Приложение 1
к приказу АТМ/13.03.2023/1-п
от «13» марта 2023 г.

Политика информационной безопасности в ООО «Атомайз» v1

Москва 2023

ЛИСТ ИЗМЕНЕНИЙ

Политика информационной безопасности в ООО «Атомайз»		
Версия	**Дата изменения**	**Содержание изменений**
v1	13.03.2023	Первоначальная версия документа.

Оглавление

1. Термины, определения и сокращения

В настоящем документе используются следующие термины и определения:

Аудит ИБ – мероприятия для проверки текущего состояния защиты информации, независимая экспертная оценка соответствия требованиям ИБ, выполняемая работниками организации, являющейся внешней по отношению к Компании, допускающая возможность формирования профессионального аудиторского суждения о состоянии ИБ организации.

Безопасность – состояние защищенности интересов (целей) Компании в условиях угроз ИБ.

Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Доступность – свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная безопасность – свойство информации сохранять конфиденциальность, целостность и доступность.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Компании, находящаяся в распоряжении Компании и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме (сама информация, а также вспомогательные системы и средства, используемые для защиты и надлежащей работы информационных систем Компании, оборудования, носители информации и прочее).

Информация – сведения (сообщения, данные) независимо от формы их представления.

Инцидент ИБ – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Классификация информационных активов – разделение существующих информационных активов по типам, выполняемое в соответствии со степенью тяжести последствий от потери активом свойств ИБ.

Компания – ООО «Атомайз», включая региональные управления и иные обособленные структурные подразделения.

Конфиденциальная информация – информация, для которой в соответствии с законодательством Российской Федерации, нормативными документами Банка России и (или) внутренними документами Компании обеспечивается сохранение свойства конфиденциальности.

Конфиденциальность – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

Пользователь – работник Компании или иное лицо, использующее активы Компании.

Процесс – совокупность взаимосвязанных ресурсов и деятельности, преобразующая входную поступающую информацию и/или ресурсы в выходную информацию и/или ресурсы.

Работники (работники Компании) – лица, работающие в Компании на основе трудового договора (контракта), с полной или частичной занятостью независимо от их должности в Компании.

Регистрация событий защиты информации – фиксация данных о совершенных действиях или данных о событиях ИБ.

Риск ИБ – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Событие ИБ – идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

Угроза ИБ – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Управление рисками ИБ – систематический процесс применения установленных процедур (оценки рисков, обработки рисков, мониторинга рисков и пересмотра рисков) к деятельности Компании, связанной с

использованием основных информационных активов.

Утечка информации – несанкционированное предоставление или распространение конфиденциальной информации, не контролируемое Компанией.

Целостность – свойство сохранять правильность и полноту активов.

В настоящем документе используются следующие сокращения:
ИБ – информационная безопасность;
ИС – информационная система;
МВД России – Министерство внутренних дел Российской Федерации;
СКЗИ – средства криптографической защиты информации;
СКУД – система контроля и управления доступом;
ФСБ России– Федеральная служба безопасности;
ФСТЭК России– Федеральная служба по техническому и экспортному контролю;
ЦФА – цифровые финансовые активы.

2. Общие положения

2.1. Настоящая Политика информационной безопасности (далее – Политика) разработана с целью документально опередить и зафиксировать требования, правила, процедуры обеспечения информационной безопасности (далее – ИБ) в ООО «Атомайз».

2.2. ООО «Атомайз» (далее – Компания) – юридическое лицо, действующее в качестве оператора обмена цифровыми финансовыми активами (далее – ЦФА) и оператора информационной системы в соответствии с федеральным законом о ЦФА и включенное Банком России в реестр операторов обмена ЦФА и операторов информационных систем (далее – ИС).

3. Цели и задачи информационной безопасности

3.1. Основной целью Компании в области обеспечения ИБ является минимизация рисков ИБ, которым подвержены технологии и информационные системы, используемые для достижения бизнес-целей, а также обеспечение эффективности мероприятий по ликвидации неблагоприятных последствий реализации угроз и инцидентов ИБ.

3.2. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для авторизованных пользователей – устойчивого функционирования ИС Компании, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время;
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в ИС Компании и

передаваемой по каналам связи;

- конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.

3.3. Достижение данной цели должно обеспечиваться решением следующих задач:

- вовлечение руководителей прямого подчинения Генеральному директору Компании в процесс обеспечения ИБ;
- документирование требований ИБ;
- реализация мер по защите информационных активов Компании от угроз ИБ;
- оптимизация стоимости владения средствами защиты информации в рамках Компании;
- прогнозирование угроз и оценка рисков ИБ;
- предотвращение и/или снижение до приемлемого уровня ущерба от реализации актуальных угроз ИБ в Компании;
- соблюдение законодательных, нормативных и договорных требований в области ИБ, включая требования регуляторов;
- повышение стабильности функционирования Компании в условиях возможной реализации угроз ИБ;
- реагирование на инциденты ИБ;
- контроль состояния ИБ Компании;
- повышение осведомленности в вопросах обеспечения ИБ;
- постоянное совершенствование систем обеспечения ИБ Компании, включая проводимую политику обеспечения и управления ИБ.

4. Основные информационные активы

4.1. Основными информационными активами Компании, подлежащими защите, являются:

- информация, составляющая коммерческую тайну, персональные данные, внутренние документы Компании, иная информация, чувствительная по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности (в том числе открытая (общедоступная) информация), представленная в виде документов и информационных массивов, независимо от формы и вида их представления;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства обработки, передачи и отображения информации, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты ИС;
- процессы обработки информации в ИС – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, процессы жизненного цикла ИС.

4.2. Перечень информационных активов, подлежащих защите, определяется по результатам инвентаризации (учета) и классификации, проводимой в соответствии с установленным в Компании порядком, описанным отдельным внутренним документом.

5. Основные угрозы информационным активам

5.1. Основные угрозы информационным активам Компании включают в себя:

- разглашение защищаемой информации;
- компрометацию ключевой информации, персональных идентификаторов, паролей;
- несанкционированный доступ к защищаемой информации Компании;
- ввод некорректных (ложных) данных в ИС Компании;
- выход из строя материальных носителей защищаемой информации;
- уничтожение (утеря) защищаемой информации;
- нештатная ситуация в работе программного обеспечения ИС Компании;
- вирусное заражение;
- злонамеренные действия, осуществляемые посредством локальной вычислительной сети Компании;
- целенаправленные атаки на информационные активы Компании с использованием уязвимостей «нулевого дня»;
- выход из строя программно-технических средств Компании;
- нарушение функционирования технических мер защиты;
- несанкционированное или некорректное внесение изменений в информационные системы Компании;
- несанкционированное делегирование полномочий и/или использование привилегий;
- халатность, игнорирование установленных правил обеспечения ИБ, увеличивающие вероятность реализации угрозы ИБ;
- угрозы нарушения целостности и функционирования Компании в целом.

5.2. Источники угроз ИБ делятся на два основных класса:

- источники, связанные с действиями людей – внешние и внутренние нарушители;
- источники, связанные с природными явлениями (стихийными бедствиями) и неблагоприятными техногенными факторами.

5.3. В качестве внешних нарушителей ИБ рассматриваются лица, не входящие в состав пользователей и обслуживающего персонала ИС Компании, например, разработчики ИС, внешние лица (хакеры, члены криминальных организаций, бывшие работники Компании и т.п.).

5.4. В качестве потенциальных внутренних нарушителей ИБ рассматриваются пользователи и обслуживающий персонал ИС Компании, другие субъекты (лица), вовлеченные в информационные процессы Компании,

которые также имеют возможность санкционированного доступа к ИС и информационным активам Компании.

5.5. Перечень угроз безопасности информации и нарушителей безопасности определяется в ходе процедуры моделирования угроз и закрепляется в Модели угроз Компании.

6. Принципы обеспечения информационной безопасности

6.1. В основе реализации обеспечения ИБ лежит комплексный подход, который включает в себя следующие группы мер защиты информации:

- нормативно-правовые;
- организационные;
- программно-технические.

6.2. При построении ИБ Компания руководствуется рядом основополагающих принципов:

6.3. **Неотъемлемость**

Безопасность ИС является их неотъемлемым свойством (характеристикой), а не дополнительным сервисом. Соблюдение требований ИБ должно быть обязательным для всех работников и являться частью корпоративной культуры Компании.

6.4. **Комплексность**

Необходимо согласованное применение разнородных средств при построении целостной системы защиты информации, перекрывающей все каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами, обеспечивающими в комплексе инженерно-техническую защиту объектов, защиту от несанкционированного доступа к компьютерам пользователей и серверам, разграничение доступа работников к информационным ресурсам, криптографическую защиту информации, защиту каналов обмена информацией, защиту информации от утечек по техническим каналам и т.д.

6.5. **Системность**

Деятельность по защите информации должна быть строго и всесторонне регламентирована – Политика как совокупность норм, требований, положений, порядков и инструкций, должна учитывать все наиболее слабые и уязвимые места ИС и охватывать весь их жизненный цикл. При этом необходим учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения ИБ в ИС. Необходим анализ и учет всех текущих слабых и уязвимых мест ИС, возможных объектов и направлений атак, и, учитывая высокую квалификацию злоумышленников, возможных в будущем каналов реализации угроз ИБ.

6.6. **Непрерывность**

Защита информации – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС Компании, начиная с самых ранних стадий их проектирования.

6.7. **Адекватность**

Применяемые методы и средства защиты информации должны быть адекватны угрозам ее уничтожения, утечке или искажения. Недопустима как недостаточная, так и чрезмерная защита. Создать абсолютно защищенную систему принципиально невозможно, взлом системы есть вопрос только времени и средств. В связи с этим, при проектировании систем защиты информации необходимо говорить только о некотором приемлемом уровне безопасности. Важно выбрать золотую середину между стойкостью защиты и ее стоимостью, потреблением вычислительных ресурсов, удобством работы пользователей и другими характеристиками систем защиты информации. Продукт – результат компромисса между функциональностью и безопасностью.

6.8. **Идентификация и оценка активов**

Реализация принципа должна основываться на идентификации всех информационных активов и определении их ценности для целей и задач Компании.

6.9. **Гибкость и управляемость**

Системы защиты информации должны обеспечивать возможность варьировать уровень защищенности ИС. Гибкость управления и применения системы защиты информации избавляет от необходимости принятия кардинальных мер по полной замене средств защиты на новые при смене условий функционирования защищаемых систем. В целях обеспечения гибкости и управляемости защиты ИС, при выборе между организационными и техническими мерами, приоритет должен отдаваться мерам технического характера.

6.10. **Своевременность**

Разработка подсистемы ИБ должна вестись вместе с разработкой защищаемой системы. Недопустима ситуация, когда та или иная система разработана и вводится в эксплуатацию, а затем делаются попытки ее защитить. Разработка подсистемы безопасности, осуществляемая параллельно разработке защищаемой системы, оптимизирует затраты ресурсов и позволяет вырабатывать наиболее эффективные решения.

6.11. **Упреждение**

Акцент в работе системы обеспечения ИБ должен делаться на предотвращении (предупредительных мерах) событий ИБ, которые могут повлиять на целостность, доступность и конфиденциальность информации.

6.12. **Контролируемость**

Обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации. Постоянный контроль ИБ Компании, выявление и устранение уязвимостей, мониторинг событий, влияющих на ее состояние, является обязательной составляющей эффективной системы обеспечения ИБ.

6.13. **Следование лучшим практикам**

При реализации мер по обеспечению ИБ рекомендуется учитывать требования отечественных и международных стандартов в области ИБ как

лучших практик.

6.14. **Анализ и совершенствование**

Необходима постоянная работа по оценке эффективности и совершенствованию мер и средств защиты информации на основе анализа функционирования ИС, изменений в методах и средствах перехвата информации и воздействия на компоненты систем, изменений нормативных требований по защите, отечественного и зарубежного опыта в области защиты информации.

6.15. **Минимизация полномочий**

Предоставление пользователям прав доступа определяется исключительно производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, в каком это минимально необходимо работнику для выполнения его должностных обязанностей.

6.16. **Разделение функций**

При определении состава ролей, использующихся для распределения прав доступа, запрещается совмещение в рамках одной роли такого состава функций (концентрации полномочий), которое позволило бы одному работнику единолично осуществлять выполнение критичных операций или получать полный и неконтролируемый доступ к какой-либо системе Компании. Действия работников, обладающих административными полномочиями, должны находиться под особым контролем со стороны структурного подразделения по обеспечению ИБ.

6.17. **Персонификация**

Действия всех работников Компании должны осуществляться от имени персонифицированной учетной записи. Такая учетная запись у каждого работника должна быть единственной в связи с тем, что наличие у работника двух и более учетных записей делает не эффективной систему распределения и контроля полномочий. Исключение по решению руководства Компании могут составлять администраторы систем, должностные обязанности которых предполагают внесение изменений в указанные системы. Для них в дополнение к учетной записи с стандартными правами пользователя, может быть создана административная учетная запись с расширенными привилегиями. Наличие учетных записей, не закрепленных за конкретным работником, не допустимо.

6.18. **Запрещено все, что не разрешено**

Доступ к любому объекту ИС должен предоставляться только при наличии соответствующего разрешения (правила), зафиксированного в проектной документации, регламенте бизнес-процесса и настройках средств защиты информации. Любой доступ (не разрешенный явно) должен быть запрещен. Функция безопасности – разрешать необходимые доступы. Такой подход обеспечивает только известные безопасные доступы (действия) и освобождает от необходимости распознавать любую угрозу.

6.19. **Простота применения защитных мер и средств**

Используемые средства зашиты должны быть интуитивно понятны и просты в использовании. Их применение не должно быть связано со значительными дополнительными трудозатратами при обычной работе

пользователей (работники и клиенты) ИС.

6.20. **Стойкость средств защиты**

Уровень стойкости применяемых средств и эффективность мер защиты информации должны определяться ценностью защищаемого объекта и требовать от злоумышленника неадекватно больших затрат времени и вычислительных мощностей на их преодоление.

6.21. **Эшелонированность средств защиты**

Нельзя полагаться на единственный защитный рубеж, каким бы надежным он не считался. Помимо средств защиты периметра должны использоваться системы защиты внутренней сети, серверов, рабочих станций, баз данных и т.д.

6.22. **Осведомленность**

Осведомленность работников и клиентов в вопросах ИБ – обязательное условие безопасного функционирования систем.

6.23. **Персональная ответственность**

Ответственность за обеспечение безопасности информации и систем ее обработки возлагается не только на структурное подразделение по обеспечению ИБ, но и на каждого работника организации в пределах его полномочий.

6.24. **Лояльность персонала**

Необходимо создание благоприятной атмосферы во всех структурных подразделениях Компании, при которой выполнение требований ИБ не воспринимается работниками как дополнительная нагрузка, от которой желательно избавиться, а воспринимается как осознанная необходимость и неотъемлемая часть корпоративной этики. В указанной обстановке работники осознанно соблюдают установленные правила и требования ИБ и эффективно взаимодействуют со структурным подразделением по обеспечению ИБ.

6.25. **Вовлеченность руководства**

Необходимо осознание руководством Компании необходимости обеспечения ИБ, непосредственное участие в принятии стратегических решений по вопросам функционирования системы обеспечения ИБ, включая вопросы принятия рисков.

6.26. **Взаимодействие и координация**

Эффективное обеспечение ИБ достигается на основе взаимодействия и координации со структурным подразделением информационных технологий, всеми заинтересованными структурными подразделениями Компании, Управлением информационной безопасности, такими организациями как Банк России, ФСТЭК России, ФСБ России, МВД России) и другие профильные министерства, ведомства и объединения, функционирующие в стране, под чьей юрисдикцией находится Компания.

7. Управление рисками информационной безопасности

7.1. Обеспечение ИБ Компании основывается на управлении рисками ИБ, что предусматривает анализ существующих угроз ИБ, оценку рисков реализации указанных угроз и принятие необходимых мер (в том числе

применение средств защиты информации) по отношению к рискам ИБ, недопустимым для Компании.

7.2. Целью управления рисками ИБ является:

- минимизация негативных последствий от реализации рисков;
- оптимизация затрат, направленных на предотвращение негативных последствий от реализации рисков.

7.3. Порядок управления рисками должен регламентироваться отдельным внутренним документом Компании.

7.4. Ответственным за процесс управления рисками ИБ в Компании является Управление информационной безопасности.

8. Основные направления информационной безопасности

8.1. Документирование требований по ИБ

8.1.1. В Компании должен быть разработан, утвержден и доведен до работников и соответствующих внешних сторон комплект документов (политик, положений, инструкций), регламентирующих отдельные направления ИБ.

8.1.2. Документы по ИБ для гарантии их постоянной пригодности, соответствия и результативности должны пересматриваться через запланированные интервалы времени или в случае существенных изменений бизнес-процессов Компании или изменений требований законодательства Российской Федерации, нормативных документов Банка России.

8.1.3. В Компании должен быть разработан перечень, в который должны быть включены все внутренние документы Компании, регламентирующие отдельные положения обеспечения ИБ.

8.2. Организация ИБ

8.2.1. Управление ИБ должно обеспечиваться как при осуществлении информационного обмена внутри Компании, так и при взаимодействии со сторонними организациями и третьими лицами (субъектами).

8.2.2. В Компании должны быть определены структурное подразделение и лица, ответственные за организацию планирования, совершенствования и развития обеспечения и управления ИБ в Компании.

8.2.3. В Компании должны быть назначены структурные подразделения и лица, ответственные за обеспечение ИБ. Обязанности ответственных лиц должны быть определены в их должностных инструкциях.

8.2.4. Для снижения возможностей несанкционированного ознакомления, удаления, модификации, искажения и (или) злоупотребления информационными активами в Компании должен соблюдаться принцип разделения сфер ответственности. Этот принцип должен учитываться при организации всех мероприятий по ИБ в Компании, в том числе при обеспечении доступа к информационным активам Компании тех работников Компании и третьих лиц, которым это объективно необходимо, исходя из степени их ответственности, функциональных обязанностей, решаемых задач и условий заключенных договоров.

8.2.5. При выборе средств обеспечения и контроля ИБ Компания должно

ориентироваться на использование отечественных продуктов, в том числе на использование отечественного и санкционно-устойчивого системного и прикладного ПО, вычислительной техники и сетевого оборудования.

8.3. **Аудит и контроль соблюдения требований ИБ**

8.3.1. Для оценки эффективности применяемых мер и средств обеспечения ИБ, а также пригодности и адекватности подхода к обеспечению ИБ, в Компании должны периодически проводиться мероприятия по аудиту (проверке) ИБ.

8.3.2. Аудит ИБ может быть как внутренним, так и внешним. Цель, порядок и периодичность проведения аудитов ИБ Компании в целом или его отдельных структурных подразделений должны указываться в программе аудита ИБ. Порядок проведения внутреннего аудита ИБ определяется отдельным внутренним документом Компании.

8.3.3. При проведении аудитов ИБ должны использоваться стандартные процедуры документальной проверки, опрос и интервью с руководством, и персоналом организации и технические процедуры тестирования (тестирование на проникновение, нагрузочное стресс тестирование).

8.3.4. К проведению внутренних аудитов ИБ могут привлекаться специалисты, обладающие специальными навыками и знаниями, имеющих значение для проведения аудита.

8.4. **Обеспечение безопасности технологии Hyperledger Fabric**

8.4.1. В качестве информационной системы, используемой Компанией для предоставления пользователям услуг, используется технология блокчейн и фреймворк Hyperledger Fabric (далее – Платформа).

8.4.2. В качестве ядра технологического стека для Платформы используется блокчейн, основанный на фреймворке Hyperledger Fabric, предоставляемый международной компанией IBM. Безопасность транзакций заложена в продвинутом механизме консенсуса BFT (Byzantine Fault Tolerant), который позволяет реализовать систему с открытой моделью управления пользователями.

8.4.3. Система размещается в публичном облаке Yandex.Cloud, что гарантирует безопасность пользовательских данных, соответствие требованиям ФЗ-152 «О персональных данных», а также защиту от внешних и внутренних угроз.

8.5. **Управление информационными активами**

8.5.1. Защите подлежит любая информация, принадлежащая Компании или переданная Компании клиентом или контрагентом 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.

8.5.2. Порядок классификации и управления информационными активами должен регламентироваться отдельным внутренним документом Компании.

8.6. **Управление доступом к информационным активам**

8.6.1. Управление доступом (в т.ч. удаленного) к информационным

активам Компании должно определяться принципами предоставления работникам и иным третьим лицам минимально необходимых для осуществления их деятельности привилегий. Доступ к информационным активам Компании должен предоставляться по согласованию с владельцем актива и Управление информационной безопасности только на основании документально обоснованной производственной необходимости (подписанная служебная записка, электронное письмо, согласование в системе заявок и т.д.).

8.6.2. Подходы к управлению доступом (в т.ч. удаленным доступом) должны регламентироваться отдельным внутренним документом Компании.

8.7. **Защита от вредоносного кода**

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

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

8.7.3. Вопросы защиты от вредоносного кода должны регламентироваться отдельным внутренним документом Компании.

8.8. **Защита от утечек информации**

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

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

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

8.8.3. Распространение информации и передача информационных активов (за исключением общедоступной информации) должны быть запрещены, если только такое действие не осуществляется согласно случаям, предусмотренным законодательством Российской Федерации, нормативными документами Банка России, внутренними документами Компании, включая Политику.

8.8.4. При переводе работника Компании на другое место работы, вынос информационных активов из структурного подразделения, в котором он работал до перевода, запрещен, за исключением случаев, когда такие действия осуществляются в соответствии с внутренними документами Компании, включая Политику.

8.8.5. Работники Компании не должны распространять информацию о Компании. Это касается всех работников Компании, вне зависимости от их положения, должности или деятельности вне службы.

8.8.6. Дополнительные требования в части защиты от утечек информации должны регламентироваться отдельным внутренним документом Компании.

8.9. **Управление носителями информации**

8.9.1. 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 информации.

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

8.9.3. Порядок работы с носителями информации должен регламентироваться отдельным внутренним документом Компании.

8.10. **Безопасность сетевой инфраструктуры**

8.10.1. 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.

8.10.2. Вопросы обеспечения безопасности сетевой инфраструктуры должны регламентироваться отдельным внутренним документом Компании.

8.11. **Криптографические меры защиты информации**

8.11.1. В целях защиты конфиденциальной информации в Компании могут применяться средства криптографической защиты информации (далее – СКЗИ).

8.11.2. Использование СКЗИ должно учитывать законодательство Российской Федерации и осуществляться в полном соответствии с технической и эксплуатационной документацией, представляемой производителем СКЗИ.

8.11.3. Вопросы применения СКЗИ должны регламентироваться отдельным внутренним документом Компании.

8.12. **Защита среды виртуализации**

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

8.12.2. Защита среды виртуализации должна обеспечиваться в соответствии с общими подходами в части обеспечения ИБ, установленными в Компании.

8.12.3. Дополнительные требования в части защиты среды виртуализации должны регламентироваться отдельным внутренним документом Компании.

8.13. **Регистрация и мониторинг событий**

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

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

8.13.3. Вопросы регистрации и мониторинга событий должны регламентироваться отдельным внутренним документом Компании.

8.14. **Обеспечение безопасности на этапах жизненного цикла информационных систем**

8.14.1. Разработка, приобретение, а также внесение изменений (модернизация) в существующие элементы ИС Компании и их сопровождение

должно проводиться только после выполнения следующих требований:

- определения требований ИБ, предъявляемых к разрабатываемой, приобретаемой, а также эксплуатируемой ИС Компании или ее элементам, удовлетворяющих требованиям законодательства Российской Федерации, нормативных документов Банка России и внутренних 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.

8.14.2. Требования безопасности должны обосновываться и документально оформляться в рамках общего проекта по внедрению ИС.

8.14.3. Вопросы обеспечения безопасности на этапах жизненного цикла ИС должны регламентироваться отдельным внутренним документом Компании.

8.15. **Управление уязвимостями**

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

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

8.15.3. Вопросы управления уязвимостями должны регламентироваться отдельным внутренним документом Компании.

8.16. **Управление инцидентами ИБ**

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

8.16.2. Вопросы управления инцидентами ИБ должны регламентироваться отдельным внутренним документом Компании.

8.17. **Управление изменениями**

8.17.1. В Компании должен быть организован процесс управления изменениями. Все изменения, вносимые в программное обеспечение ИС и оборудование, должны регистрироваться и контролироваться.

8.17.2. Должны быть определены и зафиксированы параметры безопасных конфигураций ИС и оборудования. Данные параметры должны в обязательном порядке применяться при настройке и восстановлении работоспособности оборудования и ИС.

8.17.3. Вопросы управления изменениями должны регламентироваться отдельным внутренним документом Компании.

8.18. **Резервное копирование и восстановление информации**

8.18.1. В Компании должно выполняться регулярное резервное

копирование информации, программного обеспечения и образов ИС.

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

8.18.3. Вопросы организации резервного копирования и восстановления информации должны регламентироваться отдельным внутренним документом Компании.

8.19. **Управление непрерывностью деятельности (бизнеса)**

8.19.1. В Компании должен быть разработан и поддерживаться процесс обеспечения непрерывности обмена информацией и доступа к информационным активам в масштабах всего Компании, учитывающий требования Политики и внутренних документов по ИБ Компании, включающий в себя меры по выявлению и снижению рисков отказов и блокирования элементов ИС, ограничению последствий отказов ИС или аварий, и обеспечивающий доступность информационных активов, в том числе возможность их оперативного восстановления, требуемую для подержания непрерывности бизнес-процессов Компании.

8.19.2. Принятые меры по обеспечению непрерывности деятельности должны быть отражены в разрабатываемом Плане обеспечения непрерывности и восстановления деятельности (далее – План).

8.19.3. План должен подвергаться проверке на регулярной основе. По результатам проверки в случае необходимости должен осуществляться пересмотр данного Плана.

8.20. **Обеспечение соответствия требованиям в области ИБ**

8.20.1. Для выполнения всех обязательных требований по защите конфиденциальной информации, предписанных законодательными и другими регулирующими (нормативными) документами, в Компании должен выполняться регулярный пересмотр документов по ИБ и содержащихся в них требований.

8.20.2. Руководители структурных подразделений Компании в пределах своей области ответственности должны регулярно анализировать соответствие обработки информации и процедур требованиям внутренних документов Компании по ИБ, в том числе требованиям Политики.

8.21. **Обеспечение безопасности при работе с персоналом**

8.21.1. С целью снижения риска субъективных ошибок, краж, мошенничества или производственных злоупотреблений при приеме кандидатов на работу в Компания должны выполняться процедуры оценки благонадежности кандидатов на работу.

8.21.2. Должно осуществляться выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности работников, в том числе должен проводиться вводный инструктаж по ИБ для работников при приеме на работу, а также дальнейший контроль (проверка) полученных знаний. Должен быть разработан и доведен до сведения персонала порядок принятия дисциплинарных взысканий к тем работникам, которые допустили нарушение установленных требований ИБ.

8.21.3. Должна быть определена и доведена до сведения работников

область их ответственности в части выполнения обязанностей по обеспечению ИБ, остающихся в силе после прекращения или изменения трудовых отношений с Компанией.

8.22. **Повышение осведомленности в области ИБ**

8.22.1. В Компании должно осуществляться обучение и повышение осведомленности работников в области обеспечения ИБ.

8.22.2. Должны проводиться регулярные обучающие мероприятия для работников, а также иных третьих лиц, допущенных к информационным активам Компании. По результатам проведенных мероприятий должны проводиться регулярные проверки полученных знаний.

8.22.3. Вопросы повышения осведомленности должны регламентироваться отдельным внутренним документом Компании.

8.23. **Обеспечение безопасности при взаимодействии с третьими лицами**

8.23.1. Меры безопасности при организации работ с третьими лицами и сторонними организациями должны предусматривать:

- определение и оценку потребностей Компании в необходимости организации работ с привлечением сторонних организаций, а также проведение анализа и оценки рисков, являющихся следствием данного вида работ (в том числе определение критериев выбора и оценки сторонних организаций);
- постоянный контроль доступа третьих лиц и сторонних организаций к информационным активам Компании и средствам ее обработки;
- осуществление допуска сторонних организаций и третьих лиц к информационным активам Компании только после определения и реализации необходимых требований безопасности и ответственности за их нарушение, а также включения таких требований в заключенные с указанными лицами и организациями договоры и соглашения;
- возможность на регулярной основе отслеживать и проводить аудит услуг, предоставляемых третьим лицом или сторонней организацией.

8.23.2. Вопросы обеспечения ИБ при взаимодействии с третьими лицами должны регламентироваться отдельным внутренним документом Компании.

8.24. **Организация защиты персональных данных**

8.24.1. Персональные данные являются важным информационным активом Компании, в связи с чем Компания должно принимать меры по их защите в соответствии с требованиями законодательства Российской Федерации, нормативными документами Банка России.

8.24.2. Защита персональных данных должна обеспечиваться путем организации корректной обработки, передачи и хранения персональных данных, а также комплексом организационных и технических мероприятий, направленных на обеспечение их безопасности.

8.24.3. Вопросы обеспечения защиты персональных данных должны

регламентироваться отдельным внутренним документом Компании.

8.25. **Организация физической защиты**

8.25.1. С целью предотвращения несанкционированного доступа, повреждения оборудования, вторжения в здания и помещения Компании должны быть выделены зоны (области) безопасности (в том числе особо важные и выделенные помещения), в которых должен поддерживаться режим физической безопасности.

8.25.2. В зонах безопасности, а также во всех офисных, вспомогательных, подсобных, технических и т.п. помещениях должны быть реализованы меры по противопожарной защите, защите от аварий в системах электро-, тепло-, водо-, газоснабжения, канализации и стихийных бедствий.

8.25.3. Лица, имеющие право на доступ в помещения Компании, должны регистрироваться, должен осуществляться контроль доступа в помещения (в том числе с использованием системы контроля и управления доступом (СКУД));

8.25.4. Проводится учет следующих категорий лиц:

- лиц, которые не являются работниками, но имеют право на доступ в помещения;
- технического (вспомогательного) персонала.

8.25.5. Вышеуказанные лица должны допускаться в помещения только под контролем и в сопровождении ответственных работников Компании;

8.25.6. Для всех помещений должен быть назначен их владелец (распорядитель доступа). Доступ в помещения должен предоставляться только по согласованию с владельцем;

8.25.7. Входные двери помещений должны быть оборудованы механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время;

8.25.8. Серверное и сетевое оборудование ИС должно быть расположено в запираемых серверных стоечных шкафах. Доступ к данным шкафам должен контролироваться;

8.25.9. В случае применения средств видеонаблюдения видеозаписи должны храниться не менее 14 (четырнадцати) календарных дней.

8.25.10. Вопросы организации физической защиты должны регламентироваться отдельным внутренним документом Компании.

8.26. **Применение технических средств защиты информации**

8.26.1. Технические средства защиты информации перед их использованием должны быть размещены в информационной инфраструктуре Компании и настроены (сконфигурированы) в соответствии с требованиями эксплуатационной документации.

8.26.2. Для всех применяемых технических средств защиты информации должны быть обеспечена возможность их поддержки (сопровождения) в течение всего срока использования.

8.26.3. В случае необходимости использования технических средств защиты информации для нейтрализации актуальных угроз безопасности информации в соответствии с Моделью угроз Компании, должны применяться

средства, сертифицированные ФСТЭК России по требованиям безопасности.

9. Ответственность

9.1. Генеральный директор Компании при обеспечении ИБ в Компании несет ответственность за:

- утверждение Политики и внутренних документов Компании в части обеспечения ИБ;
- утверждение направлений развития ИБ в контексте снижения общих бизнес-рисков Компании;
- выделение финансовых и материальных средств, а также кадровых ресурсов для организации обеспечения ИБ;
- утверждение организационной структуры управления ИБ;
- назначение ответственных лиц за обеспечение ИБ.

9.2. Руководитель Управления информационной безопасности при обеспечении ИБ в Компании несет ответственность за:

- планирование, контроль, организацию и развитие мер обеспечения и управления ИБ в Компании.

9.3. Управление информационной безопасности при обеспечении ИБ в Компании несет ответственность за:

- разработку, документирование и внедрение мер обеспечения и управления ИБ;
- определение мер, необходимых для реализации планов и стратегий в части управления и защиты информации на каждом этапе ее обработки;
- анализ угроз и рисков ИБ, планирование и реализация мероприятий по снижению угроз и управлению рисками, согласование бюджета мероприятий перед руководством Компании;
- выполнение требований законодательства Российской Федерации, нормативных документов Банка России и иных применимых требований в области ИБ;
- управление применяемыми техническими средствами защиты информации, а также их сопровождение;
- контроль за применяемыми мерами ИБ и улучшение (совершенствование) применяемых мер;
- организацию обучения и повышения осведомленности работников в области ИБ.

9.4. Управление информационных технологий при обеспечении ИБ в Компании несет ответственность за:

- поддержку и участие в процессах обеспечения ИБ, связанных с использованием информационных технологий;
- соблюдение установленных требований в части обеспечения ИБ при разработке, внедрении и эксплуатации информационных систем и информационных активов;
- участие в процессе анализа угроз и рисков ИБ, планирование и реализация мероприятий по снижению угроз и управлению

рисками совместно с Управлением информационной безопасности;
- планирование, реализация мероприятий и бюджета, направленных на сопровождение закупок, эксплуатацию оборудования и информационных систем в целях информационной безопасности;
- управление применяемыми техническими средствами защиты информации, а также их сопровождение;
- предоставление информации о применяемых информационных технологиях и ИС Управлению информационной безопасности.

9.5. Руководители структурных подразделений Компании при обеспечении ИБ в Компании несут ответственность за:

- управление информационными активами, согласование прав доступа к информационным активам, принятие решений по рискам нарушения ИБ, связанным с информационными активами;
- доведение требований по обеспечению ИБ до работников подчиненных структурных подразделений;
- своевременное информирование Управления информационной безопасности о выявленных рисках и инцидентах информационной безопасности;
- исполнение требований Управления информационной безопасности по митигации рисков ИБ, устранению условий и последствий инцидентов.

9.6. Работники Компании при обеспечении ИБ в Компании несут ответственность за:

- исполнение требований внутренних документов Компании в части обеспечения ИБ.

10. Заключительные положения

10.1. Настоящая Политика подлежит регулярному пересмотру не реже 1 раза в год, а также в следующих случаях:

- изменения требований законодательства Российской Федерации, нормативных документов Банка России;
- существенных изменений в информационной инфраструктуре или организационной структуре Компании;
- выявления инцидентов ИБ, свидетельствующих о неполноте или несовершенстве настоящей Политики.

10.2. Предпосылками для пересмотра и совершенствования настоящей Политики могут также являться результаты мониторинга состояния ИБ, результаты анализа актуальных внутренних и внешних угроз, а также результаты анализа нарушений, выявленных в ходе внутреннего и внешнего контроля (несоответствие реальных технологий и состояния информационной безопасности требованиям нормативных и регламентирующих документов).

10.3. Политика должна быть доведена до всех работников и принята ими к обязательному исполнению. Политика также должна быть доведена до контрагентов и иных третьих лиц, допущенных к информационным активам Компании, и принята ими к обязательному исполнению в части, их касающейся.

10.4. Все работники Компании, а также иные третьи лица при обращении с информационными активами Компании должны руководствоваться утвержденными требованиями организационно-распорядительных, эксплуатационных, методических и иных документов, связанных с обеспечением ИБ, в том числе требованиями Политики.

10.5. За нарушение требований в области ИБ работники Компании несут персональную ответственность в соответствии с законодательством Российской Федерации.

10.6. Ответственность за осуществление общего контроля выполнения Политики, предоставление рекомендаций по их выполнению, поддержание Политики в актуальном состоянии с учетом требований международных и национальных стандартов, а также законодательства Российской Федерации, нормативных документов Банка России несет руководитель Управления информационной безопасности.

10.7. Настоящая Политика, а также все изменения к ней утверждаются Генеральным директором Компании и вступают в силу после их опубликования.

10.8. С момента вступления в силу настоящей редакции Политики, предыдущую редакцию считать недействительной.

11. Нормативные ссылки

11.1. При разработке настоящей Политики использовались следующие нормативные документы:

- Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ;
- Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»;
- Положение Банка России от 20 апреля 2021 г. № 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".