УТВЕРЖДАЮ

Генеральный директор
ООО «КОГНИТИВ»

И.А. Полянский

«10» января 2023 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

г. Москва

2023г.

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Политика информационной безопасности (далее - Политика ИБ) ООО «Когнитив» (далее - Общество), представляет собой систему взглядов на обеспечение цифровой устойчивости бизнеса и безопасности информационных активов в информационном пространстве.

Политика ИБ разработана в соответствии с законодательством Российской Федерации, международными стандартами, законодательством стран присутствия, лучших практик в области ИБ.

Действие Политики ИБ распространяется на всех работников Общества, его структурные подразделения, филиалы, представительства.

Политика ИБ является основой для разработки ВНД нижнего уровня в области системы управления и обеспечения ИБ.

Информационные активы Общества имеют ценность для бизнеса и нуждаются в непрерывной защите.

Риски прямого финансового ущерба, прерывания оказания услуг клиентам, ущерба репутации, потери клиентов, применения санкций со стороны государственных регуляторов могут возникнуть в случае успешной реализации даже единичной кибератаки.

Политика ИБ разработана с целью установления общих принципов и правил, определения организационных и управленческих подходов, необходимых для обеспечения и управления ИБ Общества и защиты интересов Общества и его клиентов от угроз в информационном пространстве.

2. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ И УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЩЕСТВА

Система обеспечения и управления ИБ Общества ориентирована на достижение следующих целей:

– обеспечение цифровой устойчивости бизнеса Общества;

– предоставление клиентам безопасных информационных систем;

– определение и обеспечение уровня риска ИБ, необходимого для устойчивого развития Общества.

Для достижения поставленных целей Обществом решаются следующие задачи:

– установка целей в области развития ИБ с учетом разработанной модели угроз, отслеживание текущего состояния ИБ Общества, разработка и периодический пересмотр Плана развития ИБ;

– создание системы управления и обеспечения ИБ на основе риск-ориентированного подхода: принятие управленческих решений в области ИБ по результатам анализа, оценки и обработки рисков ИБ.

– определение приемлемого уровня рисков ИБ, мониторинг текущего уровня рисков и реагирование на превышение установленных ограничений;

– внедрение ИБ в культуру повседневной деятельности работников и клиентов Общества с использованием всех возможных информационных каналов, современных методов и средств обучения;

– обеспечение безопасности периметра Общества, включая современные методы и средства идентификации и аутентификации клиентов и работников;

– обеспечение защиты от утечек информации;

– обеспечение безопасной разработки/внедрения автоматизированных систем;

– организация противодействия различным видам кибермошенничества;

– реализация в Обществе политик и стандартов по управлению и обеспечению ИБ;

– организация необходимого взаимодействия с государственными институтами для обмена информацией об угрозах ИБ и мерах противодействия;

– обеспечение информационной безопасности продуктов (услуг) Общества.

3. КЛАССИФИКАЦИЯ ОБЪЕКТОВ ЗАЩИТЫ

3.1. Объектом защиты в рамках деятельности по обеспечению ИБ являются информационные активы Общества в информационном пространстве, вовлеченные в бизнес-деятельность, а также связанные с ними активы Общества.

– процессы и работники Общества, вовлеченные в обеспечение процессов;

– финансово-аналитическая, служебная, управляющая, персональные данные и т.д.;

– ИТ-инфраструктура: совокупность технологий, оборудования и прикладного/платформенного ПО, обеспечивающая функционирование автоматизированных систем и сервисов, предоставляемых клиентам и работникам Общества.

3.2. Архитектура системы обеспечения информационной безопасности

Объект защиты (информационные активы Общества в информационном пространстве и связанные с ними активы Общества) неоднороден по своему характеру и подлежит декомпозиции на отдельные компоненты, например - сегменты сети (зоны, периметры).

Обеспечение ИБ достигается применением различных организационных и технических мер, сгруппированных в сервисы (подсистемы) ИБ: управление доступом, антивирусная защита, криптографическая защита, контроль и анализ защищенности, регистрация и анализ инцидентов, событий ИБ, обнаружение вторжений и мониторинг активности, резервное копирование, физическая защита и пр.

Архитектура системы обеспечения ИБ представляет собой описание средств защиты, их размещение в корпоративной архитектуре, роли работников и их размещение, учитывает сложность и изменчивость Общества, не ограничивая его бизнес-возможности.

4. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИБ Общества обеспечивается в соответствии со следующими принципами.

Повышение качества и ценности бизнес-продуктов. ИБ создает ценность для бизнеса не только путем предотвращения потерь, но и повышением качества продуктов. В цифровом бизнесе ни один продукт не может быть качественным, если он небезопасен.

Системность. При обеспечении ИБ Общества учитываются все взаимосвязанные, взаимодействующие и изменяющиеся во времени элементы, условия и факторы, значимые с точки зрения ИБ. При создании системы обеспечения ИБ учитываются все слабые и наиболее уязвимые места, а также характер и возможные направления кибератак.

Непрерывность. Обеспечение ИБ Общества представляет собой непрерывно совершенствуемый процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных активов и связанных с ними активов Общества, включая компоненты ИТ-инфраструктуры.

Обоснованность и простота применения средств защиты. Меры по обеспечению ИБ реализуются на современном уровне развития технологий, и должны быть достаточными для защиты от актуальных угроз ИБ, понятными и простыми в применении. Использование средств защиты не может быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе пользователей.

Обязательность контроля. В Обществе обеспечивается обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения ИБ. Осуществление контроля ИТ-архитектуры со стороны ИБ, в том числе регулярный пересмотр архитектуры, прав доступа и требований ИБ. Контроль за деятельностью любого пользователя, ИТ-системы, средства защиты осуществляется на основе применения средств оперативного мониторинга и регистрации событий ИБ и охватывает как несанкционированные, так и санкционированные действия.

Обнаружение и реагирование. Обществом обеспечивается обнаружение и реагирование на угрозы с учетом перехода от "data-центричной" к "человеко-центричной" модели безопасности: мониторинг инцидентов и событий ИБ должен опираться на анализ поведения пользователей и учетных записей.

Соответствие нормативным требованиям. ИБ Общества обеспечивается в соответствии с положениями и требованиями действующих законов, нормативных правовых актов Российской Федерации в области ИБ и ИБ, применимых норм международного права, а также ВНД Общества. Обеспечение ИБ также основывается на применимых отечественных и международных стандартах и нормативно-методических документах органов государственной власти.

Инновационность и развитие компетенций. В Обществе на постоянной основе проводится исследовательская работа по поиску, изучению и реализации в продуктах и услугах оптимальных решений в области ИБ, которая включает:

– использование рекомендаций международных и национальных стандартов;

– изучение передового опыта ИТ-сектора, отраслевого опыта в области современных технологий и решений ИБ;

– адаптацию и внедрение лучших технологий обеспечения ИБ в продукты и услуги Общества.

Совершенствование культуры информационной безопасности. Проводится реализация мер по повышению культуры ИБ работников и клиентов, включая обучение безопасному использованию цифровых сервисов, в том числе пониманию рисков, связанных с использованием цифровых сервисов и размещением в них информации.

Централизация управления. Общество проводит единую политику ИБ.

Идентификация информационных активов (и связанных с ним активов). У каждого актива определяется его владелец, категория обрабатываемой в нем информации, уровень критичности и индивидуальные требования по обеспечению ИБ.

Классификация информации по уровням критичности. Информация, обрабатываемая в Обществе, классифицируется по степени влияния фактов ее разглашения на деятельность Общества и его положение на рынке. Допускается одновременное использование нескольких систем классификации информации.

Минимизация привилегий. Доступ к информационным активам работнику Общества предоставляется в том минимальном объеме, который необходим ему для выполнения трудовых обязанностей.

Персональная ответственность и разделение обязанностей. Ответственность за обеспечение ИБ Общества возлагается на каждого работника в пределах его полномочий. Распределение прав и обязанностей работников строится таким образом, чтобы в случае нарушения круг нарушителей был четко определен.

Разумная достаточность. На всех этапах управления риском ИБ обеспечивается соблюдение баланса между затратами на защиту и получаемым эффектом, в том числе и экономическим, заключающимся в снижении потерь.

Принцип "двух персон". Выполнение критичных операций проводится двумя работниками. Принцип "двух персон" также применяется при изменении критичных параметров ИТ - инфраструктуры, АС и средств защиты информации.

К функционированию и совершенствованию системы обеспечения ИБ применяются подход на основе актуальных угроз и подход на основе требований (обязательных для выполнения правил и условий) ИБ. Меры по обеспечению безопасности активов принимаются по всем идентифицированным видам угроз, связанных с нарушителями ИБ, их уровнем возможностей и используемыми способами (методами) реализации угроз ИБ. ИБ не ограничивается запретительными мерами, но отвечает на актуальные запросы бизнеса, разъясняет возникающие риски и предлагает решения по их минимизации.

5. ОСНОВНЫЕ УЧАСТНИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Генеральный директор

Генеральный директор осуществляет общее руководство системой управления и обеспечения ИБ в Обществе, несет ответственность за организацию ее эффективной работы.

5.2. Подразделение информационной безопасности (далее ПКБ)

5.2.1. Общий функционал ПКБ

Подразделение информационной безопасности выполняет следующие функции[1]:

– разрабатывает и внедряет внутренние нормативные и организационно-распорядительные документы Общества по обеспечению и управлению ИБ;

– разрабатывает требования по обеспечению ИБ на основе анализа актуальных угроз;

– осуществляет разработку, документирование и внедрение процедур реагирования на инциденты ИБ;

– проводит анализ и расследование инцидентов и фактов нарушений ИБ и информирует руководство Общества о результатах проведенных расследований;

– осуществляет формирование системы управления рисками ИБ Общества и ее развитие, в том числе проведение оценки рисков ИБ и регулярный мониторинг и контроль уровня рисков ИБ;[2]

– осуществляет инструментальный контроль и мониторинг текущего состояния ИБ, информирует руководство Общества;

– осуществляет контроль соответствия АС требованиям по обеспечению ИБ на всех стадиях жизненного цикла, от проектирования до снятия с эксплуатации;

– обеспечивает использование средств криптографической защиты информации в соответствии с установленными требованиями;

– эксплуатирует специализированные средства обеспечения безопасности информационных активов Общества и обеспечивает соответствие характеристик данных средств необходимому подразделениям Общества уровню доступности;

– осуществляет мониторинг и контроль выполнения требований по обеспечению ИБ;

– организует повышение осведомленности персонала Общества по вопросам ИБ, разрабатывает учебные материалы;

– проводит консультации работников Общества по вопросам ИБ;

– регулярно (не реже одного раза в полгода) информирует руководство Общества о состоянии ИБ в Обществе, в том числе в составе сводных отчетов;

---

[1] Для осуществления указанных функций, Подразделению информационной безопасности выделяются необходимые кадровые и финансовые ресурсы.

[2] В случае отсутствия отдельного структурного подразделения по рискам ИБ в Обществе

– взаимодействует с представителями правоохранительных органов по вопросам проведения расследований, выполнения компьютерно-технических экспертиз и сбора цифровых доказательств.

5.2.2. DPO Общества

DPO Общества может входить в состав ПКБ. DPO Общества, наделен полномочиями принимать решения в части исполнения требований по обработке и защите ПДн и контролировать их исполнение.

5.3. Подразделение ИТ

Подразделение ИТ выполняет следующие функции:

– обеспечивает настройку и эксплуатацию ИТ-систем Общества (включая коммуникационного оборудования, ОС, СУБД и др.) с соблюдением требований ИБ, разрабатывает внутренние нормативные и организационно-распорядительные документы по защите от ошибок при разработке ПО, от ошибок администраторов ИТ-систем, от сбоев элементов ИТ - инфраструктуры;

– обеспечивает выполнение требований ИБ на всех этапах жизненного цикла АС;

– проводит обновление системного и иного ПО, связанного с устранением критичных уязвимостей;

– обеспечивает доступность информационных активов, обеспечивая работу коммуникационного оборудования, ОС, СУБД, систем доставки и АС, в том числе в условиях отказов и других неблагоприятных событий;

– проводит идентификацию, классификацию информационных активов и обеспечивает поддержание в актуальном состоянии сведений о них;

– ведет Фонд программ и документации Общества[3];

– разрабатывает требования в области технологий, участвует в формировании решений, связанных с организацией процессов Общества, разрабатывает предложения по использованию современных технологий с учетом требований ИБ.

5.4. Самостоятельные структурные подразделения Общества

Самостоятельные структурные подразделения Общества:

– предоставляют информацию ПКБ при обнаружении инцидентов ИБ, потенциальных и реализовавшихся рисков ИБ и оказывают содействие при расследовании причин реализации риска ИБ;

– устанавливают в пределах своей компетенции порядок доступа и правила работы с активами Общества в информационном пространстве, владельцами которых они являются;

– осуществляют первичную идентификацию риска ИБ, участвуют совместно с ПКБ в оценке рисков ИБ в рамках своих компетенций;

---

[3] Указать систему учета Общества (Фонд – пример системы учета ПО, документации)

– учитывают требования и риски ИБ при разработке новых, модификации существующих продуктов и услуг;

– разрабатывают нормативные и распорядительные документы с учетом требований ИБ;

– участвуют в проведении служебных расследований случаев несанкционированного использования АС, мошенничества работников Общества, совершаемого с использованием АС Общества, а также инцидентов ИБ в АС;

– обеспечивают содействие ПКБ в части допуска на объекты и передачу информации, необходимой для выполнения функциональных обязанностей;

– взаимодействуют с территориальными органами государственной власти по вопросам ИБ[4], в пределах своей компетенции;

– взаимодействуют с Управлением внутреннего аудита и ПКБ по результатам проверок выполнения требований по обеспечению ИБ.

5.5. Руководители самостоятельных структурных подразделений

Руководители самостоятельных структурных подразделений:

– несут персональную ответственность за доведение до работников требований ИБ и состояние системы обеспечения ИБ в подчиненном подразделении, включая обеспечение безопасности обрабатываемых персональных данных;

– осуществляют руководство работой по обеспечению ИБ в подразделении, обеспечивают выполнение работниками подразделения требований ИБ;

– принимают решения о предоставлении прав доступа работникам подчиненного подразделения к информации, согласовывают эти решения в установленном порядке;

– принимают решения о предоставлении прав доступа к информации, владельцем которой является подразделение, работникам других подразделений по обращению руководителей этих подразделений, согласовывают эти решения в установленном порядке;

– определяют категории информации, владельцем которой является подразделение;

– назначают ответственного за действия работников сторонней организации в корпоративной сети Общества (при заключении по инициативе подразделения договора со сторонней организацией);

– несут ответственность за действия работников сторонней организации в корпоративной сети Общества (при отсутствии назначенного ответственного);

– взаимодействуют с ПКБ по вопросам организации системы обеспечения ИБ в подразделении.

– утверждают решение о стратегии реагирования на риск ИБ в зоне своей ответственности.

---

[4] При соответствующем указании со стороны ПИБ

5.6. Пользователи корпоративных АС и сервисов

Пользователи обязаны:

– знать и соблюдать требования Политики ИБ и других ВНД по обеспечению ИБ в части, их касающейся;

– использовать каналы связи Общества, ПО и оборудование только в целях выполнения трудовых обязанностей;

– выполнять установленные требования по обеспечению ИБ при работе с информацией, АС и корпоративными ИТ-сервисами.

– незамедлительно докладывать руководителю подразделения и ПКБ о нарушениях информационной безопасности.

6. СИСТЕМА УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Система обеспечения ИБ представляет собой совокупность правовых, организационных и технических мер, направленных на предотвращение или снижение ущерба активам Общества от последствий реализации рисков ИБ[5].

Ее основными составляющими являются:

– нормативные документы и процессы Общества в области ИБ;

– персонал, вовлеченный в обеспечение ИБ;

– комплекс технических средств, механизмов и технологий защиты информации.

6.1. Нормативные документы и процессы Общества в области ИБ

6.1.1. Документирование мероприятий по управлению и обеспечению информационной безопасности

Документирование мероприятий по управлению и обеспечению ИБ осуществляется в объеме, необходимом и достаточном для достижения целей и задач настоящей Политики.

Внутренние нормативные документы Общества и другие материалы в области ИБ размещаются в помещении архива.

6.1.2. Соответствие требованиям законодательства и стандартов

Порядок обеспечения ИБ Общества соответствует положениям и требованиям действующих законов и нормативных правовых актов Российской Федерации, а также

---

[5] Управление риском ИБ осуществляется в отношении активов, которые подразделяются на:

1) первичные активы - информация и бизнес-процессы;

2) активы поддержки (вторичные активы) - аппаратные средства, программное обеспечение, сети, персонал, снабжение, обеспечивающие процессы.

применимым нормам международного права. Общество руководствуется национальными и международными стандартами и лучшими практиками в области управления и обеспечения ИБ и ИБ. Система обеспечения ИБ учитывает изменения требований законодательства, рекомендаций национальных и международных стандартов в области ИБ и ИБ.

Безопасность АС, обрабатывающих данные платежных карт, обеспечивается в соответствии с требованиями международного стандарта PCI DSS.

6.1.3. Идентификация угроз, нарушителей и рисков информационной безопасности

В целях реализации эффективной системы обеспечения ИБ в Обществе осуществляется деятельность по управлению риском ИБ, направленной на устранение рисков и обеспечивающей интеграцию принятия решений, основанных на рисках, в процесс функционирования и совершенствования системы обеспечения ИБ.

В рамках управления риском ИБ устанавливается контекст, происходит идентификация и оценка риска, осуществляется реагирование на риски ИБ и мониторинг на постоянной основе с учетом установленной системы лимитов и ограничений в Обществе.

В рамках идентификации рисков проводится определение активов, входящих в область оценки, осуществляется идентификация угроз ИБ и связанных с ними уязвимостей, а также существующих мер защиты и определяется временной горизонт. Перечень актуальных угроз и уязвимостей для рассматриваемого актива или группы активов определяется на основе модели угроз организации и экспертного анализа области оценки.

6.1.4. Управление доступом к информационным активам

Ограничение круга лиц и технологических процессов, имеющих доступ к информационным активам, обеспечивается на уровне прав пользователей и на уровне сети.

Предоставление доступа к АС Общества на уровне прав пользователей осуществляется согласно назначенным типовым ролям.

Процедура управления доступом на уровне прав пользователей является сквозной и непрерывной, и длится от момента приема работника на работу до момента его увольнения.

Перед использованием АС пользователь обязан идентифицировать себя с помощью уникального идентификатора пользователя (логина). Идентификатор однозначно идентифицирует пользователя и должен соответствовать принятым правилам именования учетных записей в Обществе. Использование информационных систем под чужим идентификатором (логином) категорически запрещено. Пользователь несет персональную ответственность за любые действия, совершенные с использованием его учетной записи.

Привилегированный доступ (уровень доступа, предоставляющий полномочия по изменению всех параметров конфигурации, либо параметров безопасности системы, предоставления прав административного, операторского или пользовательского доступа к информационным системам, изменения, удаления всех данных в информационных ресурсах) предоставляется исключительно для выполнения задач, в которых необходим соответствующий уровень доступа. Для каждого информационного ресурса составляется и

поддерживается в актуальном состоянии реестр административных учетных записей. Привилегированный доступ к информационным ресурсам должен пересматриваться на регулярной основе.

Защищенный удаленный доступ к информационным ресурсам Общества через сеть Интернет предоставляется тем работникам Общества, которым он необходим для выполнения своих трудовых обязанностей. При этом предоставление удаленного доступа прекращается по истечении такой необходимости.

Работникам Общества предоставляется доступ к ресурсам сети Интернет в рамках выполнения ими трудовых обязанностей.

Ключевыми мерами по управлению доступом на сетевом уровне является защита периметра корпоративной сети и зонирование/сегментирование внутри сети. Хранение информации во внутренней или во внешней сети определяется ее критичностью. Разграничение доступа на уровне сети выполняется средствами межсетевого экранирования (в том числе соответствующими встроенными механизмами сетевых маршрутизаторов).

Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными процедурами.

В Обществе используется набор механизмов и методов, позволяющих обеспечить аутентификацию, авторизацию и разграничение при доступе к информационным активам.

6.1.5. Безопасная разработка информационных продуктов

ОИБ совместно с другими заинтересованными подразделениями Общества осуществляют оценку рисков ИБ на всех стадиях разработки и внедрения продуктов и услуг, начиная с самых ранних этапов (подготовка концепции), анализ соблюдения требований ИБ, регламентированных ВНД Общества, а также принятие адекватных мер противодействия.

Информационные услуги предоставляются с оптимальным уровнем безопасности "по умолчанию" (обеспечивающим защищенность от актуальных угроз ИБ). Данный уровень определяется для каждой услуги индивидуально в процессе взаимодействия подразделений Общества.

При создании информационных продуктов необходимо предусматривать возможность перехода в "красную тактику" - заранее согласованные владельцем бизнес-продукта и ОИБ дополнительные меры по управлению риском (временное ограничение функциональности продукта, изменение уровня предоставляемого сервиса т.п.) как ответ на повышение уровня риска ИБ свыше установленного порога.

Безопасность программного кода ПО Общества обеспечивается на всех стадиях жизненного цикла. Это достигается путем:

- использования специализированных систем и процедур контроля на наличие ошибок и недокументированных возможностей;

- контроля за внедрением ПО для АС Общества (включая критичные АС) и внесением в него изменений, контроля целостности кода в процессе эксплуатации.

6.1.6. Обеспечение непрерывности бизнеса

В Обществе реализуются технические, технологические и организационные мероприятия, направленные на обеспечение непрерывности бизнеса. Непрерывность бизнеса заключается в выполнении Обществом в условиях чрезвычайных ситуаций (экономических и политических кризисов, природных и техногенных катастроф, пандемии, террористических угроз и т.д.) на минимально необходимом уровне функций, без которых деятельность Общества невозможна.

Мероприятия по обеспечению непрерывности включают в себя создание процедур резервирования и восстановления функций Общества, в том числе для чрезвычайных ситуаций невысокой вероятности возникновения. Необходимость резервирования и восстановления функций определяется оценкой ущерба от их прерывания.

Непрерывность бизнеса подразумевает также обеспечение непрерывности и надежности средств защиты. Надежность средств защиты не должна быть меньше надежности защищаемой системы; данные показатели определяются лицами, ответственными за обеспечение функционирования средств защиты и защищаемой системы.

6.1.7. Управление инцидентами информационной безопасности

Управление инцидентами ИБ является важным процессом и осуществляется в целях минимизации ущерба, вызванного реализованной угрозой ИБ, максимально быстрого устранения последствий кибератак, консолидации статистики по инцидентам ИБ, выявления причин возникновения инцидентов и принятия упреждающих мер по исключению подобных ситуаций в будущем.

Каждый работник Общества, допущенный к работе с корпоративными АС, обязан знать признаки инцидента ИБ. Для этого организуется необходимое обучение или инструктаж пользователей.

О возникновении инцидента ИБ (в т.ч. подозрении на него) каждый работник Общества обязан незамедлительно сообщить в ОИБ.

6.1.8. Мониторинг, контроль и ответственность

В Обществе осуществляется постоянный мониторинг и контроль работы системы обеспечения ИБ, по результатам которого проводится анализ эффективности принятых мер обеспечения ИБ, планируются и внедряются дополнительные меры защиты с учетом изменений ИТ-среды, появления новых угроз, инцидентов и проблем. Функции контроля работы системы обеспечения ИБ реализуются ОИБ.

В Обществе на систематической основе проводится контроль системы управления и обеспечения ИБ как со стороны Управления внутреннего аудита Общества, так и со стороны внешних аудиторов. Результаты проведения мониторинга учитываются при совершенствовании систем управления и обеспечения ИБ.

Обеспечение ИБ затрагивает каждого работника Общества, использующего его активы, и накладывает на него обязанности и ограничения, направленные на сохранность активов.

Особым видом контроля соблюдения требований по обеспечению ИБ является выявление и предотвращение утечек конфиденциальной информации, реализуемое на техническом уровне.

Применяемые инструментальные средства контроля и обеспечения ИБ не предоставляют доступ работникам, ответственным за их эксплуатацию, непосредственно к критичной информации Общества.

Ответственность за нарушение требований по обеспечению ИБ возлагается непосредственно на работников, допустивших нарушения, и на руководителя подразделения, в котором нарушения допущены. Вид ответственности (материальная, дисциплинарная, административная, уголовная) определяется составом допущенного умышленно или неумышленно (в том числе по халатности, из-за невнимательности) нарушения.

6.2. Персонал, вовлеченный в обеспечение информационной безопасности

6.2.1. Обучение и повышение осведомленности по вопросам обеспечения информационной безопасности

Одним из ключевых направлений деятельности по обеспечению ИБ в Обществе является повышение осведомленности работников по вопросам ИБ:

- ведение разъяснительной работы о значимости обеспечения ИБ, информирование пользователей ресурсов Общества об актуальных угрозах ИБ, правилах "компьютерной гигиены", в том числе путем подготовки мультимедийных и печатных обучающих материалов;
- ежегодное обязательное обучение работников и тестирование на знание политики и процедур обеспечения ИБ;
- включение в обучение пользователей независимых тестов реакции на методы социальной инженерии;
- поощрение лиц, сообщающих об уязвимостях в продуктах и сервисах Общества;
- формирование единой культуры ИБ и риск-культуры у работников Общества.

В целях поддержания высокой профессиональной квалификации и уровня компетенций в Обществе обеспечивается систематическое обучение работников ИБ на профильных курсах. Общество предоставляет возможность специалистам в области ИБ посещать российские и международные выставки и конференции, а также совершать референс-визиты для получения сведений о последних достижениях в области обеспечения ИБ и обмена опытом в профессиональном сообществе. Планирование обучения и повышения профессиональной квалификации работников ИБ возлагается на руководителя кадровой службы.

Помимо повышения осведомленности собственных работников, Общество осуществляет деятельность по повышению осведомленности клиентов путем их информирования при пользовании каналами обслуживания, по организации для клиентов обучающих игр (геймификация), по формированию у клиентов современной культуры ИБ.

6.3.Комплекс технических средств, механизмов и технологий защиты информации

6.3.1. Общие сведения

Для обеспечения ИБ в Обществе применяется комплекс технических средств, механизмов и технологий защиты информации, в состав которого входят специализированные устройства и ПО, средства мониторинга, встроенные механизмы защиты ОС, СУБД, АС (приложений), телекоммуникационного оборудования и других устройств.

Управление техническими средствами и механизмами защиты информации осуществляют (в зоне своей ответственности) ОИБ и подразделения ИТ.

Технические решения в области ИБ создаются в рамках проектной деятельности и проходят все стадии разработки, включая оценку с последующим учетом в финансово-экономическом обосновании проекта, разработку и реализацию проектных решений, тестирование, опытную эксплуатацию, приемку и передачу в промышленную эксплуатацию.

На этапе создания любой АС или продукта к нему предъявляются требования со стороны ОИБ; данные требования должны быть реализованы при помощи технических средств и механизмов и/или организационных мер. Переход по этапам жизненного цикла всех АС Общества (в том числе ввод в опытную, промышленную эксплуатацию, вывод из эксплуатации) происходит по согласованию с ОИБ.

Для отдельных сервисов и систем ОИБ разрабатываются частные политики ИБ и модели угроз.

6.3.2. Защита периметра корпоративной сети

Защита периметра является обязательным элементом системы обеспечения ИБ корпоративной сети и включает в себя шлюзы безопасности, средства межсетевого экранирования (FW), организацию виртуальных частных сетей (VPN), системы обнаружения и предотвращения вторжений (IDS/IPS).

6.3.3. Защита от вредоносного программного обеспечения

Защита от вредоносного ПО реализуется как на уровне прикладных информационных потоков и централизованных сервисов, так и на уровне отдельных компьютеров. В Обществе применяются меры по борьбе с вредоносным ПО, создаваемым, в том числе, для реализации целенаправленных атак (Advanced Persistent Threat, APT).

6.3.4. Использование средств криптографической защиты информации

Для обеспечения конфиденциальности критичной информации при передаче по каналам связи и хранении за пределами защищенного периметра, а также в иных требующих этого случаях, применяется шифрование.

Средства криптографической защиты информации применяются в соответствии с действующей нормативно - правовой базой в этой области.

Для обеспечения аутентичности и/или целостности критичной информации применяется электронная подпись (ЭП). В зависимости от ситуации могут применяться простая ЭП (PIN-код, одноразовый пароль), неквалифицированная либо квалифицированная ЭП. Могут применяться и другие механизмы, установленные внешними и внутренними требованиями.

6.3.5. Использование облачных технологий и личных мобильных устройств

Использование облачных технологий и личных мобильных устройств рассматривается Обществом как объективная реальность и возможность повышения эффективности основной деятельности. Вместе с тем, учитывая повышенные риски использования этих технологий, необходимо принятие дополнительных мер обеспечения ИБ.

Хранение (в том числе кратковременное) информации Общества на ресурсах, не принадлежащих Обществу, в обязательном порядке согласуется с ОИБ.

Общество устанавливает ограничения и требования по безопасному использованию личных мобильных устройств (принцип "BYOD - Bring Your Own Device").

6.3.6. Защита от DDoS-атак

Постоянная доступность сервисов для клиентов - важный приоритет в деятельности подразделений ИТ и ИБ. Для защиты от распределенных атак отказа в обслуживании (DDoS) Обществом принимаются и наращиваются специальные меры, направленные на обеспечение постоянной защиты в режиме 24/7, расфокусировку массированных атак, работу с провайдерами, обеспечивающими очистку трафика.

6.3.7. Система выявления и предотвращения кибермошенничества

6.3.7.1.Выявление и предотвращение кибермошенничества

Деятельность Общества по противодействию кибермошенничеству ведется в отношении собственных недобросовестных работников, недобросовестных клиентов, а также в отношении злоумышленников, не являющихся клиентами Общества. Для этого в Обществе внедрена и непрерывно совершенствуется система фрод-мониторинга, нацеленная на снижение уровня убытков от мошенничества и безопасное развитие АС Общества в условиях роста рисков ИБ.

6.3.8. Комплекс организационных мер обеспечения информационной безопасности

6.3.8.1.Общие сведения

Организационные меры обеспечения ИБ направлены на регламентирование функционирования ИТ-систем и средств защиты информации, использования информационных активов Общества, организацию деятельности персонала и взаимодействия подразделений, разработку и поддержание в актуальном состоянии ВНД по ИБ.

Применение несогласованных с ОИБ технических решений и организационных мер в целях обеспечения ИБ не допускается.

6.3.8.2.Безопасное использование программного обеспечения

В Обществе допускается к использованию только официально приобретенное или созданное своими силами ПО, прошедшее тестирование и размещенное в Фонде программ и документации (находится в ведении подразделения ИТ, см. п. 5.5 настоящей Политики).

Установка и использование свободно распространяемого, условно бесплатного ПО допускается только при условии отсутствия в нем уязвимостей, а также добавления ПО в Фонд программ и документации Общества установленным порядком или закачивания в официальные репозитории Общества установленным порядком, за исключением случаев, согласованных ОИБ.

Оперативное управление ПО (установка и настройка ПО, установка пакетов обновлений, актуализация лицензий, хранение и учет эталонных копий ПО) возлагается на специалистов подразделения ИТ и ОИБ (в части, касающейся обслуживания технических средств защиты информации).

Безопасное использование ПО работниками Общества обеспечивается выполнением требований, ограничивающих возможности пользователей по произвольному обращению с ПО. Установка ПО на компьютеры пользователей осуществляется только уполномоченными работниками Общества по заявке, поданной в установленном порядке. Аналогичные требования действуют в отношении внесения изменений в настройки ПО (за исключением индивидуальных настроек графических интерфейсов и прочих параметров, не влияющих на функциональность ПО).

В Обществе обеспечивается своевременное обновление ОС и прикладного ПО на рабочих станциях и серверах путем установки соответствующих программных пакетов, выпускаемых компаниями-разработчиками.

В Обществе запрещается использование коммерческого ПО, не обслуживаемого компаниями - разработчиками (отказ в разработке и публикации обновлений безопасности ПО). Вывод из эксплуатации не обслуживаемого ПО возлагается на специалистов подразделения ИТ и ОИБ (в части, касающейся обслуживания технических средств защиты информации).

6.3.8.3.Обращение с носителями информации

В целях предотвращения несанкционированного разглашения, модификации или уничтожения хранимой на съемных носителях информации в Обществе устанавливаются ограничения на использование таких носителей. Запрещено подключение съемных носителей информации к средствам вычислительной техники, включенным во внутреннюю производственную сеть Общества.

К внешней производственной сети подключение съемных носителей допускается. Работники Общества, которым разрешено использование съемных носителей информации, подключаемых к внешней производственной сети Общества, должны выполнять требования по безопасной работе с указанными носителями, в том числе, для предотвращения рисков ИБ при утере или хищении носителей информации.

В Обществе ведется учет съемных носителей, предназначенных для хранения информации.

При транспортировании носителей информации принимаются меры по их защите от несанкционированного доступа или повреждения. Данные, передаваемые на съемных носителях (CD, DVD, USB и т.д.), защищаются принятыми в Обществе методами и средствами.

При выводе из эксплуатации компьютеров, серверов, систем хранения данных и иного оборудования, в составе которых имеются машинные носители информации, производится процедура гарантированного уничтожения данных.

6.3.8.4.Передача функций на аутсорсинг

При передаче функций на аутсорсинг обеспечивается принятие контрагентами мер обеспечения ИБ, аналогичных мерам, принимаемым Обществом. При заключении договоров и соглашений включаются требования выполнения стандартов ИБ Общества, осуществляется контроль соблюдения требований в течение всего периода оказания услуг. Порядок взаимодействия и распределения ответственности определяется договором между Обществом и контрагентом. Начало оказания услуг Обществу по схеме аутсорсинга предваряется экспертизой со стороны ОИБ принятых организационных и технических мер обеспечения ИБ. При отрицательном заключении экспертизы оказание услуг не допускается.

6.3.8.5.Взаимодействие с контрагентами

При организации взаимодействия с контрагентами до начала взаимного обмена конфиденциальной информацией необходимо заключить в установленном в Обществе порядке соглашение о неразглашении конфиденциальной информации (non-disclosure agreement, NDA).

В договоры со сторонними организациями, предусматривающими передачу информации ограниченного доступа, в обязательном порядке включаются соответствующие требования неразглашения коммерческой тайны, персональных данных

клиентов и работников Общества. Производится обязательное ознакомление с указанными требованиями работников привлекаемых сторонних организаций, оказывающих услуги.

Персоналу привлекаемых сторонних организаций запрещен доступ к информации, подлежащей защите в соответствии с действующим законодательством, запрещен административный доступ к средствам вычислительной техники, обеспечивающим обработку указанной информации. Доступ к тестовым средам Общества обеспечивается только при использовании технических решений, исключающих копирование данных на локальные носители (жесткие диски, съемные носители и др.).

В случае, если взаимодействие с контрагентом предполагает его допуск к работе в корпоративной сети Общества, руководитель самостоятельного структурного подразделения, по инициативе которого организовано взаимодействие с контрагентом, назначает ответственного за контроль действий работников сторонней организации во внутренней корпоративной сети.

На уровне системы обеспечения ИБ могут приниматься дополнительные меры по регистрации и мониторингу действий работников сторонней организации в корпоративной сети Общества.

6.3.8.6.Взаимодействие с государственными органами

ОИБ проводятся мероприятия по обеспечению деятельности Общества в соответствии с законодательными требованиями в области ИБ и ИБ, выстраиваются отношения с государственными органами по вопросам обеспечения ИБ.

6.3.8.7.Взаимодействие со специальными группами

ОИБ поддерживает взаимодействие со специальными группами (комитетами, ассоциациями и др.) включая Центры компетенций по вопросам развития ИБ. Задачами такого взаимодействия являются получение и передача информации:

- о лучших практиках в области ИБ и ИБ, о перспективных технологиях и методиках;
- о новых угрозах и уязвимостях;
- об изменениях в законодательстве, в национальных и международных стандартах в области ИБ и ИБ.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Развитие систем управления и обеспечения ИБ Общества и повышение их эффективности достигается путем совершенствования Политики ИБ, других внутренних нормативных документов Общества в области ИБ, своевременного и должного использования результатов внутренних и внешних аудитов, анализа инцидентов и событий ИБ, лучших мировых практик.

Руководство Общества и коллегиальные органы на регулярной основе рассматривают отчеты о состоянии ИБ в подразделениях Общества и о фактах нарушений установленных требований, а также общие и частные вопросы ИБ, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы.

Плановый пересмотр Политики ИБ проводится не реже, чем раз в 3 (три) года.

Внеплановый пересмотр Политики ИБ должен проводиться:

- в случае планирования изменений системы управления и обеспечения ИБ;
- в случаях изменения действующего законодательства РФ и требований органов государственной власти;
- по результатам оценки мониторинга и контроля состояния ИБ или реализации угроз ИБ.

ПРИЛОЖЕНИЕ 1

Список терминов и определений

Активы – для целей настоящей Политики под активами Общества подразумеваются информация, а также бизнес-процессы, бизнес-приложения, программное обеспечение, аппаратные средства, сети, персонал Общества, обеспечивающие процессы, сервисы.

Внешняя сеть - внешний сегмент корпоративной сети, из которого допускается взаимодействие пользователей и информационных систем с сетью Интернет.

Внутренняя сеть - внутренний защищенный сегмент корпоративной сети, в котором размещаются критичные для бизнеса системы и ПК пользователей, выполняющих операции в данных системах. Внутренняя сеть изолирована от взаимодействия с сетью Интернет.

Информационная безопасность - обеспечение конфиденциальности, целостности и доступности информации. В зависимости от контекста, данное понятие может включать в себя также свойство сохранять аутентичность, подотчетность, неотказуемость авторства и надежность.

Информационные активы - информация (платежная, финансово-аналитическая, служебная, управляющая, персональные данные, иная информация). Совместно с информационными активами, рассматриваются иные активы Общества, необходимые для получения, хранения, обработки, передачи информации.

Инцидент информационной безопасности - реализованная угроза в информационном пространстве; любое непредвиденное или нежелательное событие, которое может нарушить бизнес-процесс или состояние защищенности актива.

Кибермошенничество - хищение или попытка хищения денежных средств с использованием электронных средств платежа без согласия клиента.

Киберпространство - информационное пространство, образованное совокупностью телекоммуникационных сетей и оборудования, средств вычислительной техники и программного обеспечения, а также деятельностью человека по его информационному наполнению.

Неотказуемость авторства - неотказуемость от авторства информации, а также факте ее изменения, отправки, получения и пересылки.

Подразделение информационной безопасности - структурное подразделение в составе компании, осуществляющее деятельность по обеспечению и управлению информационной безопасностью согласно положению о подразделении.

Риск - возможность возникновения одного или нескольких событий с неблагоприятными последствиями.

Риск ИБ – риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения ИБ, в том числе проведения технологических и

других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности организации.

Руководство Компании – Генеральный директор.

Самостоятельное структурное подразделение - структурное подразделение Общества.

Система обеспечения информационной безопасности - совокупность правовых, организационных и технических мер, направленных на предотвращение или снижение ущерба информационным активам организации и ее клиентов от последствий реализации рисков информационной безопасности.

Специальные группы – ассоциации, комиссии, рабочие группы и другие объединения внешних по отношению к Обществу физических, юридических лиц и государственных органов.

Угроза - потенциально возможное событие, действие (воздействие), которое может нарушить бизнес-процесс или состояние защищенности актива.

Цифровая устойчивость - способность Общества к нормальному функционированию и развитию в условиях постоянно реализующихся рисков информационной безопасности; обеспечивается благодаря непрерывной готовности Общества к применению защитных и ответных мер реагирования на кибератаки и оперативному восстановлению в случае их реализации.

Шлюз безопасности - Программно-аппаратное средство, точка соединения между сегментами сетей, предназначенная для защиты сетевой инфраструктуры Общества.

ПРИЛОЖЕНИЕ 2

Перечень сокращений

АС	-	Автоматизированная система;
ВНД		Внутренний нормативный документ;
ДКБ	-	Департамент информационной безопасности;
ИБ	-	Информационная безопасность;
ИТ	-	Информационные технологии;
ОС	-	Операционная система;
ПО	-	Программное обеспечение;
ОИБ	-	Подразделение ИБ Общества
СУБД	-	Система управления базами данных;
ЭП	-	Электронная подпись;
DPO	-	Data Protection Officer
NDA	-	Non-disclosure agreement, соглашение о неразглашении конфиденциальной информации;
PCI DSS	-	Payment Card Industry Data Security Standard, стандарт безопасности платежных карт

ПРИЛОЖЕНИЕ 3

Перечень ссылочных документов

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" N 149-ФЗ от 27.07.2006.
2. Федеральный закон "О персональных данных" N 152-ФЗ от 27.07.2006.
3. Федеральный закон "О коммерческой тайне" N 98-ФЗ от 29.07.2004.
4. Федеральный закон "Об электронной подписи" N 63-ФЗ от 06.04.2011.
5. The Payment Card Industry Data Security Standard (PCI DSS).
6. ISO/IEC 27001: 2013. Information technology - Security techniques - Information security management systems - Requirements.
7. Устав Общества.
8. NIST Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View (March 2011);
9. ISO/IEC 31000:2018. Risk management – Principles and guidelines;
10. ISO/IEC 27005: 2011. Information technology - Security techniques - Information security risk management.