DeloPorts
ГРУППА КОМПАНИЙ «ДЕЛО»

УТВЕРЖДЕН
приказом ООО «ДелоПортс»
от «09» сентября 2022 г. № 46

Генеральный директор
ООО «ДелоПортс»

_____ И.А. Яковенко

ПОЛИТИКА
В ОБЛАСТИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ООО «ДЕЛОПОРТС»
(редакция №1)

город Новороссийск
2022 г.

Содержание:

1. ВВЕДЕНИЕ

1.1. Настоящая Политика в области управления информационной безопасностью ООО «ДелоПортс» (далее- Политика) является основополагающим документом, регулирующим деятельность Общества с ограниченной ответственностью «ДелоПортс» в области информационной безопасности.

1.2. Политика является локальным нормативным актом Общества с ограниченной ответственностью «ДелоПортс», входящего в Группу компаний «Дело», определяющим ключевые требования к организации системы правления информационной безопасностью.

1.3. Данная Политика разработана в соответствии с требованиями законодательства РФ и положениями международного стандарта ISO/IEC 27001:2013.

1.4. Группа компаний «Дело» (далее - ГК «Дело), являющаяся крупнейшим в России транспортно-логистическим холдингом, проводит политику осуществления всех необходимых мер для обеспечения информационной безопасности в соответствии с требованиями действующего законодательства.

1.5. ООО «УК «Дело» (далее – УК Дело) - головная компания Группы компаний «Дело».

1.6. ООО «ДелоПортс» (далее также - ДелоПортс) - стивидорный холдинг, объединяющий крупнейшие контейнерный и зерновой терминалы на российском черноморском побережье, а также Сервисную Компанию «Дело», предоставляющую услуги буксировки и агентирования (далее также - подконтрольные активы):

ООО «Контейнерный терминал «НУТЭП» (ООО «НУТЭП») – современный глубоководный контейнерный терминал, осуществляющий перевалку контейнерных, генеральных и Ро-Ро грузов в порту Новороссийск,

АО «Зерновой терминал «КСК» (АО «КСК») - глубоководный зерновой терминал, осуществляющий перевалку насыпных генеральных и Ро-Ро грузов в порту Новороссийск,

ООО «Сервисная компания «Дело» (ООО СК «Дело») - компания, оказывающая услуги по буксировке, агентированию и бункеровке судов в порту Новороссийск.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Данная Политика распространяется на все регионы деятельности и на все подконтрольные активы ДелоПортс, присоединившиеся к действию настоящей Политики, в том числе на всю информацию и ресурсы обработки информации. Все сотрудники ДелоПортс и подконтрольных активов, присоединившихся к действию настоящей Политики, обязаны соблюдать настоящую Политику.

2.2. Присоединение подконтрольных активов к действию настоящей Политики либо введение в действие собственных локальных нормативных актов с

учётом норм и требований настоящей Политики осуществляется на основании решения уполномоченного органа управления/приказа исполнительного органа такой компании в соответствии с установленным у неё порядком утверждения и введения в действие локальных нормативных актов.

2.3. Здесь и далее при упоминании по тексту настоящей Политики, под подконтрольными активами подразумеваются подконтрольные активы ДелоПортс, присоединившиеся к действию настоящей Политики в порядке, установленном п.2.2. настоящей Политики.

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Бизнес-процесс – последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности ДелоПортс и подконтрольных ему активов.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Доступность информации – состояние, характеризуемое способностью информационной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

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

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность (ИБ) – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

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

Инцидент – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Инцидент информационной безопасности – одно или серия нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу информационной безопасности.

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы,

избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – состояние защищённости информации, характеризуемое способностью информационной системы обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Привилегии – это права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.

Риск – сочетание вероятности события и его последствий.

Руководство – работники ДелоПортс и подконтрольных ему активов, имеющие непосредственное подчинение исполнительному органу компании, либо руководители структурных подразделений такой компании.

СУИБ – система управления информационной безопасностью, часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

Угроза – опасность, предполагающая возможность потерь (ущерба).

Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

4. ЦЕЛИ И ЗАДАЧИ

4.1. В области управления информационной безопасностью ДелоПортс и подконтрольных ему активов устанавливаются следующие стратегические цели:

4.1.1. защита конкурентных преимуществ ДелоПортс от угроз в области информационной безопасности;

4.1.2. соответствие требованиям законодательства, отраслевым нормам и договорным обязательствам в части информационной безопасности;

4.1.3. эффективное управление информационной безопасностью и непрерывное совершенствование системы управления информационной безопасностью;

4.1.4. достижение адекватности мер по защите от угроз информационной безопасности;

4.1.5. обеспечение безопасности активов ГК Дело, включая персонал, материально-технические ценности, информационные ресурсы, бизнес-процессы.

4.2. Система управления информационной безопасностью ДелоПортс и подконтрольных ему активов призвана решать следующие задачи:

4.2.1. **Вовлечение руководства ДелоПортс и подконтрольных ему активов в процесс обеспечения информационной безопасности:** деятельность по обеспечению информационной безопасности инициирована и контролируется руководством ДелоПортс и подконтрольных ему активов.

4.2.2. **Соответствие требованиям законодательства РФ:** ДелоПортс и подконтрольные ему активы реализуют меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством, отраслевыми нормами и договорными обязательствами.

4.2.3. **Согласованность действий по обеспечению информационной, физической и экономической безопасности:** действия по обеспечению информационной, физической и экономической безопасности осуществляются на основе четкого взаимодействия заинтересованных подразделений ДелоПортс и подконтрольных ему активов и согласованы между собой по целям, задачам, принципам, методам и средствам.

4.2.4. **Применение экономически целесообразных мер:** ДелоПортс стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации.

4.2.5. **Документированность требований информационной безопасности:** в ДелоПортс все требования в области информационной безопасности фиксируются в разрабатываемых внутренних нормативных документах.

4.2.6. **Повышение осведомленности в вопросах обеспечения информационной безопасности:** документированные требования в области информационной безопасности доводятся до сведения работников всех структурных подразделений ДелоПортс и контрагентов в части их касающейся.

4.2.7. **Реагирование на инциденты информационной безопасности:** ДелоПортс ведёт систематизированную работу по выявлению, учету и оперативному реагированию на действительные, предпринимаемые и вероятные нарушения информационной безопасности.

4.2.8. **Оценка рисков:** в ДелоПортс на постоянной основе реализуются мероприятия по оценке и управлению рисками информационной безопасности, повышению уровня защищенности информационных активов.

4.2.9. **Учет требований информационной безопасности в проектной деятельности:** ДелоПортс учитывает требования информационной безопасности в проектной деятельности. Разработка и документирование требований по обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации.

4.2.10. **Постоянное совершенствование системы управления информационной безопасностью:** совершенствование системы управления информационной безопасности является непрерывным процессом.

5. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. В ДелоПортс и подконтрольных ему активах применяются следующие принципы обеспечения информационной безопасности:

5.1.1. **Системность** - в ГК Дело ДелоПортс и подконтрольные ему активы рассматриваются как взаимосвязанные и взаимовлияющие компоненты единой системы. Система защиты строится с учетом известных каналов получения несанкционированного доступа к информации и возможности появления принципиально новых путей реализации угроз безопасности.

5.1.2. **Коллективная защита** - реагирование на угрозы и инциденты информационной безопасности осуществляется коллективно всеми подразделениями кибербезопасности активов, подконтрольных ДелоПортс.

Координатором и центром компетенций выступает ДелоПортс.

5.1.3. **Полнота (комплексность)** - для обеспечения информационной безопасности используется широкий спектр мер, методов и средств защиты информации. Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающих все существующие каналы угроз и не содержащих слабых мест на стыках отдельных ее компонентов.

5.1.4. **Эшелонированность** - система обеспечения информационной безопасности стоится таким образом, чтобы наиболее защищаемая зона безопасности находилась внутри других защищаемых зон.

5.1.5. **Непрерывность** - в ДелоПортс и подконтрольных ему активах обеспечение информационной безопасности является непрерывным целенаправленным процессом, предполагающим принятие соответствующих мер на всех этапах жизненного цикла активов.

5.1.6. **Разумная достаточность** - выбор средств защиты активов ДелоПортс и подконтрольных ему активов, адекватных реально существующим угрозам (т.е. обеспечивающих допустимый уровень возможного ущерба в случае реализации угроз), осуществляется на основе проведения анализа рисков.

5.1.7. **Законность** - при выборе и реализации мер и средств обеспечения информационной безопасности ДелоПортс и подконтрольных ему активах строго соблюдается законодательство Российской Федерации, требования нормативных правовых и технических документов в области обеспечения информационной безопасности ДелоПортс и подконтрольных ему активов.

5.1.8. **Управляемость** - все процессы обеспечения и управления информационной безопасностью в ДелоПортс и подконтрольных ему активах должны быть управляемыми, т.е. должна быть возможность мониторинга и измерения процессов и компонентов, своевременного выявления нарушений информационной безопасности и принятия соответствующих мер.

5.1.9. **Персональная ответственность** - ответственность за обеспечение безопасности активов ДелоПортс и подконтрольных ему активов возлагается на каждого работника ДелоПортс и подконтрольных ему активов в пределах его полномочий.

6. ОТВЕТСТВЕННЫЕ ЛИЦА

6.1. Единоличный исполнительный орган ДелоПортс:

6.1.1. Утверждает настоящую Политику, изменения и дополнения к ней.

6.1.2. Утверждает иные локальные нормативные акты, направленные на создание и совершенствование СУИБ в ДелоПортс и подконтрольных ему активах.

6.1.3. Назначают лиц, ответственных за реализацию предусмотренных настоящей Политикой требований к управлению информационной безопасностью и обеспечение требований применимого законодательства.

6.1.4. Принимает к сведению отчёты ответственных лиц ДелоПортс о принятых мерах по реализации Политики и иных локальных нормативных актов, направленных на создание и совершенствование СУИБ, в ДелоПортс и подконтрольных ему активах в ДелоПортс и подконтрольных активах.

6.1.5. Принимает при необходимости иные меры, направленные на совершенствование СУИБ в ДелоПортс и подконтрольных ему активах (в т.ч. проведение проверок, привлечение к дисциплинарной ответственности виновных лиц, смена ответственных лиц и т.п.).

6.2. **Единоличные исполнительные органы активов, подконтрольных ДелоПортс:**

6.2.1. Назначают лиц, ответственных за реализацию предусмотренных настоящей Политикой требований к управлению информационной безопасностью и обеспечение требований применимого законодательства.

6.2.2. Принимают во исполнение требований настоящей Политики собственные локальные нормативные акты, направленные на создание и совершенствование СУИБ, либо присоединяются к соответствующим локальным нормативным актам ДелоПортс, применимым к данному конкретному подконтрольному активу, в соответствии с установленным у него порядком утверждения и введения в действие локальных нормативных актов.

6.2.3. Принимает к сведению отчёты ответственных лиц о принятых мерах по реализации Политики и иных локальных нормативных актов, направленных на создание и совершенствование СУИБ.

6.2.4. Принимает при необходимости иные меры, направленные на совершенствование СУИБ (в т.ч. проведение проверок, привлечение к дисциплинарной ответственности виновных лиц, смена ответственных лиц и т.п.).

6.3. **Назначенное ответственное лицо (в ДелоПортс):**

6.3.1. Инициирует актуализацию соответствующих локальных нормативных актов и представляет их на утверждение единоличному исполнительному органу ДелоПортс.

6.3.2. Контролирует результаты применения Политики и иных локальных нормативных актов, направленных на создание и совершенствование СУИБ, в ДелоПортс и у подконтрольных ему активов, а также внедрение в ДелоПортс и у подконтрольных ему активов соответствующих процедур (в т.ч. проверяет отчёты ответственных лиц подчинённых активов, инициирует проведение проверок, привлечение к дисциплинарной ответственности виновных лиц, смену ответственных лиц у подчинённых активов и т.п.).

6.3.3. Контролирует проведение соответствующих проверок в ДелоПортс и в подконтрольных ему активах.

6.3.4. Анализирует и оценивает достаточность и эффективность системы принимаемых мер в ДелоПортс и у подконтрольных ему активов, представляет единоличному исполнительному органу ДелоПортс соответствующие предложения по улучшению для утверждения и применения в ДелоПортс и у подчинённых ему активов.

6.3.5. Подготавливает соответствующие отчетные материалы руководству и акционерам (участникам) компаний ГК «Дело» (по запросу).

6.3.6. Формирует программу, разрабатывает и внедряет соответствующие процедуры, обеспечивает контроль их исполнения организует обучающие мероприятия, индивидуальное консультирование работников, информирование по вопросам информационной безопасности совместно со структурными подразделениями, ответственными за управление персоналом и правовое обеспечение деятельности.

6.3.7. Выявляет и оценивает соответствующие риски для СУИБ в ДелоПортс и у подконтрольных ему активов.

6.3.8. Принимает при необходимости иные меры, направленные на совершенствование СУИБ в ДелоПортс и у подконтрольных ему активов.

6.4. **Назначенное ответственное лицо (в подчинённых активах):**

6.4.1. Инициирует актуализацию соответствующих локальных нормативных актов и представляет их на утверждение единоличному исполнительному органу (проекты локальных нормативных актов предварительно направляются на согласование ответственному лицу ДелоПортс).

6.4.2. Контролирует результаты применения Политики и иных локальных нормативных актов, направленных на создание и совершенствование СУИБ, а также внедрение соответствующих процедур (в т.ч. инициирует проведение проверок, привлечение к дисциплинарной ответственности виновных лиц и т.п.).

6.4.3. Анализирует и оценивает достаточность и эффективность системы принимаемых мер в рамках совершенствования СУИБ, представляет единоличному исполнительному органу соответствующие предложения по улучшению для утверждения и применения (указанные предложения предварительно направляются на согласование ответственному лицу ДелоПортс).

6.4.4. Подготавливает соответствующие отчетные материалы руководству, акционерам (участникам) компаний ГК «Дело» и ответственному лицу ДелоПортс (по запросу).

6.4.5. Формирует программу, разрабатывает и внедряет соответствующие процедуры, обеспечивает контроль их исполнения организует обучающие мероприятия, индивидуальное консультирование работников, информирование по вопросам информационной безопасности совместно со структурными подразделениями, ответственными за управление персоналом и правовое обеспечение деятельности.

6.4.6. Выявляет и оценивает соответствующие риски для СУИБ.

6.4.7. Принимает при необходимости иные меры, направленные на совершенствование СУИБ.

6.5. **Руководители структурных подразделений ДелоПортс и подконтрольных активов ДелоПортс:**

6.5.1. Обеспечивают эффективное функционирование СУИБ.

6.5.2. Выявляют уязвимые процессы и процедуры в области информационной безопасности и докладывают о них соответствующему ответственному лицу.

6.5.3. Содействуют предварительной проверке или внутреннему расследованию.

6.5.4. Своевременно информируют соответствующее ответственное лицо о признаках инцидента информационной безопасности.

6.5.5. Инициируют применение мер дисциплинарного воздействия.

6.6. **Работники ДелоПортс и подконтрольных активов ДелоПортс:**

6.6.1 Выполняют все требования Политики и локальных нормативных актов в области управления информационной безопасностью.

6.6.2 Содействуют проведению проверочных мероприятий, предварительных проверок и внутренних расследований, включая предоставление объяснений, необходимых документов.

6.6.3 Незамедлительно информируют своих руководителей или соответствующих ответственных лиц о инцидентах информационной безопасности.

7. СТАНДАРТЫ, НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ И МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

7.1. **Система управления информационной безопасностью (СУИБ).**

7.1.1. Для достижения указанных целей и задач в ДелоПортс внедряется СУИБ. СУИБ документирована в настоящей Политике, в правилах, процедурах, рабочих инструкциях и иных локальных нормативных и ненормативных актах ДелоПортс и подчинённых ему активов. Документированные требования СУИБ доводятся до сведения работников в установленном порядке.

7.1.2. Средства управления информационной безопасностью внедряются по результатам проведения оценки рисков информационной безопасности.

7.2. **Стандарт документирования.**

7.2.1. В целях создания взаимосвязанной структуры нормативных документов ДелоПортс и подконтрольных ему активов в области обеспечения информационной безопасности, разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:

- Настоящая Политика является внутренним нормативным документом по информационной безопасности первого уровня.

- Документы второго уровня – инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников ДелоПортс и подконтрольных ему активов по реализации документов первого и второго уровня.

- Документы третьего уровня – отчётные документы о выполнении требований документов верхних уровней.

7.3. **Категорирование ресурсов.**

7.3.1. В ДелоПортс должны быть выявлены и оценены с точки зрения их важности все ресурсы.

7.3.2. Для всех ценных ресурсов должен быть составлен реестр (перечень).

7.3.3. Благодаря информации о ресурсах ДелоПортс реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

7.3.4. В информационных системах ДелоПортс и подконтрольных ему активов присутствуют следующие типы ресурсов: информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности ДелоПортс и подконтрольных ему активов; открыто распространяемая информация, необходимая для работы ДелоПортс и подконтрольных ему активов, независимо от формы и вида её представления; информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

7.3.5. Для каждого ресурса должен быть назначен владелец, который отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки информации, а также за назначение и периодическую проверку прав доступа и категорий, определённых политиками управления доступа.

7.4. **Классификация информации.**

7.4.1. Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа.

7.4.2. Классификация информации должна быть документирована и утверждена руководством ДелоПортс и подконтрольных ему активов, по представлению ответственного лица ДелоПортс и подконтрольных ему активов соответственно.

7.4.3. Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса.

7.4.4. Периодически классификация должна пересматриваться для поддержания актуальности её соответствия с категорией ресурса.

7.4.5. Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку (гриф).

7.5. **Оценка и обработка рисков.**

7.5.1. В ДелоПортс и подконтрольных ему активах должны быть определены требования к безопасности путём методической оценки рисков.

7.5.2. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес-целями учреждения.

7.5.3. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками информационной безопасности и набор механизмов контроля для защиты от этих рисков.

7.5.4. Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков. Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

- учесть изменения бизнес-требований и приоритетов;
- принять во внимание новые угрозы и уязвимости;
- убедиться в том, что реализованные средства сохранили свою эффективность.

7.5.5. Перед обработкой каждого риска ДелоПортс должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для ДелоПортс. Такие решения должны регистрироваться. Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

- применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска, если он точно удовлетворяет требованиям настоящей Политики и критериям принятия рисков;
- уклонение от риска путём недопущения действий, могущих быть его причиной;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

7.6. **Обучение информационной безопасности.**

7.6.1. Все сотрудники должны проходить периодическую подготовку в области политики и процедур информационной безопасности, принятых в ДелоПортс и подконтрольных ему активах.

7.6.2. Сроки и периодичность проведения обучения информационной безопасности определяются по инициативе начальника отдела информационной безопасности ДелоПортс/соответствующего ответственного лица у подчинённых активов и утверждаются единоличным исполнительным органом ДелоПортс и подконтрольных ему активов.

7.7. **Контроль доступа.**

7.7.1. Основными пользователями информации в информационной системе ДелоПортс и подконтрольных ему активов являются сотрудники структурных подразделений.

7.7.2. Уровень полномочий каждого пользователя определяется индивидуально.

7.7.3. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

7.7.4. Допуск пользователей к работе с информационными ресурсами строго регламентируется.

7.7.5. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке.

7.7.6. Регистрируемые учётные записи подразделяются на:

- Пользовательские – предназначенные для аутентификации пользователей ДелоПортс;
- Системные – используемые для нужд операционной системы;
- Служебные – предназначенные для функционирования отдельных процессов или приложений.

7.8. **Управление привилегиями.**

7.8.1. Доступ сотрудника к информационным ресурсам ДелоПортс должен быть санкционирован владельцами соответствующих информационных ресурсов.

7.8.2. Управление доступом осуществляется в соответствии с установленными процедурами.

7.8.3. Наделение привилегиями и их использование должно быть строго ограниченным и управляемым.

7.8.4. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий.

7.9. **Управление паролями.**

7.9.1. Пароли – средство проверки личности пользователя для доступа к информационной системе, информационному ресурсу или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

7.9.2. Управление паролями должно обеспечивать:

- установление требований к сложности пароля - необходимо установить требования к длине пароля, набору символов и числу попыток ввода;
- обеспечения сохранности в тайне личных паролей;
- назначенные производителем программного обеспечения пароли должны быть изменены сразу после завершения инсталляции;
- обеспечения выполнения требования периодического изменения пароля пользователя;

7.9.3. При наличии технической возможности – использовать другие технологии идентификации и аутентификации пользователей, в частности, биометрических технологий, проверки электронной подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

7.10. **Работа в сети Интернет.**

7.10.1. Доступ к сети Интернет предоставляется сотрудникам ДелоПортс и подконтрольных ему активов в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам, в минимально достаточном для указанных целей объёме.

7.10.2. При использовании сети Интернет запрещается:

- использовать предоставленный ДелоПортс и подконтрольными ему активами доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- совершать любые действия, направленные на нарушение нормального функционирования элементов информационных технологий ДелоПортс.

7.10.3. ДелоПортс оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

7.10.4. Информация о посещаемых сотрудниками ДелоПортс Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству ДелоПортс для контроля.

7.11. Защита от вредоносного программного обеспечения

7.11.1. В ДелоПортс и подконтрольных ему активах должна быть выстроена систематизированная и автоматизированная работа по предупреждению проникновения вредоносного программного обеспечения и предотвращению негативных последствий от его воздействия.

7.12. Электронные цифровые подписи.

7.12.1. Электронные цифровые подписи обеспечивают защиту аутентификации и целостности электронных документов, могут применяться для любой формы документа, обрабатываемого электронным способом.

7.12.2. Электронная цифровая подпись является аналогом собственноручной подписи.

7.12.3. Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа электронной цифровой подписи, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа.

7.12.4. Передача личной электронной цифровой подписи третьим лицам (заместителям, исполняющим обязанности, секретарям-референтам и прочим исполнителям) категорически запрещается.

7.13. Управление инцидентами информационной безопасности.

7.13.1. Формальная процедура уведомления о происшествиях в области информационной безопасности в ДелоПортс и подконтрольных ему активах, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии, разрабатываются по инициативе начальника отдела информационной безопасности ДелоПортс/соответствующего ответственного лица подчинённого актива, и утверждается уполномоченным органом управления ДелоПортс/подчинённого актива.

7.13.2. Механизмы и автоматизированный мониторинг, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты разрабатываются по инициативе начальника отдела информационной безопасности ДелоПортс/соответствующего ответственного лица подчинённого актива, и утверждается уполномоченным органом управления ДелоПортс/подчинённого актива.

7.13.3. Процедура уведомления об инцидентах в области информационной безопасности в обязательном порядке предусматривает меры по оперативному информированию субъектов данных, подвергшихся воздействию в результате инцидента.

7.14. **Управление непрерывностью и восстановлением.**

7.14.1. Планы, позволяющие продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес-процессов разрабатываются по инициативе начальника отдела информационной безопасности ДелоПортс/соответствующего ответственного лица подчинённого актива, и утверждается уполномоченным органом управления ДелоПортс/подчинённого актива.

7.14.2. В каждом плане поддержки непрерывности бизнеса указываются условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана.

7.14.3. При появлении новых требований вносятся поправки в принятые планы действия в нештатных ситуациях.

7.14.4. Для каждого плана назначается определённый владелец.

7.14.5. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности находятся в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

7.15. **Аудит информационной безопасности.**

7.15.1. ДелоПортс и подконтрольные ему активы проводит внутренние проверки СУИБ через запланированные интервалы времени. Основные цели проведения таких проверок:

- оценка текущего уровня защищённости информационных систем;
- выявление и локализация уязвимостей в системе защиты информационных систем;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении информационных ресурсов;
- оценка соответствия информационных систем требованиям внутренних нормативных документов ДелоПортс;
- выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

7.15.2. В число задач, решаемых при проведении проверок и аудитов СУИБ, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре информационных систем, необходимых для оценки состояния информационной безопасности;
- анализ существующей политики безопасности и других организационно распорядительных документов по защите информации на предмет их полноты

и эффективности, а также формирование рекомендаций по их разработке (или доработке);

- технико-экономическое обоснование механизмов безопасности;

- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности информационных систем;

- разбор инцидентов информационной безопасности и минимизация возможного ущерба от их проявления.

7.15.3. Руководство и сотрудники ДелоПортс и подконтрольных ему активов при проведении у них аудита (проверки) СУИБ обязаны оказывать содействие и предоставлять всю необходимую для проведения аудита информацию.

7.16. **Передача информации третьим лицам.**

7.16.1. При передаче ДелоПортс и подконтрольными ему активами информации третьим лицам, владельцем, либо оператором которой оно является, необходимо:

- не допускать передачу информации без оформленных надлежащим образом договорных обязательств между владельцем информации и ДелоПортс/подконтрольным ему активом, прямо предусматривающих согласие владельца информации на передачу третьим сторонам;

- при передаче информации, правообладателем или владельцем которой является ДелоПортс/подконтрольный ему актив, либо передача которой осуществляется с согласия третьих лиц, рекомендуется включать в договорные обязательства требования выполнять положения настоящей политики.

8. ОТВЕТСТВЕННОСТЬ

8.1. В случае нарушения установленных правил работы с информационными активами, нарушения требований настоящей Политики и иных локальных актов, направленных на обеспечение СУИБ, работник, независимо от занимаемой должности, может быть ограничен в правах доступа к таким активам, а также привлечен к ответственности в соответствии с законодательством РФ.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящая Политика изменяется и отменяется приказом единоличного исполнительного органа ДелоПортс.

9.2. Настоящая Политика подлежит пересмотру в случае:

9.2.1. Изменения действующего законодательства РФ;

9.2.2. Изменения внутренних нормативных документов ДелоПортс.

9.3. Актуализация настоящей Политики осуществляется начальником отдела информационной безопасности ДелоПортс.

9.4. В случае пересмотра и внесения изменений в настоящую Политику все заинтересованные стороны и субъекты информируются об этом посредством публикации политики на публичном ресурсе ДелоПортс.

9.5. Начальник отдела информационной безопасности вправе давать разъяснения по применению настоящей Политики.

9.6. Контроль за исполнением требований настоящей Политики возлагается на начальника отдела информационной безопасности.

9.7. При наличии в тексте настоящей Политики ссылки на документ, в который внесены изменения после даты утверждения настоящей Политики, следует пользоваться актуальной версией такого документа. В случае если в Политике сделана ссылка на документ, действие которого отменено, соответствующий раздел Политики применяется в части, не затрагивающей ссылку на утративший силу документ.

9.8. Если отдельные нормы настоящей Политики вступают в противоречие с законодательством Российской Федерации или Уставом ДелоПортс, эти нормы утрачивают силу, и в части регулируемых этими нормами вопросов следует руководствоваться нормами законодательства Российской Федерации.

9.9. Недействительность отдельных норм настоящей Политики не влечет признание недействительности других норм Политики или Политики в целом.

Исполнитель Бурвицкий О.О.