и кибербезопасности. Такая оценка используется Банком для обеспечения своевременного мониторинга состояния внедрения и эффективности функционирования СУИБ, определения возможностей усовершенствования и необходимости проведения корректирующих действий.

Также, Банк обязан проводить ежегодную самооценку состояния информационной безопасности/киберзащиты путем составления ежегодного Отчета по оценке рисков информационной безопасности/киберрисков с учетом сведений по результатам ежегодного проведения:

1) оценка рисков информационной безопасности/киберзащиты в соответствии с внутренними нормативными документами;

2) оценка результативности информационной безопасности и эффективности СУИБ;

3) внешнему аудиту информационной безопасности;

4) внутренний аудит информационной безопасности/киберзащиты (далее - "Внутренний аудит").

Ответственность за составление отчета несет ответственное подразделение Банка за информационную безопасность.

2.2.9. Информирование и обучение по информационной безопасности

Для повышения осведомленности и ответственности работников Банка и третьих сторон в сфере информационной безопасности Банком разработана соответствующая программа обучения. Целью этой программы является обеспечение того, что все работники, имеющие доступ к банковской информации и информационным системам, понимают необходимость защиты такой информации и принимают ответственность, которую они несут. Более того, программа нацелена на разъяснение общих принципов информационной безопасности, которые должны соблюдаться всеми сотрудниками, и развитие знаний по информационной безопасности.

2.2.10. Надлежащее использование информации

Работники Банка ответственны за использование надлежащим образом банковской информации и информационных систем/инфраструктуры в соответствии с существующими политиками, процедурами, стандартами, инструкциями, регламентами и методическими рекомендациями информационной безопасности для обеспечения целей и требований бизнеса.

2.2.11. Непрерывность бизнеса

Для обеспечения непрерывности бизнеса и минимизации ущерба, который может быть причинен в случае непредвиденных ситуаций (стихийные бедствия, отказ систем и т.п.). Банк разрабатывает и применяет Планирование непрерывности бизнеса (Business continuity plan) и План восстановления деятельности подразделений (Disaster recovery plan). Руководство Банка отвечает за принятие соответствующих мер, гарантирующих непрерывность бизнеса в соответствии с потребностями бизнеса.

2.2.12. Управление персоналом

Достижение целей информационной безопасности может быть осуществлено путем включения специальных положений в договоры персонала, внедрением соответствующих мер в процесс найма новых работников, распределением обязанностей, а также наличием постоянного процесса обучения персонала по соблюдению норм и требований информационной безопасности. Обучение персонала по вопросам информационной безопасности должно осуществляться не реже одного раза в год, а также при пересмотре Политики информационной безопасности и внесении важных изменений в данную Политику или другие политики и/или процедуры, сопровождающие систему информационной безопасности Банка.

Политика информационной безопасности Банка распространяется на все подразделения Банка, а также представителей компаний, которые имеют доступ, обрабатывают или используют банковскую информацию в своей деятельности. Любые случаи несоблюдения Политики информационной безопасности расследуются и в случае выявления нарушений могут применяться дисциплинарные санкции.

2.2.13. Контроль доступа

Владельцы информации и информационных систем несут ответственность за определение лиц, которым будет предоставлен доступ к информации и информационным системам в соответствии с потребностями бизнеса и ролями пользователей. Права доступа обновляются и пересматриваются в соответствии с потребностями бизнеса. Предоставление, изменение, отмена, блокировка и

временная передача прав доступа к информации/информационным системам происходит согласно разработанным Банком регулятивных документов.

2.2.14. Мониторинг защищенности систем

Для определения уровня безопасности критических информационных активов периодически проводится мониторинг с помощью технических средств, согласно графику проведения плановых аудитов систем, для соблюдения защищенности систем. Результаты проверки критических систем анализируются и предоставляются Руководству Банка.

2.2.15. Оценка рисков

Оценка рисков должна проводиться на регулярной основе для идентификации угроз и уязвимостей, определения приемлемого уровня риска для Банка и избрания соответсвующих средств защиты, административных и технических контролей по управлению рисками.

2.2.16. Требования информационной безопасности

Требования информационной безопасности Банка разработаны и внедрены в соответствии с целями информационной безопасности и результатами регулярного процесса оценки рисков. При внедрении новой информационной системы, сервиса, службы или проекта для Банка соблюдение требований информационной безопасности является необходимым условием.

2.2.17. Обработка инцидентов по информационной безопасности

Административные и технические контроли безопасности, относящиеся к инцидентам информационной безопасности Банка, должны эффективно идентифицировать и обеспечивать обработку таких инцидентов в случае их возникновения. Пользователи информационных систем должны быть уведомлены о существующих требованиях по информационной безопасности и сразу сообщать соответствующие подразделения в случае выявления их нарушения. Инцидент информационной безопасности может быть предотвращен или идентифицирован, проанализирован и обработан.

2.2.18. Информационная безопасность при приобретении, разработке и поддержке информационных систем и приложений

Информационная безопасность должна быть приоритетным направлением при приобретении и/или разработке и поддержке информационных систем. Информационные системы, которые проектируются и/или разрабатываются и взаимодействуют с другими информационными системами, должны соответствовать утвержденным Банком политикам, процедурам, стандартам, инструкциям, регламентам и методическим рекомендациям по информационной безопасности.

2.2.19. Физическая безопасность

Здания и/или помещения Банка, используемые для хранения важного оборудования (центры обработки данных, сетевое оборудование, серверные/коммутационные комнаты и т.п.), а также критические для процессов Банка помещения должны быть обеспечены физической защитой в соответствии с установленными в Банке требованиями по физической безопасности. Физический доступ к таким помещениям предоставляется только авторизованному персоналу.

2.2.20. Управление связями с внешними сторонами

Управление связями Банка с внешними сторонами соответствует определенным нормам безопасности и внедряется в соответствии с утвержденными политиками, процедурами, стандартами, инструкциями, регламентами и методическими рекомендациями по информационной безопасности.

2.2.21. Управление связями с партнерами

Информационные системы Банка могут быть взаимосвязаны с информационными системами и/или сетями третьих сторон для быстрого поиска неисправностей или других потребностей бизнеса. В случае необходимости для таких подключений осуществляются надлежащие меры информационной безопасности для защиты банковской информации и контроля действий третьих сторон.

2.2.22. Доступ третьих сторон к информационным системам Банка

Предоставление доступа третьим сторонам к информационным системам Банка и/или банковской информации, информационным системам/инфраструктуре выполняется при условии:

- Наличие заключенных соответствующих договоров, котрые описывают юридическую сторону сотрудничества и подписанного соглашения про неразглашение конфиденциальной информации (например, non-disclosure Agreement, NDA);
- Четко определенных необходимых и достаточных требований и контролей информационной безопасности;
- Наличие технической возможности для предоставления доступа.

Доступ к банковской информации при наличии всех необходимых контролей может быть предоставлен только авторизованным пользователям.

2.2.23. Минимальный уровень полномочий

Для проведения любой деятельности в информационных системах Банка предоставление полномочий и прав доступа происходит согласно принципу минимального уровня полномочий, а именно: полномочия и права доступа, имеющие субъекты в информационной системе банка минимально необходимы для качественного выполнения возложенных задач.

3. Пересмотр Политики информационной безопасности

Политика информационной безопасности пересматривается при необходимости, но не реже одного раза в год. Внеплановый пересмотр Политики информационной безопасности возможен в случае внесения изменений в информационную инфраструктуру и/или внедрение новых информационных технологий, а также изменений в законодательные, регуляторные и нормы и т.д.

В случае изменений в законодательстве Украины, нормативно-правовых актах Национального банка Украины и международных требований, эта Политика используется в частях, не противоречащих приведенным изменениям, до ее обновления.

4. Ознакомление с требованиями Политики информационной безопасности

Для обеспечения ознакомления персонала Банка и представителей третьих сторон, которые имеют доступ (в частности, удаленный) к информации и/или информационным системам/инфраструктуре Банка, с Политикой, нормы настоящей Политики размещаются на корпоративном портале Банка в форме отдельного электронного документа.

При обновлении содержимого Политики обязательно производится обновление документа на корпоративном портале Банка.

Ответственность за определение объема норм и требований Политики, публикуемая на корпоративном портале Банка, возлагается на Управляющий орган СУИБ.

Персонал Банка и представители третьих сторон, имеющих доступ к информации и/или информационным системам Банка во время приема на работу (перед получением доступа к информации/информационным системам для представителей третьих сторон) обязаны ознакомиться с Политикой и предоставить обязательство о неразглашении конфиденциальности.