ОсОО «АЗИЯ КЭПИТАЛ»

УТВЕРЖДЕНО
приказом Генерального Директора
Общества с ограниченной
ответственностью "Азия Кэпитал"

Асанбаев А.Ж. _____
от «13» января 2025 года

ПОРЯДОК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КИБЕРБЕЗОПАСНОСТИ), ОБЕСПЕЧЕНИЕ ТЕХНИЧЕСКИХ, ИНФОРМАЦИОННЫХ, ТЕХНОЛОГИЧЕСКИХ МЕР ЗАЩИТЫ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. ОсОО «Азия Кэпитал» (далее по тексту-Общество) уделяет особое внимание вопросам обеспечения информационной безопасности, постоянно совершенствует систему управления информационной безопасностью, применяемые средства и способы защиты от угроз информационной безопасности, а также обеспечивает непрерывное обучение сотрудников Общества для поддержания компетенции в области защиты информации на высоком уровне.
1.2. Порядок описывает систему взглядов на проблему обеспечения безопасности информации, основные принципы, направления и требования по защите информации.
1.3. Нормативно-правовую основу Порядка составляет положения законодательства Кыргызской Республики по вопросам использования информационных систем и информационной безопасности, а также требования международных стандартов управления информационной безопасностью.
1.4. Порядок обеспечения информационной безопасности (кибербезопасности) и непрерывности деятельности обязательны для исполнения всеми сотрудниками Общества, стажерами, практикантами, а также должны доводиться до сведения клиентов и иных третьих лиц, имеющих доступ к информационным системам и документам Общества в той их части, которая непосредственно взаимосвязана с Обществом и их деятельностью.
1.5. Порядок охватывает все информационные системы и документы, владельцем и пользователем которых является Общество.
1.6. Обеспечение информационной безопасности – необходимое условие для успешного осуществления коммерческой деятельности Общества.

2. ЦЕЛИ, ТРЕБОВАНИЯ И ОСНОВНЫЕ ПРИНЦИПЫ

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

2.2. Информационная безопасность не является самоцелью, ее обеспечение необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами имеющимся информационным ресурсам Общества. С этой целью необходимо поддерживать главные свойства информации, а именно:

- доступность – свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия;
- конфиденциальность – свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;
- целостность – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

2.3. Процесс создания надежной информационной защиты никогда не бывает законченным. В целях обеспечения достаточно надежной системы информационной безопасности, необходима постоянная регулировка ее параметров, адаптация для отражения новых опасностей, исходящих из внешней и внутренней среды.

2.4. Не должно существовать каких-либо препятствий при внесении изменений в стандарты, процедуры или Порядка по мере возникновения такой необходимости.

2.5. В соответствии с данным Порядком, определяются следующие этапы цикла управления информационной безопасностью (модель PDCA: Plan-Do-Check-Act).

1) PLAN – Планирование (разработка) – анализ рисков, определение Порядка, целей, задач, процессов, процедур, программноаппаратных средств, относящихся к управлению рисками и совершенствованию информационной безопасности для получения результатов в соответствии с общей стратегией и целями Общества;
2) DO – Реализация (внедрение и эксплуатация) – внедрение и эксплуатация Порядка, механизмов контроля, процессов, процедур, программно-аппаратных средств;
3) CHECK – Проверка (мониторинг и анализ) – оценка и там, где это применимо, измерение характеристик исполнения процессов в соответствии с Порядком, целями и практическим опытом, анализ изменения внешних и внутренних факторов, влияющих на защищенность информационных ресурсов, предоставление отчетов руководству для анализа;
4) ACT – Корректировка (сопровождение и совершенствование) – принятие корректирующих и превентивных мер, основанных на результатах внутренних и внешних проверок состояния информационной безопасности, требований со стороны руководства, иных факторов, в целях обеспечения непрерывного совершенствования системы информационной безопасности.

2.6. Построение системы обеспечения информационной безопасности Общества и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

2.6.1. законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего

законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Общества;
2.6.2. ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности Общества;
2.6.3. непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Общества должны осуществляться без прерывания или остановки текущих бизнеспроцессов Общества;
2.6.4. комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;
2.6.5. обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска;
2.6.6. приоритетность – категорирование (ранжирование) всех информационных ресурсов Общества по степени важности при оценке реальных, а также потенциальных угроз информационной безопасности;
2.6.7. необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;
2.6.8. специализация – эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными специалистами Общества;
2.6.9. информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;
2.6.10. взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений Общества, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;
2.6.11. подтверждаемость – важная документация и все записи – документы, подтверждающие исполнение требований по информационной безопасности и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

3. ОБЪЕКТЫ ЗАЩИТЫ, ОБЛАСТЬ ПРИМЕНЕНИЯ ПОРЯДКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Основными объектами обеспечения информационной безопасности в Обществе признаются следующие элементы:

3.1.1. Информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Общества к коммерческой тайне Общества, любая иная информация, необходимая для обеспечения нормального функционирования Общества (далее – защищаемая информация);
3.1.2. Средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;
3.1.3. Программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы Общества, с помощью которых производится обработка защищаемой информации;
3.1.4. Процессы Общества связанные с управлением и использованием информационных ресурсов; помещения, в которых расположены средства обработки защищаемой информации;
3.1.5. Рабочие помещения и кабинеты работников Общества, помещения Общества, предназначенные для ведения закрытых переговоров и совещаний; персонал Общества, имеющий доступ к защищаемой информации;
3.1.6. Технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.
3.2. Подлежащая защите информация может:
3.2.1. размещаться на бумажных носителях; существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);
3.2.2. передаваться по телефону, электронной почте и т.п. в виде электрических сигналов.

4. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Под угрозами информационной безопасности понимается потенциальная возможность нарушения главных свойств информации.
4.2. Угрозы информационной безопасности подразделяются на: случайные – стихийные бедствия, ошибки по невниманию, ошибки аппаратных и программных средств и т.д.; преднамеренные, т.е. фальсификация или уничтожение данных, неправомерное использование данных, компьютерные преступления и т.д.
4.3. К числу угроз информационной безопасности относятся (но не ограничены ими):
4.3.1. утрата информации, составляющих коммерческую тайну Общества и иную защищаемую информацию; искажение (несанкционированная модификация, подделка) защищаемой информации;
4.3.2. утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);
4.3.3. несанкционированное использование информационных ресурсов (злоупотребления, мошенничества и т.п.);
4.3.4. недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, активного сетевого

оборудования, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форсмажорных обстоятельств и злонамеренных действий.
4.4. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Общества и его нормальное функционирование:
4.4.1. финансовые потери, связанные с утечкой или разглашением защищаемой информации;
4.4.2. финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
4.4.3. ущерб от дезорганизации деятельности Общества и потери, связанные с невозможностью выполнения им своих обязательств;
4.4.4. ущерб от принятия управленческих решений на основе необъективной информации;
4.4.5. ущерб от отсутствия у руководства Общества объективной информации; ущерб, нанесенный репутации Общества;
4.4.6. иной вид ущерба.

5. МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

5.1. Основными мерами по обеспечению информационной безопасности Общества являются:
1) Административно-правовые и организационные меры;
2) Меры физической безопасности;
3) Программно-технические меры.

5.2. Административно-правовые и организационные меры включают:
1) Контроль исполнения требований законодательства Кыргызской Республики;
2) Разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Порядок;
3) Контроль соответствия бизнес-процессов требованиям Порядка;
4) Информирование и обучение работников Общества работе с информационными системами и требованиям информационной безопасности;
5) Реагирование на инциденты, локализацию и минимизацию последствий;
6) Анализ новых рисков информационной безопасности;
7) Отслеживание и улучшение морально-делового климата в коллективе;
8) Определение действий при возникновении чрезвычайных ситуаций; проведение профилактических мер при приеме на работу и увольнении работников Общества.

5.3. Меры физической безопасности, включают (но не ограничены ими):
1) Оганизацию пропускного и внутриобъектового режимов;
2) Построение периметра безопасности защищаемых объектов;
3) Организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
4) Организацию противопожарной безопасности охраняемых объектов;
5) Контроль доступа работников Общества в помещения ограниченного доступа.

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

1) Использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
2) Использование средств защиты периметра (firewall, IPS и т.п.);
3) Применение комплексной антивирусной защиты;
4) Использование средств информационной безопасности, встроенных в информационные системы;
5) Обеспечение регулярного резервного копирования информации;
6) Контроль за правами и действиями пользователей, в первую очередь, привилегированных;
7) Применение систем криптографической защиты информации;
8) Обеспечение безотказной работы аппаратных средств;
9) Мониторинг состояния критичных элементов информационной системы.

6. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПОРЯДКА

6.1. В Обществе внедрены соответствующие процессы для обеспечения соблюдения требований нормативных правовых актов, соблюдения прав интеллектуальной собственности, защиты охраняемой законом персональной информации, соблюдения ограничений по использованию криптографических средств.
6.2. Все требования и положения международных стандартов являются обязательными для исполнения в области их применения, определяемой соответствующими документами.
6.3. При разработке и применении средств и методов информационной безопасности учитываются требования договорных обязательств и контрактов, заключенных Обществом с третьими сторонами.
6.4. Доступ третьей стороны к информационным ресурсам Общества осуществляется только после анализа рисков, которые могут возникнуть при предоставлении такого доступа, и принятия адекватных защитных мер.
6.5. В случае необходимости (в частности, при наличии требований нормативных правовых актов или международных стандартов), Общество проводит проверку контрагентов (поставщиков товаров и услуг) на соответствие определенным требованиям (например, проверку документов, подтверждающих соответствие предоставляемых услуг требованиям стандарта PCI DSS).
6.6. На основании Порядка разрабатывается ряд подчиненных внутренних нормативных документов, регламентирующих конкретные правила и методы обеспечения информационной безопасности, частные политики в области действия стандартов и т.п.
6.7. Такие документы могут дополнять и расширять требования Порядка, но не могут вступать с ними в противоречие.