ГРУППА КОМПАНИЙ

Политика в области управления информационной безопасностью ООО «УК «Дело»

Управляющая компания «Дело»

СОДЕРЖАНИЕ

ТЕРМИНЫ И ПОНЯТИЯ

Настоящая Политика является основополагающим документом, регулирующим деятельность Общества с ограниченной ответственностью «Управляющая компания «Дело» (далее – УК Дело) в области информационной безопасности.

Политика информационной безопасности разработана в соответствии с требованиями законодательства Российской Федерации и положениями международного стандарта ISO/IEC 27001:2013.

Группа компаний «Дело»

(Группа «Дело»), в состав которой входят УК Дело и компании, находящиеся под прямым или косвенным контролем УК Дело.

Руководство

Работники, имеющие непосредственное подчинение генеральному директору, либо руководители структурных подразделений.

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.

Бизнес-процесс

Последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности УК Дело.

Владелец актива

Физическое или юридическое лицо, которое наделено административной ответственностью за руководство изготовлением, разработкой, хранением, использованием и безопасностью актива. Термин «владелец» не означает, что этот человек фактически имеет право собственности на этот актив.

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 защищённости интересов УК Дело.

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.

Политика

Общие цели и указания, формально выраженные руководством.

Привилегии

Это права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.

Риск

Сочетание вероятности события и его последствий.

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.

ОБЩИЕ ПОЛОЖЕНИЯ

Под информационной безопасностью понимается состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

!

Политика информационной безопасности утверждается Генеральным директором УК Дело.

В области управления информационной безопасностью «УК Дело» устанавливаются следующие стратегические цели:

- Защита конкурентных преимуществ УК Дело от угроз в области информационной безопасности.
- Соответствие требованиям законодательства, отраслевым нормам и договорным обязательствам в части информационной безопасности.
- Эффективное управление информационной безопасностью и непрерывное совершенствование системы управления информационной безопасностью.
- Достижение адекватности мер по защите от угроз информационной безопасности.
- Обеспечение безопасности активов Группы компаний «Дело», включая персонал, материально-технические ценности, информационные ресурсы, бизнес-процессы.

- Система управления информационной безопасностью УК Дело призвана решать следующие задачи:
- Вовлечение руководства УК Дело в процесс обеспечения информационной безопасности: деятельность по обеспечению информационной безопасности инициирована и контролируется руководством УК Дело.
- Соответствие требованиям законодательства Российской Федерации: УК Дело реализует меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством, отраслевыми нормами и договорными обязательствами.
- Согласованность действий по обеспечению информационной, физической и экономической безопасности: действия по обеспечению информационной, физической и экономической безопасности осуществляются на основе четкого взаимодействия заинтересованных подразделений УК Дело и согласованы между собой по целям, задачам, принципам, методам и средствам.

ЦЕЛИ И ЗАДАЧИ

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

- Документированность требований информационной безопасности: в УК Дело все требования в области информационной безопасности фиксируются в разрабатываемых внутренних нормативных документах.

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

- Реагирование на инциденты информационной безопасности: УК Дело ведёт систематизированную работу по выявлению, учету и оперативному реагированию на действительные, предпринимаемые и вероятные нарушения информационной безопасности.

- Оценка рисков: в УК Дело на постоянной основе реализуются мероприятия по оценке и управлению рисками информационной безопасности, повышению уровня защищенности информационных активов.

- Учет требований информационной безопасности в проектной деятельности: УК Дело 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.

- Постоянное совершенствование системы управления информационной безопасностью: совершенствование системы управления информационной безопасностью является непрерывным процессом.

Системность

В Группе компаний «Дело» 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.

Коллективная защита

Реагирование на угрозы и инциденты информационной безопасности осуществляется коллективно всеми подразделениями кибербезопасности компаний, подконтрольных УК Дело.

> Координатором и центром компетенций выступает УК Дело.

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.

Эшелонированность

Система обеспечения информационной безопасности стоится таким образом, чтобы наиболее защищаемая зона безопасности находилась внутри других защищаемых зон.

Непрерывность

В УК Дело обеспечение информационной безопасности является непрерывным целенаправленным процессом, предполагающим принятие соответствующих мер на всех этапах жизненного цикла активов.

Разумная достаточность

Выбор средств защиты активов, адекватных реально существующим угрозам (т.е. обеспечивающих допустимый уровень возможного ущерба в случае реализации угроз), осуществляется на основе проведения анализа рисков.

Законность

При выборе и реализации мер и средств обеспечения информационной безопасности УК Дело строго соблюдается законодательство Российской Федерации, требования нормативных правовых и технических документов в области обеспечения информационной безопасности УК Дело.

Управляемость

Все процессы обеспечения и управления информационной безопасностью в УК Дело должны быть управляемыми, т. е. должна быть возможность мониторинга и измерения процессов и компонентов, своевременного выявления нарушений информационной безопасности и принятия соответствующих мер.

Персональная ответственность

Ответственность за обеспечение безопасности активов возлагается на каждого работника в пределах его полномочий.

ОБЛАСТЬ ПРИМЕНЕНИЯ

Требования в сфере обеспечения информационной безопасности распространяются на все регионы деятельности и на все подконтрольные компании УК Дело, на всю информацию и ресурсы обработки информации.

Соблюдение настоящей Политики обязательно для всех работников УК Дело.

Генеральный директор УК Дело

- Утверждает Политику, изменения и дополнения к ней.
- Отвечает за реализацию Политики в УК Дело.
- Контролирует результаты применения Политики и внедрения в Группе компаний «Дело» соответствующих процедур.
- Контролирует проведение соответствующих проверок.
- Организует контроль за реализацией мер, принятых исполнительными органами подконтрольных УК Дело компаний в рамках функционирования системы управления информационной безопасностью.

Единоличные исполнительные органы компаний, подконтрольных УК Дело

- Отвечают за обеспечение требований применимого законодательства и локальных нормативных актов соответствующей компании Группы «Дело».
- Отвечают за реализацию Политики в соответствующей компании Группы «Дело».

Ответственное лицо

- Инициирует актуализацию соответствующих локальных нормативных актов
- Анализирует и оценивает достаточность и эффективность системы принимаемых мер, представляет единоличному исполнительному органу соответствующие предложения по улучшению; подготавливает соответствующие отчетные материалы руководству и акционерам (участникам) компаний Группы «Дело».

ЛИЦА, УЧАСТВУЮЩИЕ В РЕАЛИЗАЦИИ ПОЛИТИКИ

- 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.
- Выявляет и оценивает соответствующие риски.

Руководители структурных подразделений УК Дело и подконтрольных компаний УК Дело

- Обеспечивают эффективное функционирование системы управления информационной безопасности.
- Выявляют уязвимые процессы и процедуры в области информационной безопасности.
- Содействуют предварительной проверке или внутреннему расследованию.
- Своевременно информируют ответственное лицо о признаках инцидента информационной безопасности.
- Инициируют применение мер дисциплинарного воздействия.

Работники УК Дело и подконтрольных компаний УК Дело

- Выполняют все требования Политики и локальных нормативных актов УК Дело в области информационной безопасности.
- Содействуют проведению проверочных мероприятий, предварительных проверок и внутренних расследований, включая предоставление объяснений, необходимых документов.
- Незамедлительно информируют об инцидентах информационной безопасности.

01

Система управления информационной безопасностью

Для достижения указанных целей и задач в УК Дело внедряется система управления информационной безопасностью (далее - СУИБ). СУИБ документирована в настоящей политике, в правилах, процедурах, рабочих инструкциях. Документированные требования СУИБ доводятся до сведения работников. Средства управления информационной безопасностью внедряются по результатам проведения оценки рисков информационной безопасности.

02

Стандарт документирования

В целях создания взаимосвязанной структуры нормативных документов УК Дело 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 УК Дело по реализации документов первого и второго уровня.
- Документы третьего уровня – отчётные документы о выполнении требований документов верхних уровней.

03

Категорирование ресурсов

В УК Дело должны быть выявлены и оценены с точки зрения их важности все ресурсы. Для всех ценных ресурсов должен быть составлен реестр (перечень). Благодаря информации о ресурсах УК Дело реализуется защита информации, степень которой соразмерна ценности и важности ресурсов. В информационных системах УК Дело присутствуют следующие типы ресурсов: информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности УК Дело; открыто распространяемая информация, необходимая для работы УК Дело, 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.

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.

04

Классификация информации

Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена руководством УК Дело. Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация должна пересматриваться для поддержания актуальности её соответствия с категорией ресурса. Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку (гриф).

05

Оценка и обработка рисков

В УК Дело должны быть определены требования к безопасности путём методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес-целями учреждения. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками информационной безопасности и набор механизмов контроля для защиты от этих рисков. 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.

05

Перед обработкой каждого риска УК Дело должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для УК Дело. 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 Политике УК Дело и критериям принятия рисков;
- уклонение от риска путём недопущения действий, способных быть его причиной;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

06

Обучение информационной безопасности

Все сотрудники должны проходить периодическую подготовку в области Политики и процедур информационной безопасности, принятых в УК Дело. Сроки и периодичность проведения обучения информационной безопасности определяются по инициативе заместителя директора по информационным технологиям по кибербезопасности и утверждается уполномоченным органом управления УК Дело.

07

Контроль доступа

Основными пользователями информации в информационной системе УК Дело являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями. Допуск пользователей к работе с информационными ресурсами строго регламентируется. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке.

Регистрируемые учётные записи подразделяются на:

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

08

Управление привилегиями

Доступ сотрудника к информационным ресурсам УК Дело должен быть санкционирован владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами. Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий.

09

Управление паролями

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

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;
- 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.).

10

Работа в сети Интернет

Доступ к сети Интернет предоставляется сотрудникам УК Дело в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам, в минимально достаточном для указанных целей объёме.

При использовании сети Интернет запрещается:

- использовать предоставленный УК Дело 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 УК Дело.

10

УК Дело 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.

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

11

Защита от вредоносного программного обеспечения

В УК Дело должна быть выстроена систематизированная и автоматизированная работа по предупреждению проникновения вредоносного программного обеспечения и предотвращению негативных последствий от его воздействия.

12

Защита от вредоносного программного обеспечения

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

Электронная цифровая подпись является аналогом собственноручной подписи.

12

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.

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

13

Управление инцидентами информационной безопасности

Формальная процедура уведомления о происшествиях в области информационной безопасности в УК Дело, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии, разрабатываются по инициативе заместителя директора по информационным технологиям по кибербезопасности и утверждается уполномоченным органом управления УК Дело.

Механизмы и автоматизированный мониторинг, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты разрабатываются по инициативе заместителя директора по информационным технологиям по кибербезопасности и утверждается уполномоченным органом управления УК Дело.

13

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

14

Управление непрерывностью и восстановлением

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 заместителя директора по информационным технологиям по кибербезопасности и утверждается уполномоченным органом управления УК Дело. В каждом плане поддержки непрерывности бизнеса указываются условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований вносятся поправки в принятые планы действия в нештатных ситуациях. Для каждого плана назначается определённый владелец. 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.

Аудит информационной безопасности

УК Дело 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 УК Дело;
- выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

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);
- 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.

Руководство и сотрудники УК Дело при проведении у них аудита СУИБ обязаны оказывать содействие и предоставлять всю необходимую для проведения аудита информацию.

16

Передача информации третьим лицам

При передаче УК Дело информации третьим лицам, владельцем, либо оператором которой оно является, необходимо:

- не допускать передачу информации без оформленных надлежащим образом договорных обязательств между владельцем информации и УК Дело, прямо предусматривающих согласие владельца информации на передачу третьим сторонам;
- при передаче информации, правообладателем или владельцем которой является УК Дело, либо передача которой осуществляется с согласия третьих лиц, УК Дело обязуется включать в договорные обязательства требования выполнять положения настоящей Политики.

ОТВЕТСТВЕННОСТЬ

В случае нарушения установленных правил работы с информационными активами работник, независимо от занимаемой должности, может быть ограничен в правах доступа к таким активам, а также привлечен к ответственности в соответствии с законодательством Российской Федерации.

ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

01

Настоящая Политика изменяется и отменяется приказом генерального директора УК Дело.

02

Настоящая Политика подлежит пересмотру в случае изменения:

- действующего законодательства Российской Федерации;
- внутренних нормативных документов Общества.

03

Актуализация настоящей Политики осуществляется заместителем директора по информационным технологиям по кибербезопасности УК Дело.

04

В случае пересмотра и внесения изменений в настоящую Политику все заинтересованные стороны и субъекты информируются об этом посредством публикации Политики на публичном ресурсе УК Дело.

05

Заместитель директора по информационным технологиям по кибербезопасности УК Дело вправе давать разъяснения по применению настоящей Политики.

06

Контроль за исполнением требований настоящей Политики возлагается на заместителя директора по информационным технологиям по кибербезопасности УК Дело.

07

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.