Публичное акционерное общество
«Московская Биржа ММВБ-РТС»
(ПАО Московская Биржа)

УТВЕРЖДЕНО
решением Наблюдательного совета
ПАО Московская Биржа
«31» октября 2022 г., протокол № 9

Председатель
Наблюдательного совета

_____

ПОЛИТИКА
управления информационной безопасностью Публичного акционерного общества «Московская Биржа ММВБ-РТС»

Москва – 2022

Содержание

1. Общие положения

1.1. Настоящая Политика управления информационной безопасностью Публичного акционерного общества «Московская Биржа ММВБ-РТС» (далее – Политика) является основополагающим документом системы управления информационной безопасности ПАО Московская Биржа (далее – Компания), определяющим приоритеты, принципы и методы обеспечения информационной безопасности, в условиях наличия угроз, характерных и существенных для систем и информационных технологий Компании.

1.2. Требования настоящей Политики дополняют требования Декларации информационной безопасности Компании и учитывают требования законодательства Российской Федерации в сфере информационной безопасности, международного стандарта по информационной безопасности ISO/IEC 27001:2013, современное состояние и ближайшие перспективы развития информационной инфраструктуры Компании, а также возможности современных организационно-технических методов защиты информации.

1.3. Требования настоящей Политики и других внутренних документов в части обеспечения информационной безопасности (далее – ИБ) обязательны для исполнения всеми работниками Компании.

1.4. Все отступления от требований настоящей Политики, а также иных внутренних документов в части обеспечения информационной безопасности должны быть документированы и согласованы с Департаментом операционных рисков, информационной безопасности и непрерывности бизнеса. Оформление отступления от требований Политики допустимо в случае объективного отсутствия технической возможности или нецелесообразности выполнения требований настоящей Политики, при условии разработки соответствующих компенсирующих мероприятий, которые позволяют снизить риск, вызванный невыполнением требованиям настоящей Политики. Форма документирования отступлений от требований внутренних документов ИБ приведена в Приложении А.

1.5. Система управления информационной безопасностью (далее – СУИБ) – часть общей системы управления Компании, основанная на оценке рисков информационной безопасности и предназначенная для разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

1.6. Основные термины и определения, используемые в настоящем документе, приведены в разделе Глоссарий.

2. Глоссарий

ISO/IEC 27001:2013 (Стандарт) – Международный стандарт «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

$\mathbf{P}_{\text{угрозы}}$ – вероятность реализации угрозы.

Администратор информационной системы (Администратор ИС) – работник Компании, ответственный за администрирование определенной информационной системы (ИС).

Администратор резервного копирования– сотрудник – работник Блока информационных технологий, ответственный за выполнение процедур резервного копирования. Может выделяться для одной или нескольких ИС Компании.

Актив – все, что имеет ценность для Компании и находится в ее распоряжении.

Актуализация – мониторинг и анализ действующих внутренних документов Компании, а также внесение в них в случае необходимости изменений.

Антивирусное программное обеспечение (АВПО) – программное обеспечение, предназначенное для обнаружения и уничтожения вредоносного программного обеспечения.

АРМ – автоматизированное рабочее место.

Аудитор СУИБ – работник Компании, в функции которого входит периодическая всесторонняя оценка соответствия СУИБ требованиям нормативной документации Компании по ИБ и Стандарта.

Бизнес-владелец риска – работник Компании уровня не ниже Директора Департамента, ответственный за последствия реализации выявленного риска, а также за принятие решения о способе его обработки (принятие, избежание, передача, минимизация).

Владелец актива – структурное подразделение Компании в лице руководителя, на которое возложена основная ответственность по управлению, контролю использования, обеспечению безопасности актива (информационной системы, процесса и т. п.), а также за определение степени тяжести последствий от реализации угроз ИБ в отношении активов, владельцами которых они являются.

Владелец информационной системы – ответственный работник Компании, определенный для каждой информационной системы, несущий ответственность за принятие решений по вопросам, относящимся к его компетенции согласно нормативным документам системы управления ИБ Компании.

Владелец носителя конфиденциальной информации – подразделение, которое несет ответственность за хранение и эксплуатацию данного носителя.

Владелец риска – работник Компании, ответственный за реализацию мер в соответствии с принятым решением о способе обработки риска.

Внесение изменений – модификация, в том числе внедрение, обновление и вывод из эксплуатации элементов информационной инфраструктуры, затрагивающая информационные активы Компании.

Внешняя сторона – партнер, поставщик, клиент Компании и любое другое лицо или организация, с которой взаимодействует Компания при ведении своей бизнес-деятельности за исключением компаний, входящих в Группу Московская Биржа.

Вредоносное программное обеспечение – программное обеспечение, способное нарушить информационную безопасность информационной инфраструктуры Компании.

Документирование – регламентированный процесс фиксации информации на бумажном носителе, результатом которого является официальный документ, утвержденный руководством организации.

ДОРИБиНБ – Департамент операционных рисков, информационной безопасности и непрерывности бизнеса ПАО Московская Биржа.

Доступность – свойство информации, состоящее в том, что она предоставляются авторизованному пользователю, причем в виде и месте, необходимым пользователю, и в то время, когда она ему необходима.

ДЭ – Департамент эксплуатации Блока информационных технологий ПАО Московская Биржа.

Жизненный цикл (ЖЦ) – совокупность взаимосвязанных процессов создания и последовательного изменения состояния объекта информационной инфраструктуры от формирования исходных требований к нему до окончания эксплуатации и утилизации комплекса средств автоматизации.

Запись – документ, содержащий достигнутые результаты или свидетельства осуществленной деятельности.

Изменение прав доступа – предоставление или отзыв прав доступа.

Инвентаризация – процесс, позволяющий выявить и документально закрепить активы, находящиеся в распоряжении Компании и имеющие ценность для нее.

Информационная безопасность (ИБ) – безопасность, связанная с угрозами в информационной сфере.

Информационная инфраструктура (ИТ-инфраструктура) – совокупность систем обработки информации и обрабатываемых данных, используемая для обеспечения деятельности Компании.

Информационная система (ИС) – система, состоящая из совокупности взаимосвязанных аппаратных и программных средств автоматизации, реализующая информационную технологию выполнения функций Компании.

Информационный актив – программное обеспечение, аппаратный комплекс или программно-аппаратный комплекс, реализующий необходимые функции в рамках бизнес-процесса Компании.

Инцидент ИБ – единичное нежелательное или неожиданное событие ИБ (или совокупность таких событий), которое может угрожать ИБ (может нарушить конфиденциальность, целостность или доступность информации Компании).

Классификация информационных активов – разделение существующих информационных активов Компании по типам, выполняемое в соответствии с их критичностью с точки зрения их значимости для достижения бизнес-целей Компании.

Команда управления чрезвычайной ситуацией (КУЧС) – коллегиальный орган Компании, уполномоченный на координацию действий подразделений и отдельных

работников Компании в условиях ЧС, в рамках предоставленных ему полномочий в соответствии с их должностными инструкциями и положениям Политики обеспечения непрерывности бизнеса

Комитет по управлению нефинансовыми рисками и информационной безопасностью (Комитет по управлению НР и ИБ) – консультативно-совещательный орган ПАО Московская Биржа, подотчетный Правлению ПАО Московская Биржа, рассматривающий вопросы управления нефинансовыми рисками, рисками информационной безопасности и непрерывности бизнеса Группы Московская Биржа.

Компания – ПАО Московская Биржа.

Компрометация оборудования – факт несанкционированного доступа к оборудованию, а также подозрение осуществления такого доступа.

Компрометация пароля – утрата гарантии того, что пароль известен только авторизованным лицам.

Конфиденциальная информация – информация в электронном (цифровом) виде, обрабатываемая в информационной инфраструктуре Компании, а также в бумажном и ином виде, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации и внутренними документами Компании. Конфиденциальная информация Компании включает в себя коммерческую тайну, а также персональные данные и иную охраняемую законом тайну.

Конфиденциальность – свойство информации, заключающееся в том, что она не станет доступной и не будет раскрыта неавторизованным пользователям.

Криптографический ключ (ключевая информация) – секретная информация, используемая СКЗИ при шифровании/расшифровке сообщений, создании и проверке электронной подписи, вычислении кодов аутентификации.

Куратор по информационной безопасности (Куратор по ИБ) – Директор Департамента операционных рисков, информационной безопасности и непрерывности бизнеса.

Лицензионный ключ – файл, содержащий данные, подтверждающие наличие лицензии на определенный период времени, необходимый для корректной работы антивирусного программного обеспечения.

Локально-вычислительная сеть (ЛВС) – совокупность серверов, автоматизированных рабочих мест и периферийного оборудования, функционирующих в единой информационной среде, образованной путем организации между ними взаимодействия средствами телекоммуникационного оборудования.

Менеджер по обеспечению непрерывности бизнеса – работник Компании, в функции которого входит координация мероприятий по обеспечению бесперебойной деятельности Компании и бесперебойного функционирования бизнес-процессов Компании.

Менеджер по информационной безопасности (Менеджер ИБ) – работник Компании, ответственный за координацию деятельности по реализации, эксплуатации, контролю и поддержанию на должном уровне СУИБ Компании.

Менеджер по обучению ИБ – работник Компании, в функции которого входит организация, планирование, регулярное проведение обучения по ИБ, в том числе организация учебного процесса и тестирование знаний работников по вопросам ИБ.

Менеджер рисков ИБ – работник Компании, ответственный за проведение всестороннего анализа СУИБ и выработки рекомендаций по совершенствованию механизмов управления.

Менеджер управления инцидентами – работник Компании, в функции которого входит организация и сопровождение комплекса мероприятий, направленных на предотвращение и реагирование на инциденты ИБ, а также организация сбора информации об инцидентах ИБ.

Методолог СУИБ – работник Компании, ответственный за управление процессами разработки, внедрения и пересмотра нормативных документов, относящихся к СУИБ.

Метрика эффективности процесса СУИБ (Метрика) – числовое значение, позволяющее определить показатель эффективности СУИБ.

Мобильное устройство – переносное устройство, используемое для хранения, обработки и передачи информации (например, ноутбук).

Мониторинг прав доступа – проверка соответствия назначенных прав доступа пользователей фактически установленным в информационных системах.

Мониторинг учетных записей – поверка актуальности существующих в ИС учетных записей.

Носитель информации – материальный объект, способный достаточно длительное время сохранять (нести) в своей структуре занесённую в/на него информацию.

Область действия СУИБ – совокупность процессов, информационных активов и элементов информационной инфраструктуры Компании.

Область инвентаризации – границы проведения инвентаризации, в которые могут включаться один или несколько бизнес-процессов Компании.

Обновления безопасности (Обновления) – обновления ПО, без которых может быть нарушена конфиденциальность, целостность или доступность информации, обрабатываемой в ИС.

Объект информационной инфраструктуры (ОИИ) – программное обеспечение, техническое средство, их комплекс либо информационная система, используемые в Компании при обработке и передаче информации в цифровом виде.

Объект Компании – помещение, здание или комплекс зданий, в котором расположены компоненты информационной инфраструктуры Компании.

Объект среды информационного актива – материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, защиты и т.д.).

Остаточный риск – риск, остающийся после его обработки.

Оценка рисков ИБ – описание выявленных рисков ИБ, определение таких характеристик, как вероятность реализации угрозы ($\mathbf{P}_{угрозы}$) и степень тяжести последствий (СТП).

Перечень стандартного ПО подразделения – список наименований и версий программных продуктов, используемых большинством пользователей подразделения.

Повышение осведомленности – регулярный процесс обучения и повышения уровня практических и теоретических навыков работников и представителей внешних сторон с использованием различных методов и инструментов.

Показатель эффективности СУИБ – величина, полученная в результате математического преобразования соответствующих метрик, позволяющая определить эффективность работы системы управления информационной безопасностью.

Пользователи документа – группа работников Компании, которым адресован нормативный документ, и которые принимают участие в процессе, регламентированном нормативным документом, руководствуясь его положениями.

Пользователь – работник Компании или представитель внешней стороны, использующий в своей деятельности информационные системы Компании.

Привилегированный пользователь – пользователь, обладающий административными полномочиями в отношении ИС.

Программное обеспечение (ПО) – совокупность программ и программных комплексов для обеспечения работы СВТ и вычислительных сетей.

Режим сканирования – запускаемый непосредственно работником Компании или запускающийся автоматически процесс проверки информации, направленный на выявление вредоносного ПО.

Риск – мера, учитывающая потенциальную возможность использования уязвимостей актива или группы активов для причинения ущерба Компании. Определяется в терминах комбинации вероятности реализации угрозы и величины потерь (ущерба) от реализации этой угрозы.

Риск информационной безопасности (Риск ИБ) – риск, связанный с возможностью утраты свойств ИБ (конфиденциальности, целостности, доступности) информационных активов Компании в результате реализации угроз ИБ. Определяется вероятностью реализации угрозы ($\mathbf{P}_{угрозы}$) и степенью тяжести последствий (СТП).

Руководитель группы тестирования систем обеспечения ИБ – работник Компании, в функции которого входит организация и проведение мероприятий по оценке устойчивости применяемых средств и механизмов защиты.

Руководитель группы эксплуатации инфраструктуры обеспечения ИБ – работник Компании, в функции которого входит сопровождение, мониторинг и настройка средств защиты информации.

Свободно распространяемое программное обеспечение – программное обеспечение, для использования которого не требуется приобретение каких-либо прав.

Сигнатурные базы – базы данных, используемые в работе антивирусного ПО, содержащие описание всех вредоносных кодов (вирусов), известных на настоящий момент разработчику антивирусного ПО, а также способов их обезвреживания.

Система антивирусной защиты информации (Система АВЗ) – комплекс организационных мероприятий, технических и программных средств, предназначенных для обеспечения защиты информационной инфраструктуры Компании от угроз, реализуемых вирусами и другим вредоносным ПО, а также распространения спама.

Система управления информационной безопасностью (СУИБ) – часть общей системы управления Компании, основанная на оценке рисков ИБ и предназначенная для разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

Примечание: Система управления включает в себя организационную структуру, политики, разработку планов, распределение ответственности, инструкции, процедуры, процессы и ресурсы.

Средство вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средство защиты информации (СЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Средство криптографической защиты информации (СКЗИ) – совокупность программно-аппаратных средств, обеспечивающих реализацию следующих функций: создание/проверку электронной подписи, шифрование/расшифрование электронных документов и электронных сообщений, создание открытых и закрытых (секретных) ключей электронных подписей и шифрования, криптографическое преобразование информации для обеспечения ее конфиденциальности и целостности.

СТП – степень тяжести последствий нарушения свойств информационных активов. В зависимости от свойств информационных активов: СТП нарушения конфиденциальности, СТП нарушения целостности, СТП нарушения доступности.

Структурное подразделение – официально выделенная часть Компании и относящиеся к ней работники, выполняющие установленный круг обязанностей и отвечающие за выполнение возложенных на них задач.

Угроза – опасность, предполагающая возможность потерь (ущерба).

Угроза информационной безопасности – угроза нарушения свойств ИБ (доступности, целостности или конфиденциальности) информационных активов Компании.

Управление рисками ИБ – непрерывный, цикличный и документируемый процесс выявления, сбора, использования и анализа информации, позволяющей провести оценку рисков ИБ.

Ущерб – убытки, непредвиденные расходы, утрата имущества, упущенная выгода, полученные в результате неблагоприятного воздействия на бизнес Компании (утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры Компании).

Функциональное требование – формализованное требование пользователя на реализацию нового или изменение существующего обеспечения информационной системы.

Целостность – неизменность информации в процессе ее передачи или хранения.

Электронный носитель – носитель информации, предназначенный для записи и хранения данных, в основе работы которого может лежать любой физический эффект, обеспечивающий приведение системы к двум или более устойчивым состояниям.

3. Контекст Компании

3.1. Понимание Компании и ее контекста

3.1.1. Компания является крупнейшим в России организатором торговли на товарном и финансовом рынках и предоставляет российским и зарубежным инвесторам, профессиональным участникам финансового рынка и их клиентам широкий спектр возможностей по торговле акциями, облигациями, паями, производными финансовыми инструментами, валютой, государственными ценными бумагами и товарами.

3.1.2. На платформе фондового рынка Компании, объединяющем секции фондового рынка, рынка РЕПО и рынка депозитов, проводятся торги акциями, облигациями федерального займа (ОФЗ), региональными и корпоративными облигациями, суверенными и корпоративными еврооблигациями, депозитарными расписками, инвестиционными паями, ипотечными сертификатами участия и биржевыми инвестиционными фондами; оказываются услуги по организации заключения сделок РЕПО с ЦК, междилерское РЕПО, прямое РЕПО с Банком России, кроме того, операций, организаторами которых выступают Банк России, Пенсионный фонд России, Федеральное казначейство России, Внешэкономбанк и др.

3.1.3. На срочном рынке Компании обращаются: фьючерсные контракты на индексы (Индекс МосБиржи, индекс РТС, индекс волатильности RVI); фьючерсы на российские и иностранные акции, ОФЗ и еврооблигации Россия-30, на валютные пары, на процентные ставки; контракты на драгоценные металлы (золото, серебро, платина, палладий, медь); фьючерсы на нефть и сахар; опционные контракты на некоторые из этих фьючерсов.

3.1.4. На валютном рынке Компании ведутся торги валютными парами следующих валют: долларом США (USD), евро (EUR), китайским юанем (CNY), британским фунтом

(GBP), гонконгским долларом (HKD), украинской гривной (UAH), казахским тенге (KZT) и белорусским рублем (BYR). Основными валютными парами являются USD/RUB и EUR/RUB.

3.1.5. Компания также предлагает клиентам информационные услуги и технологические сервисы. В рамках оказания информационных услуг предоставляются как рыночные данные в режиме реального времени, так и информация об итогах торгов и индексах.

3.1.6. Компания активно содействует развитию российского финансового рынка, его инфраструктуры, совершенствует технологии и повышает привлекательность своих сервисов по организации торговли на товарном и финансовых рынках для отечественных и зарубежных инвесторов и эмитентов.

3.2. Понимание потребностей и ожиданий заинтересованных сторон

3.2.1. В силу необходимости осуществления управления организованными торгами, Компания прикладывает максимальные усилия для выявления потребностей и ожиданий всех заинтересованных сторон.

3.2.2. К заинтересованным сторонам относятся:

1) Центральный Банк Российской Федерации;

2) иные государственные и законодательные органы, осуществляющие регулирование деятельности Компании;

3) компании, входящие в Группу Московская Биржа;

4) действующие и потенциальные акционеры;

5) участники торгов, потребители биржевой информации;

6) внутренние потребители – работники структурных подразделений, осуществляющие взаимодействие в процессе осуществления деятельности организации;

7) ключевые поставщики услуг.

3.2.3. Требования всех заинтересованных сторон постоянно отслеживаются, осуществляется их анализ для осуществления текущей деятельности. При планировании развития Компании именно требования всех заинтересованных сторон являются основанием для осуществления изменений и развития функционала, ввода новых услуг.

3.3. Потенциальные возможности

3.3.1. Компания обладает следующими потенциальными возможностями, позволяющими гарантировать достижение системой управления информационной безопасностью ожидаемых результатов:

1) компетентные и осведомленные работники, проходящие периодическую профессиональную подготовку;

2) определена, обеспечивается и поддерживается в рабочем состоянии необходимая инфраструктура, включая центры обработки данных;

3) высокая прозрачность деятельности Компании и соответствие современным стандартам корпоративного управления

4) кодекс корпоративного управления соответствует лучшим международным практикам.

4. Понятие, цели и задачи обеспечения информационной безопасности

4.1. Под информационной безопасностью понимается защищенность информации и средств её обработки от случайных или преднамеренных воздействий естественного или искусственного характера.

4.2. Основной целью деятельности по обеспечению ИБ является достижение адекватной защищенности бизнес-процессов Компании, а также минимизация рисков ИБ при организации торгов, предоставлении сервисов на фондовом, срочном, валютном и денежном рынках.

4.3. Указанная цель достигается посредством обеспечения и постоянного поддержания конфиденциальности, целостности и доступности защищаемых информационных активов Компании.

4.4. Для достижения основной цели обеспечения ИБ Компания обеспечивает эффективное решение следующих задач:

1) инвентаризация и классификация информационных активов Компании;

2) определение рисков ИБ и потенциальных возможностей;

3) формирование и совершенствование системы управления информационной безопасности, в том числе процессов оценки и анализа ИБ;

4) определение и документирование основных требований и процедур обеспечения ИБ;

5) внедрение и настройка средств защиты информации;

6) обучение работников Компании в области ИБ;

7) своевременное выявление и устранение уязвимостей активов Компании и тем самым предупреждение возможности нанесения ущерба и нарушения нормального функционирования бизнес-процессов Компании в результате реализации угроз ИБ;

8) уменьшение до приемлемого уровня возможного ущерба Компании при реализации угроз ИБ, в том числе сокращение времени восстановления бизнес-процессов после возможных прерываний;

9) планирование и оптимизация затрат на обеспечение информационной безопасности Компании.

5. Принципы обеспечения информационной безопасности

5.1. Основными принципами обеспечения информационной безопасности Компании являются:

5.1.1. *Законность* – применение мер и средств обеспечения ИБ в строгом соответствии с положениями действующего законодательства Российской Федерации в области ИБ.

5.1.2. *Системность* – учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для обеспечения ИБ Компании.

5.1.3. *Комплексность* – согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз ИБ и не содержащей слабых мест на стыках отдельных ее компонентов.

5.1.4. *Эшелонированность* – применение нескольких защитных барьеров на пути реализации угроз ИБ.

5.1.5. *Непрерывность защиты* – деятельность по обеспечению ИБ является составной частью повседневной деятельности Компании и не должна прерываться, в том числе должна обеспечиваться постоянная поддержка физических, технических и программных средств защиты, а также непрерывный контроль выполнения требований ИБ.

5.1.6. *Своевременность* – Компания должна своевременно обнаруживать угрозы ИБ, потенциально способные повлиять на достижение бизнес-целей Компании, прогнозировать возможные пути их развития, оценивать степень влияния на бизнес-процессы и применять меры ИБ в тех местах и в такое время, где и когда они необходимы.

5.1.7. *Адекватность* – принимаемые меры ИБ должны быть эффективны и соразмерны имеющим место рискам ИБ с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз.

5.1.8. *Реализуемость* – все предъявляемые требования ИБ должны быть реально выполнимы и непротиворечивы.

5.1.9. *Преемственность и совершенствование* – постоянное совершенствование мер и средств защиты на основе преемственности организационных и технических решений и кадрового состава.

5.1.10. *Гибкость* – СУИБ Компании должна быть способна реагировать на изменения внешней среды и условий осуществления Компанией своей деятельности.

5.1.11. *Удобство для пользователей* – при построении и модернизации СУИБ должны учитываться и по возможности сводиться к минимуму возможные затруднения пользователей в работе со средствами защиты и при выполнении основных процедур обеспечения ИБ.

5.1.12. *Документированность* – все требования и меры ИБ, а также результаты деятельности по обеспечению ИБ должны быть документально зафиксированы.

5.1.13. *Осведомленность о требованиях ИБ* – все работники Компании обязаны знать требования ИБ в объеме, соответствующем их текущим должностным обязанностям и доступу к информационным ресурсам Компании, и руководствоваться ими в своей работе.

5.1.14. *Минимизация полномочий* – работникам Компании предоставляется доступ только к тем информационным активам и в том объеме, который необходим для выполнения их должностных обязанностей.

5.1.15. *Исключение конфликта интересов* – четкое разделение обязанностей и исключение ситуаций, когда сфера ответственности работников допускает конфликт интересов. В частности, ни один работник Компании не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций.

5.1.16. *Знание своих клиентов и работников* – Компания должна обладать информацией о своих клиентах, тщательно подбирать работников и обслуживающий персонал, вырабатывать и поддерживать корпоративную этику, создавая благоприятную доверительную среду для деятельности Компании по управлению информационными активами.

5.1.17. *Персональная ответственность* – ответственность за соблюдение требований ИБ возлагается на каждого работника Компании в пределах его полномочий.

6. Организация системы управления информационной безопасности (СУИБ)

6.1. Определение СУИБ

6.1.1. СУИБ представляет собой часть общей системы управления Компании, основанная на оценке рисков ИБ и предназначенная для разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности в Компании.

6.1.2. Система управления включает в себя организационную структуру, политики, разработку планов, распределение ответственности, инструкции, процедуры, процессы и ресурсы.

6.2. Область действия СУИБ

6.2.1. Областью действия СУИБ являются бизнес-процессы Компании в части организации торгов и предоставлении сервисов на фондовом, срочном, валютном и денежном рынках и охватывает следующую единую технологическую цепочку:

6.2.2. Область действия СУИБ охватывает следующие структурные подразделения Компании:

1) основные подразделения, реализующие технологическую цепочку организации торгов и предоставления сервисов на фондовом, срочном, валютном и денежном рынках:

- Операционный Департамент;

2) вспомогательные подразделения, обеспечивающие технологическую цепочку организации торгов и предоставления сервисов на фондовом, срочном, валютном и денежном рынках:

- Департамент листинга;
- Департамент клиентской поддержки;
- Департамент сопровождения торговых и вспомогательных систем;
- Департамент эксплуатации;
- Департамент технической поддержки пользователей;

– Департамент операционных рисков, информационной безопасности и непрерывности бизнеса.

6.2.3. В область действия СУИБ также входят все информационные активы, включая конфиденциальную и открытую (общедоступную) информацию, принадлежащие и (или) обрабатываемые Компанией, которые обеспечивает реализацию, и поддерживают функционирование данной технологической цепочки.

6.2.4. В область действия СУИБ входят офисы Компании, расположенные по следующим адресам:

1) 125009, г. Москва, Большой Кисловский пер., д. 13;

2) 125009, г. Москва, ул. Воздвиженка, д.4/7, стр.1.

6.2.5. Компания обеспечивает надлежащую защиту свойств ИБ (конфиденциальности, целостности, доступности) информационных активов на каждом из уровней иерархии ИТ-инфраструктуры. При этом обеспечение свойств ИБ для информационного актива заключается в создании необходимой защиты соответствующих ему объектов среды путем уменьшения или полного закрытия уязвимостей данного объекта за счет использования защитных мер.

6.2.6. Основными объектами ИТ-инфраструктуры Компании, подлежащими защите, являются:

1) информационные активы, необходимые для работы Компании, независимо от формы и вида их представления;

2) элементы ИТ-инфраструктуры, включая информационные технологии, технические и программные средства формирования, обработки, передачи, хранения (в том числе архивирования) и использования информации, в том числе библиотеки, архивы, базы данных, каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены защищаемые элементы ИТ-инфраструктуры Компании;

3) процессы, регламенты и процедуры обработки информации в Компании;

4) работники Компании.

6.3. Реализация СУИБ

6.3.1. Реализация и функционирование СУИБ Компании основываются на «процессном подходе». Для реализации и поддержания ИБ в Компании реализуются четыре группы процессов:

1) планирование СУИБ («планирование»);

2) реализация СУИБ («реализация»);

3) мониторинг и анализ СУИБ («проверка»);

4) поддержка и улучшение СУИБ («совершенствование»).

6.3.2. Группы процессов СУИБ Компании организуются в виде циклической модели «... – планирование – реализация – проверка – совершенствование – планирование – ...», которая является основой модели СУИБ Компании.

6.3.3. На этапе «Планирование» осуществляется формирование Политики ИБ, выполняется деятельность по определению области действия СУИБ и оценке рисков ИБ, проводится выбор и формируются планы реализации защитных мер (в том числе планы обработки рисков ИБ).

6.3.4. На этапе «Реализация» осуществляется выполнение всех планов, связанных с построением, вводом в действие, совершенствованием СУИБ и внедрением защитных мер. В том числе реализуется деятельность по обучению и повышению осведомленности работников в области ИБ, обнаружению и реагированию на инциденты ИБ, обеспечению непрерывности деятельности Компании.

6.3.5. На этапе «Проверка» проходит проверка соответствия выбранных защитных мер установленным требованиям ИБ, а также оценка соответствия ИБ Компании требованиям законодательства Российской Федерации, Стандарта и внутренним документам Компании.

6.3.6. Результат выполнения деятельности на этапе «Проверка» является основой для выполнения деятельности по совершенствованию СУИБ, в рамках которой принимаются решения о реализации корректирующих и превентивных мер. При этом сама деятельность по совершенствованию СУИБ реализуется в рамках этапа «Реализация» и при необходимости – «Планирование».

6.3.7. Руководство Компании, осознавая важность вопросов обеспечения ИБ, инициирует, поддерживает, анализирует и контролирует выполнение процессов СУИБ, способствующих формированию условий для дальнейшего развития бизнеса с допустимыми рисками.

7. Направления развития и совершенствования СУИБ

7.1. Основные направления развития и совершенствования СУИБ

7.1.1. Настоящая Политика определяет следующие основные направления постоянного развития и совершенствования СУИБ:

1) распределение функций и ответственности работников Компании в сфере обеспечения информационной безопасности;

2) управление документацией СУИБ;

3) управление рисками информационной безопасности;

4) мониторинг, анализ эффективности и совершенствование процессов СУИБ;

5) обеспечение информационной безопасности при работе с персоналом;

6) повышение уровня знаний и контроль знаний работников Компании в области ИБ;

7) организация работы со сторонними организациями;

8) обеспечение физической безопасности и защита оборудования;

9) технические и организационные меры обеспечения информационной безопасности;

10) управление информационной инфраструктурой Компании;

11) управление инцидентами информационной безопасности;

12) управление информационными активами;

13) управление доступом к информационным активам;

14) обеспечение защиты от вредоносного кода;

15) обеспечение защиты от утечек информации;

16) управление носителями информации;

17) обеспечение безопасности сетевой инфраструктуры;

18) криптографические меры защиты информации;

19) обеспечение защиты среды виртуализации;

20) управление непрерывностью бизнеса;

21) соблюдение требований законодательства;

22) регистрация и мониторинг событий;

23) обеспечение безопасности на этапах жизненного цикла информационных систем;

24) управление уязвимостями;

25) резервное копирование и восстановление информации;

26) использование лицензионного программного обеспечения;

27) внутренние аудиты информационной безопасности.

7.1.2. Требования настоящей Политики должны уточняться в соответствующих частных политиках, положениях, процедурах, инструкциях и методиках, разрабатываемых в рамках СУИБ.

7.2. Распределение ролей и ответственности в области информационной безопасности

7.2.1. Для реализации, эксплуатации, контроля и поддержания на должном уровне СУИБ в Компании в рамках Департамента операционных рисков, информационной безопасности и непрерывности бизнеса сформированы следующие направления деятельности во главе с руководителем каждого из направлений:

1) информационной безопасности;

2) направление обеспечения непрерывности бизнеса;

3) направление операционных рисков.

7.2.2. Работники Департамента операционных рисков, информационной безопасности и непрерывности бизнеса в рамках своих полномочий организуют и контролируют выполнение всех мероприятий по обеспечению ИБ Компании, направленных на снижение рисков ИБ и управление ими, организуют создание и эксплуатацию СУИБ, а также эксплуатацию ИС в соответствии с правилами и требованиями, задаваемыми СУИБ.

7.2.3. Планирование затрат и выделение ресурсов, в том числе финансовых, необходимых для реализации и функционирования СУИБ и управления рисками, осуществляются Директором Департамента операционных рисков, информационной безопасности и непрерывности бизнеса на основе планов мероприятий по каждому из вышеперечисленных направлений деятельности Департамента, представленных их руководителями. В случае необходимости, к планированию могут привлекаться также и другие подразделения Компании.

7.2.4. Реализация технических мероприятий по обеспечению ИБ и разграничению доступа к информационным активам Компании осуществляется соответствующими подразделениями Блока ИТ, совместно с Департаментом операционных рисков, информационной безопасности и непрерывности бизнеса.

7.2.5. Для поддержания взаимосвязи целей обеспечения ИБ с целями основной бизнес-деятельности Компании, повышения уровня осознания ИБ и вовлечения руководства Компании в функционирование СУИБ, Директор Департамента операционных рисков, информационной безопасности и непрерывности бизнеса выступает в роли куратора деятельности вышеуказанных направлений Департамента

7.2.6. В целях координации деятельности Компании по обеспечению информационной безопасности создан Комитет по управлению НР и ИБ. Комитет является центральным органом планирования, организации и контроля реализации настоящей Политики.

7.2.7. Дополнительно в рамках СУИБ Директор Департамента операционных рисков, информационной безопасности и непрерывности бизнеса (при наличии соответствующих полномочий) назначает работников, ответственных за выполнение следующих ролей:

1) *Менеджер по информационной безопасности (Менеджер ИБ)*, является ответственным за координацию деятельности по реализации, эксплуатации, контролю и поддержанию на должном уровне СУИБ Компании;

2) *Менеджер системы обеспечения бесперебойной деятельности*, является ответственным за управление системой обеспечения бесперебойной деятельности Компании и обеспечение бесперебойного функционирования бизнес-процессов Компании;

3) *Менеджер управления инцидентами*, является ответственным за организацию и сопровождение комплекса мероприятий, направленных на предотвращение и реагирование на инциденты ИБ, а также за расследование инцидентов ИБ;

4) *Менеджер рисков ИБ*, является ответственным за проведение всестороннего анализа СУИБ и выработку рекомендаций по совершенствованию механизмов управления;

5) *Аудитор СУИБ*, является ответственным за периодическую всестороннюю оценку соответствия СУИБ требованиям нормативной документации Компании по ИБ и Стандарта;

6) *Менеджер по обучению СУИБ*, является ответственным за организацию, планирование, регулярное проведение обучения по ИБ, в том числе организацию учебного процесса и тестирование знаний работников по вопросам ИБ.

7) *Методолог СУИБ*, является ответственным за разработку, анализ, контроль и актуализацию нормативной документации по обеспечению ИБ, а также за обеспечение документооборота и делопроизводство в рамках СУИБ.

7.2.8. При назначении работников, ответственных за роли, должна быть определена Матрица конфликтующих ролей системы управления информационной безопасностью.

7.3. Управление документацией СУИБ

7.3.1. Разработка, оформление, согласование, регистрация, хранение, передача и уничтожение документации, относящейся к СУИБ Компании, должны соответствовать принятым в Компании требованиям по управлению документацией.

7.3.2. Для всей документации СУИБ должна быть обеспечена её сохранность. Доступ к документации, представленной, как на печатных носителях, так и в электронном виде и содержащей конфиденциальную информацию, должен быть ограничен и предоставляться только тем работникам Компании, которым он необходим для выполнения своих должностных обязанностей.

7.3.3. Все положения документации Компании по обеспечению ИБ должны быть согласованы между собой и не должны противоречить требованиям настоящей Политики.

7.3.4. В процессе функционирования СУИБ должны создаваться записи с целью определения соответствия СУИБ принятым требованиям по обеспечению информационной безопасности, а также анализа ее эффективности для последующего совершенствования.

7.3.5. При документировании отступлений от требований настоящей Политики, а также иных внутренних документов в части обеспечения информационной безопасности все поля Приложения А являются обязательными для заполнения, в частности должно быть задокументировано обоснование невозможности применения таких требований.

7.3.6. Копии действующих внутренних документов и записей, относящихся к СУИБ Компании, должны храниться в Департаменте операционных рисков, информационной безопасности и непрерывности деятельности.

7.4. Управление рисками

7.4.1. В целях создания эффективной СУИБ, достижения адекватной защищенности информационных активов Компании и соответствующих им объектов среды в Компании реализуется деятельность по управлению рисками ИБ, которая является неотъемлемой частью всей деятельности по обеспечению ИБ Компании и применяется как при внедрении, так и при текущем функционировании СУИБ.

7.4.2. Управление рисками ИБ представляет собой непрерывный процесс, в рамках которого проводится анализ того, что может произойти, а также возможных последствий, после чего принимаются решения о том, что и когда следует предпринять для уменьшения риска до приемлемого уровня путем предотвращения возникновения угроз ИБ и (или) минимизации последствий в случае их реализации.

7.4.3. Подход к управлению рисками ИБ должен быть согласован с общим подходом к управлению рисками основной бизнес-деятельности Компании и соответствовать среде функционирования Компании.

7.4.4. Процедура и методика оценки рисков должны быть определены и документированы. Должна быть определена ответственность за разработку и пересмотр рисков ИБ, а также за утверждение критериев принятия рисков и уровня остаточного риска. Обязательно должен проводиться пересмотр результатов оценки рисков через запланированные интервалы, включая пересмотр остаточных рисков и установленных уровней приемлемого риска.

7.4.5. Меры, принимаемые в области обеспечения информационной безопасности, должны быть направлены на выявляемые риски ИБ эффективным и своевременным образом в тех местах и в такое время, когда они необходимы.

7.5. Мониторинг, анализ эффективности и совершенствование процессов СУИБ

7.5.1. В Компании должен проводиться мониторинг процессов СУИБ с целью:

1) быстрого обнаружения ошибок в результатах обработки информации;

2) быстрого выявления удачных и неудавшихся попыток нарушений и инцидентов информационной безопасности;

3) выявления отклонений от планового процесса обеспечения информационной безопасности Компании и определение причин отклонений;

4) оценки эффективности мероприятий, предпринятых для совершенствования СУИБ (путем введения специальных показателей эффективности – метрик).

7.5.2. В Компании регулярно, не менее 1 (одного) раза в год, должен проводиться анализ СУИБ. При этом должны учитываться результаты проведения аудитов безопасности, статистика и дополнительная информация по произошедшим инцидентам ИБ, результаты оценки эффективности процессов ИБ, а также предложения и комментарии от всех заинтересованных сторон.

7.5.3. В Компании должна непрерывно совершенствоваться СУИБ путем применения корректирующих и предупреждающих мер, определенных по результатам анализа СУИБ. Порядок выбора, согласования и применения, корректирующих и предупреждающих мер должен быть документирован.

7.6. Обеспечение информационной безопасности при работе с персоналом

7.6.1. В Компании должны быть определены требования ИБ на следующих этапах взаимоотношений с работниками:

1) при приеме на работу;

2) во время действия трудового договора;

3) при увольнении или переводе на другую должность.

7.6.2. С каждым работником Компании при найме должен быть заключен трудовой договор, в котором оговариваются взаимные обязательства и права Компании и работника. В обязательном порядке с работником должно подписываться договорное обязательство о неразглашении конфиденциальной информации, определяющее обязанности работника по обеспечению ИБ в Компании.

7.6.3. При увольнении или переводе на другую должность все работники должны возвратить принадлежащие Компании информационные активы, переданные им во временное пользование для выполнения должностных обязанностей. Порядок увольнения и перевода на другую должность работников Компании, возвращения оборудования и отмены (изменения) прав доступа должен быть документирован.

7.7. Повышение уровня знаний и контроля знаний работников Компании в области ИБ

7.7.1. Все работники Компании должны быть ознакомлены под подпись со своими обязанностями и документами СУИБ в рамках своих функциональных обязанностей.

7.7.2. При приеме работника на работу с ним должен проводиться инструктаж по соблюдению требований ИБ под подпись.

7.7.3. Работники Компании должны регулярно проходить обучение (повышение уровня знаний) в области ИБ.

7.7.4. Работники Компании, ответственные за определение и контроль требований по ИБ должны постоянно поддерживать уровень своей компетенции.

7.7.5. Должен проводиться периодический контроль знаний работников Компании в области ИБ.

7.8. Организация работы со сторонними организациями

7.8.1. Компания в процессе своей деятельности взаимодействует со следующими сторонними организациями:

1) контрагенты;

2) государственные органы;

3) участники торгов;

4) информационные агентства;

5) иные лица и контрагенты, с которыми Компания взаимодействует в процессе своей деятельности.

7.8.2. При заключении договоров со сторонними организациями необходимо учитывать требования ИБ, принятые как в Компании, так и в организации второй стороны. Согласованные требования по информационной безопасности, касающиеся порядка обмена, обработки, хранения и распространения информации, предоставления доступа сторонних организаций к информационным активам Компании должны быть зафиксированы в договоре и/или соглашении о конфиденциальности и неразглашении информации сторонами.

7.8.3. В договоре с контрагентами, оказывающими услуги по физической безопасности и обслуживанию информационной инфраструктуры, должны быть учтены требования к порядку осуществления доступа на территорию, в помещения и к информационным активам Компании.

7.8.4. Взаимодействие с государственными органами регламентируются соответствующими федеральными законами и другими нормативно-правовыми актами Российской Федерации.

7.9. Обеспечение физической безопасности и защита оборудования

7.9.1. В Компании должны быть определены и документированы требования к порядку обеспечения физической безопасности и безопасности оборудования, в частности к:

1) физическому периметру безопасности и механизмам контроля входа и выхода;

2) защите от угроз окружающей среды (пожаров, затоплений, актов гражданского неповиновения и других форм стихийных бедствий и антропогенных катастроф);

3) работе в помещениях ограниченного доступа;

4) размещению и защите оборудования;

5) использованию вспомогательных систем и кабельной разводки;

6) техническому обслуживанию и перемещению оборудования;

7) безопасной утилизации и повторному использованию оборудования;

8) использованию оборудования вне территории Компании.

7.9.2. Информационные активы Компании должны располагаться в помещениях ограниченного доступа с установленным периметром безопасности с соответствующими защитными барьерами и механизмами контроля входа.

7.9.3. Порядок доступа на территорию и в помещения работников Компании и представителей сторонних организаций должен быть документирован.

7.10. Технические и организационные меры обеспечения информационной безопасности

7.10.1. В Компании должны быть определены и документированы требования к следующим группам механизмов обеспечения информационной безопасности:

1) управление правами доступа к информационным активам Компании;

2) допустимое использование информационных активов Компании;

3) настройка элементов информационной инфраструктуры в части ИБ;

4) использование средств защиты информации;

5) использование удаленного доступа.

7.10.2. В Компании должен осуществляться контроль выдачи мобильного оборудования и сменных носителей информации, а также уничтожение конфиденциальной информации, хранящейся на них, при завершении их использования.

7.11. Управление информационной инфраструктурой Компании

7.11.1. По отношению к управлению безопасностью ИТ-инфраструктуры Компании должны быть определены и документированы требования к следующим группам механизмов обеспечения безопасности:

1) планирование, приобретение и приемка компонентов ИТ-инфраструктуры;

2) обслуживание и поддержка компонент ИТ-инфраструктуры;

3) управление изменениями и конфигурацией ИТ-инфраструктуры.

7.11.2. Внедрение новых средств обработки и защиты информации должно контролироваться со стороны Комитета по управлению НР и ИБ.

7.12. Управление инцидентами информационной безопасности

7.12.1. В Компании должны проводиться сбор и анализ информации о событиях и уязвимых местах системы ИБ.

7.12.2. В Компании должен быть организован процесс управления инцидентами ИБ, в рамках которого каждый инцидент информационной безопасности должен фиксироваться и расследоваться. Результаты расследования должны доводиться до Руководства Компании. По каждому случаю нарушения требований ИБ должно приниматься решение о наложении на виновных лиц дисциплинарного взыскания.

7.12.3. Вопросы управления инцидентами ИБ должны регламентироваться отдельными нормативными документами.

7.13. Управление информационными активами

7.13.1. Защите подлежит любая информация, принадлежащая Компании или переданная Компании клиентом или сторонней организацией в рамках договорных отношений. Степень защиты информации должна выбираться в зависимости от ее

категории. Все информационные активы Компании должны защищаться в соответствии с их степенью важности для достижения целей Компании.

7.13.2. Порядок классификации и управления информационными активами должен регламентироваться отдельным нормативным документом.

7.14. Управление доступом к информационным активам

7.14.1. Управление доступом к информационным активам Компании должно определяться принципами предоставления сотрудникам и иным третьим лицам минимально необходимых для осуществления их деятельности привилегий. Доступ к информационным активам Компании должен предоставляться по согласованию с владельцем актива и ДОРИБиНБ только на основании документально обоснованной производственной необходимости.

7.14.2. Подходы к управлению доступом должны регламентироваться отдельными нормативными документами.

7.15. Обеспечение защиты от вредоносного кода

7.15.1. В Компании должны быть реализованы меры защиты от вредоносного программного обеспечения (вредоносного кода) для всех компонентов информационной инфраструктуры.

7.15.2. Должны быть внедрены меры обнаружения, предупреждения и восстановления последствий воздействия вредоносного кода.

7.15.3. Вопросы защиты от вредоносного кода должны регламентироваться отдельным нормативным документом.

7.16. Обеспечение защиты от утечек информации

7.16.1. В Компании должны осуществляться мероприятия для защиты информации от ее несанкционированного разглашения (утечки).

7.16.2. В рамках данных мероприятий должен осуществляться контроль следующей информации:

- информации, передаваемой в сеть Интернет;
- информации, передаваемой с использованием средств электронной почты;
- информации, передаваемой на печать;
- информации, записываемой на съемные носители.

7.16.3. Утечка информации и передача информационных активов (за исключением общедоступной информации) должна быть запрещена, если только такое действие не осуществляется согласно случаям, предусмотренным законодательством РФ, условиям внутренних правил и положений Компании, включая настоящую Политику, но, не ограничиваясь ею.

7.16.4. При переводе сотрудника Компании на другое место работы, вынос информационных активов из подразделения, в котором он работал до перевода, запрещен,

за исключением случаев, когда такие действия осуществляются в соответствии с внутренними правилами и положениями Компании, включая, но, не ограничиваясь настоящей Политикой.

7.16.5. Персонал Компании не должен распространять информацию Компании и её клиентов. Это касается всех работников Компании, вне зависимости от их положения, должности или деятельности вне службы.

7.16.6. Дополнительные требования в части защиты от утечек информации должны регламентироваться отдельными нормативными документами.

7.17. Управление носителями информации

7.17.1. В Компании должен вестись учет всех носителей защищаемой информации, как в письменном, так и в электронном виде. В рамках данного учета должен вестись реестр носителей.

7.17.2. Все носители информации должны быть снабжены признаками, позволяющими идентифицировать носитель и хранящуюся на нем информацию.

7.17.3. Порядок работы с носителями должен регламентироваться отдельным нормативным документом.

7.18. Обеспечение безопасности сетевой инфраструктуры

7.18.1. В Компании должно быть обеспечено управление безопасностью телекоммуникационных сетей Компании и ее элементов, позволяющее обеспечить защиту информационных активов Компании от угроз, включая постоянный мониторинг состояния сетевой безопасности сети.

7.18.2. Вопросы обеспечения безопасности сетевой инфраструктуры должны регламентироваться отдельным нормативным документом.

7.19. Криптографические меры защиты информации

7.19.1. В целях защиты конфиденциальной информации в Компании могут применяться средства криптографической защиты информации (СКЗИ).

7.19.2. Использование СКЗИ должно учитывать действующее законодательство и осуществляться в полном соответствии с технической и эксплуатационной документацией, представляемой производителем СКЗИ.

7.19.3. Вопросы применения СКЗИ должны регламентироваться отдельными нормативными документами.

7.20. Обеспечение защиты среды виртуализации

7.20.1. В Компании должны осуществляться мероприятия для защиты среды виртуализации.

7.20.2. В рамках данных мероприятий должны осуществляться:

- защита серверных компонентов среды виртуализации (в т.ч. гипервизоров);

- защита централизованного механизма управления виртуальными машинами:
- защита виртуальных машин.

7.20.3. Защита среды виртуализации должна обеспечиваться в соответствии с общими подходами в части обеспечения информационной безопасности, установленными в Компании.

7.20.4. Дополнительные требования в части защиты среды виртуализации должны регламентироваться отдельными нормативными документами.

7.21. Регистрация и мониторинг событий

7.21.1. В Компании должны осуществляться регулярный мониторинг и регистрация системных событий, действий пользователей и администраторов, ошибок и событий ИБ.

7.21.2. Все зарегистрированные события должны анализироваться на предмет наличия признаков инцидента ИБ.

7.21.3. Вопросы регистрации и мониторинга событий должны регламентироваться отдельными нормативными документами.

7.22. Обеспечение безопасности на этапах жизненного цикла информационных систем

7.22.1. Разработка, приобретение, а также внесение изменений (модернизация) в существующие элементы ИС Компании и их сопровождение должно проводиться только после выполнения следующих требований:

- определения требований информационной безопасности, предъявляемых к разрабатываемой, приобретаемой, а также эксплуатируемой ИС Компании или ее элементам, удовлетворяющих требованиям законодательства и нормативных документов Компании в области защиты информации, а также исключающих нарушение характеристик ИБ системы защиты информации Компании;
- создания отдельных сред и тестовых данных для тестирования изменений, вносимых в ИС;
- применения мер ИБ на всех этапах жизненного цикла ИС.

7.22.2. Требования безопасности должны обосновываться и документально оформляться в рамках общего проекта по внедрению информационной системы.

7.22.3. Вопросы обеспечения безопасности на этапах жизненного цикла ИС должны регламентироваться отдельным нормативным документом.

7.23. Управление уязвимостями

7.23.1. В Компании должен быть организован процесс управления уязвимостями, включающий в себя постоянное выявление, анализ и устранение выявленных уязвимостей.

7.23.2. Должны проводиться регулярные работы по тестированию на проникновение, как во внешние, так и во внутренние сети Компании.

7.23.3. Вопросы управления уязвимостями должны регламентироваться отдельным нормативным документом.

7.24. Резервное копирование и восстановление информации

7.24.1. В Компании должно выполняться регулярное резервное копирование информации, ПО и образов ИС.

7.24.2. Создаваемые резервные копии должны регулярно тестироваться. Должна быть обеспечена целостность создаваемых резервных копий.

7.24.3. Вопросы организации резервного копирования и восстановления информации должны регламентироваться отдельным нормативным документом.

7.25. Управление непрерывностью бизнеса

7.25.1. В Компании должен быть внедрен процесс управления непрерывностью бизнеса с целью снижения убытков, вызываемых авариями и сбоями в ИС Компании до приемлемого уровня путем комбинирования предупреждающих и корректирующих мер.

7.25.2. В Компании должны быть разработаны и реализованы планы, которые позволят восстановить операции основных бизнес-процессов и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя. Планы аварийного восстановления должны регулярно тестироваться и пересматриваться.

7.26. Соблюдение требований законодательства

7.26.1. Компания должна руководствоваться требованиями федерального законодательства и других нормативно-правовых актов государственных органов, требованиями внутренних документов Компании и рекомендациям международных стандартов при обеспечении ИБ и использовании материалов, охраняемых правом интеллектуальной собственности. Перечень законодательных актов Российской Федерации и стандартов по ИБ, которыми руководствуется Компания при построении СУИБ, приведен в Приложении Б.

7.27. Политика использования лицензионного программного обеспечения

7.27.1. В Компании должно использоваться только лицензионное программное обеспечение.

7.27.2. В Компании должны проводиться контроль установки лицензионного программного обеспечения и учет лицензий.

7.27.3. Должно быть организовано безопасное хранение эталонных дистрибутивов и лицензионных ключей.

7.28. Внутренние аудиты информационной безопасности

7.28.1. В Компании должны регулярно проводиться внутренние аудиты СУИБ с целью проверки того, что процессы, процедуры и механизмы контроля СУИБ:

1) соответствуют требованиям ИБ, документированным в организационно-распорядительных документах Компании;

2) соответствуют требованиям ISO/IEC 27001, а также существующим требованиям законодательства;

3) соответствуют выполнению требованиям Национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»;

4) реализованы и сопровождаются в соответствии с установленными целями и задачами информационной безопасности;

5) являются эффективными.

7.28.2. Критерии, область аудита, частота, методы проведения, ответственность, требования к планированию и проведению аудитов в Компании, а также к предоставлению отчетов по результатам и ведению записей должны быть определены и документированы.

7.28.3. Выбор аудиторов и проведение аудитов должны гарантировать объективность и непредвзятость процесса аудита. Аудиторы не должны проверять свою собственную работу.

7.28.4. Выявленные в ходе внутренних аудитов несоответствия должны устраняться в ходе корректирующих мероприятий. Если в ходе аудита принимается решение о необходимости совершенствования СУИБ для предотвращения возможных несоответствий, то такие действия выполняются в ходе предупреждающих действий.

7.28.5. Доступ к средствам аудита, с помощью которых проверяется эффективность систем защиты Компании, должен быть защищен с целью предотвращения возможного ненадлежащего использования и компрометации. Доступ к результатам аудита со стороны работников Компании и/или работников сторонних организаций должен быть ограничен.

8. Контроль выполнения требований

8.1.1. Контроль выполнения требований настоящей Политики возложен на ДОРИБиНБ.

8.1.2. Дополнительный контроль выполнения требований настоящей Политики могут осуществлять работники Службы внутреннего контроля путем регулярных проверок деятельности подразделений Компании и отдельных работников на предмет соответствия их действий требованиям законодательства Российской Федерации и внутренних документов, регулирующих деятельность по обеспечению ИБ в Компании.

9. Ответственность

9.1.1. Ответственность за обеспечение информационной безопасности Компании возлагается на все структурные подразделения Компании в рамках их полномочий и в соответствии с положениями, установленными настоящей Политикой и разработанными на ее основе документами.

9.1.2. Руководители структурных подразделений несут ответственность:

1) за своевременное доведение требований внутренних нормативных документов Компании в области ИБ до работников их подразделений в части их касающейся;

2) за выделение информационных активов Компании, подлежащих защите, владельцем которых являются их подразделения, а также согласование заявок на доступ к данным активам;

9.1.3. Все работники Компании несут персональную ответственность за свои действия при работе в информационной инфраструктуре Компании и обращении с защищаемыми информационными активами Компании, а также за выполнение требований информационной безопасности, установленных настоящей Политикой и нормативными документами, разработанными на ее основе.

9.1.4. Ответственность за контроль исполнения и актуальность настоящей Политики, а также за внесение в нее изменений возлагается на Менеджера ИБ.

9.1.5. За нарушение требований настоящей Политики и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами Компании и законодательством Российской Федерации.

9.1.6. Решение о применении и выборе мер ответственности принимается уполномоченным органом Компании по результатам проведения служебного расследования в зависимости от целесообразности применения рассматриваемых мер, а также от сведений об умышленности нарушения.

10. Порядок пересмотра и внесения изменений

10.1.1. Пересмотр положений настоящей Политики осуществляется на регулярной основе, но не реже одного раза в три года.

10.1.2. Внеплановый пересмотр настоящей Политики должен осуществляться в случае:

1) изменения нормативных документов Российской Федерации, внутренних документов Компании, определяющих требования информационной безопасности;

2) выявления снижения общего уровня информационной безопасности Компании (по результатам внутреннего или внешнего аудита);

3) существенных изменений организационной и/или технологической инфраструктуры, ресурсов и бизнес-процессов Компании;

4) выявления существенных недостатков при выполнении мероприятий, регламентированных настоящей Политикой, а также противоречий ее положений с другими внутренними документами Компании.

10.1.3. Пересмотр настоящей Политики, а также внесение в нее изменений выполняется в соответствии с порядком, установленным в Компании.

Приложение А
к Политике управления информационной безопасностью ПАО Московская Биржа

Форма документирования отступлений от требований внутренних документов ИБ

«___» _____ 20___ г. № _____

№ п/п	Описание несоответствия, обоснование	Каким документам не соответствует	Риски ИБ, связанные с несоответствием	Компенсирующие процедуры контроля	Планы по устранению	Ответственные	Срок пересмотра (не более 3 лет)

Выводы:

_____
_____
_____
_____
_____
_____

Директор ДОРИБиНБ _____ _____
(подпись) (ФИО)

«___» _____202__ г.

Приложение Б
к Политике управления информационной
безопасностью ПАО Московская Биржа

Перечень нормативных документов, регламентирующих деятельность в области ИБ

Б.1. Законодательные и подзаконные акты, регламентирующие вопросы защиты информации:

1) Конституция Российской Федерации;

2) Гражданский кодекс Российской Федерации;

3) Уголовный кодекс Российской Федерации (ст. 137, 138, 140, 183, 272, 273, 274, 274.1);

4) Кодекс Российской Федерации об административных правонарушениях (ст. 13.11, 13.12, 13.13, 13.14);

5) Трудовой кодекс Российской Федерации;

6) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

7) Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;

8) Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

9) Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;

10) Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»;

11) Федеральный закон от 21.11.2011 № 325-ФЗ «Об организованных торгах»;

12) Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;

13) приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

14) приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

15) положение Банка России от 17.10.2014 № 437-П «О деятельности по проведению организованных торгов»;

16) положение Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»;

17) национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 № 822-ст);

18) национальный стандарт Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 28.03.2018 № 156-ст).

Б.2. Законодательные и подзаконные акты по установлению режима коммерческой тайны:

1) Гражданский кодекс Российской Федерации (гл. 75);

2) Федеральный закон от 29.07.2004 №98-ФЗ «О коммерческой тайне»;

3) постановление Правительства РСФСР от 05.12.1991 № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

Б.3. Законодательные и подзаконные акты по обеспечению безопасности персональных данных:

1) Гражданский кодекс Российской Федерации (ст. 152.2);

2) Трудовой кодекс Российской Федерации (гл. 14);

3) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

4) постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

5) постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

6) постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

7) приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

8) методический документ «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021);

9) приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

10) приказ Роскомнадзора от 15.03.2013 № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

Б.4. Международные стандарты в области управления информационной безопасностью, инцидентами и непрерывностью бизнеса:

1) международный стандарт ISO/IEC 27000:2018 (Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Обзор и терминология);

2) международный стандарт ISO/IEC 27001:2013 (Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования);

3) международный стандарт ISO/IEC 27002:2013 (Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью);

4) международный стандарт ISO/IEC 27003:2017 (Информационные технологии – Методы обеспечения безопасности – Руководство по внедрению системы управления информационной безопасностью);

5) международный стандарт ISO/IEC 27004:2016 (Информационные технологии – Методы обеспечения безопасности – Измерения);

6) международный стандарт ISO/IEC 27005:2018 (Информационные технологии – Методы обеспечения безопасности – Управление рисками информационной безопасности);

7) международный стандарт ISO/IEC 27006:2015 (Информационные технологии – Методы обеспечения безопасности – Требования к органам, осуществляющим аудит и сертификацию СУИБ);

8) международный стандарт ISO/IEC 27007:2020 (Информационные технологии – Методы обеспечения безопасности – Руководство аудитора систем управления информационной безопасностью);

9) международный стандарт ISO/IEC TS 27008:2019 (Информационные технологии – Методы обеспечения безопасности – Руководство по аудиту механизмов контроля информационной безопасности);

10) международный стандарт ISO/IEC 27010:2015 (Информационные технологии – Методы обеспечения безопасности – Управление информационной безопасностью между секторами и организациями);

11) международный стандарт ISO/IEC 27014:2020 (Информационные технологии – Методы обеспечения безопасности – Управление информационной безопасностью);

12) международный стандарт ISO/IEC 27035-1:2016 (Информационные технологии – Методы обеспечения безопасности – Управление инцидентами информационной безопасности – Часть 1. Принципы управления инцидентами);

13) международный стандарт ISO/IEC 27035-2:2016 (Информационные технологии – Методы обеспечения безопасности – Управление инцидентами информационной безопасности – Часть 2. Руководство по планированию и подготовке реагирования на инцидент);

14) международный стандарт ISO/IEC 27035-3:2020 (Информационные технологии – Методы обеспечения безопасности – Управление инцидентами информационной безопасности – Часть 3. Руководство по реагированию на ИКТ-инциденты);

15) международный стандарт ISO 22300:2021 (Социальная безопасность – Терминология);

16) международный стандарт ISO 22301:2019 (Социальная безопасность – Системы управления непрерывностью бизнеса – Требования);

17) международный стандарт ISO 22313:2020 (Социальная безопасность – Системы управления непрерывностью бизнеса – Руководство);

18) международный стандарт ISO/IEC 27031:2011 (Информационные технологии – Методы обеспечения безопасности – Руководство по обеспечению готовности информационно-коммуникационных технологий к управлению непрерывностью бизнеса).