Назначение

Настоящий документ Политика информационной безопасности ПАО Софтлайн (далее — Политика) является основополагающим документом, определяющим позицию, цели, задачи и принципы ПАО Софтлайн (далее — Софтлайн) и в дочерних и зависимых обществах ПАО Софтлайн (далее – ДЗО) в области информационной безопасности. ПАО Софтлайн и ее ДЗО далее — Софтлайн или Группа.

Общие положения

Информационная безопасность (ИБ) - свойство информации сохранять конфиденциальность, целостность и доступность. Кроме того, данное понятие может включать в себя также и свойство сохранять аутентичность, подотчетность, неотказуемость и надежность.

Под информационными активами для целей настоящей Политики признаются сотрудники, информация, деловая репутация, материальные ценности и бизнес-процессы.

Деятельность Софтлайн в области ИБ основывается на стратегии развития Группы, а решаемые задачи способствуют эффективному и безопасному развитию бизнеса Софтлайн в современном мире цифровизации и цифровой трансформации.

Период действия и внесение изменений

Настоящая Политика является локальным нормативным актом постоянного действия. Настоящая Политика утверждается, изменяется и признается утратившей силу Генеральным директором ПАО Софтлайн. Пересмотр Политики проводится на регулярной основе не реже одного раза в год или по мере необходимости.

Декларация об информационной безопасности

Принятием Политики Софтлайн провозглашает и обязуется осуществлять надлежащие меры защиты информационных активов от риска причинения вреда и убытков, возникающих в результате реализации угроз ИБ.

Руководство Софтлайн осознает важность и необходимость совершенствования мер и средств обеспечения ИБ в контексте развития законодательства в области ИБ, а также усложнения используемых информационных технологий.

Руководство Софтлайн учитывает геополитическую ситуацию как один из ключевых факторов в управлении рисками ИБ, принимая меры для защиты от угроз, возникающих вследствие политической нестабильности, санкционных режимов, международных конфликтов и изменения законодательных требований в разных странах.

Руководство Софтлайн инициирует и контролирует работы в области ИБ.

Соблюдение принципов, правил и требований ИБ является элементом корпоративной культуры Группы.

Руководители и специалисты по ИБ Софтлайн должны ответственно выполнять свои обязанности, осознавая, что качество их работы непосредственно влияет на защищённость информационных активов Группы.

Сотрудники Софтлайн должны руководствоваться настоящей Политикой в профессиональной деятельности, при взаимодействии с внешними контактами, внутрикорпоративном взаимодействии, личном развитии и повышении культуры ИБ.

Каждый сотрудник Софтлайн несёт ответственность за выполнение всех локальных нормативных документов в области ИБ.

Взаимодействие с контрагентами регулируется законодательством и заключёнными договорами.

Достижение целей ИБ при соблюдении принципов дополнительно позволит упрочить конкурентные преимущества, обеспечить соответствие правовым, регуляторным и договорным требованиям, снизить риски потери деловой репутации или нанесения урона деловой репутации

Цели в области информационной безопасности

Управление и обеспечение ИБ Софтлайн ориентировано на достижение следующих целей:

- Предоставление безопасной информационной среды для функционирования и развития бизнеса.
- Повышение конкурентоспособности, ценности бизнеса и сохранение деловой репутации для акционеров путем снижения уровня риска в области ИБ.
- Соответствие требованиям законодательства в области ИБ и защиты персональных данных, а также соблюдение соответствующих договорных обязательств.
- Повышение корпоративной культуры обработки и защиты информации, в т. ч. персональных данных.
- Эффективное управление процессами ИБ и непрерывное совершенствование системы управления ИБ.

Задачи в области информационной безопасности

Для достижения целей в Софтлайн приняты следующие задачи в области ИБ:

- Проектирование, внедрение и непрерывное совершенствование системы управления ИБ (далее — СУИБ).
- Вовлечение высшего руководства Софтлайн в процесс функционирования СУИБ.

Вопросы ИБ регулярно рассматриваются уполномоченными комитетами и/или рабочими группами.

- Эффективное использование ресурсов, выделенных в целях обеспечения ИБ. Оценка эффективности расходов.

- Обеспечение безопасности информационных активов Софтлайн.
- Соблюдение законодательства, требований регулирующих организаций в области ИБ и защиты персональных данных.
- Совершенствование технических, организационных и правовых мер защиты.
- Формирование, накопление и развитие компетенций в области ИБ и защиты персональных данных.
- Использование риск-ориентированного подхода. В Софтлайн регулярно проводится оценка рисков ИБ и мероприятия по повышению уровня защищенности информационных активов.
- Управление инцидентами ИБ. Софтлайн непрерывно совершенствует механизмы реагирования на инциденты.
- Повышение осведомленности сотрудников. Сотрудники Софтлайн регулярно проходят обязательное обучение по ИБ.
- Формализация требований ИБ. Требования фиксируются в локальных нормативных актах и доводятся до сотрудников.
- Учет требований ИБ в проектной деятельности. Разработка и документирование требований к обеспечению ИБ осуществляется на начальных этапах реализации проектов.
- Проверка благонадежности сотрудников. Все кандидаты на вакантные должности проходят проверку в соответствии с установленными процедурами.
- Мониторинг и непрерывное совершенствование СУИБ по результатам периодических аудитов (проверок).

Принципы обеспечения информационной безопасности

В Софтлайн определены следующие принципы обеспечения ИБ:

Принцип системности

Активы рассматриваются как взаимозависимые компоненты единой системы. Взаимовлияние компонентов учитывается при анализе рисков и угроз ИБ.

Принцип полноты (комплексности)

В целях обеспечения ИБ используется широкий спектр мер, методов и средств защиты, комплексное использование которых обеспечивает нейтрализацию актуальных угроз и отсутствие уязвимостей в точках интеграции.

Принцип эшелонированности

Недопустимо полагаться на один защитный рубеж. Система обеспечения ИБ строится так, чтобы наиболее защищаемая зона безопасности находилась внутри других защищаемых зон.

Принцип равнопрочности

Эффективность защитных механизмов не должна быть сведена на нет слабым звеном, возникшим в результате недооценки угроз либо применения неадекватных мер защиты.

Принцип непрерывности

Обеспечение ИБ является непрерывным целенаправленным процессом, предполагающим принятие мер защиты на всех этапах жизненного цикла активов.

Принцип разумной достаточности

«Абсолютная» защита активов невозможна. Выбор средств защиты, адекватных актуальным угрозам, осуществляется на основе анализа рисков.

Принцип законности

При выборе и реализации мер обеспечения ИБ Софтлайн строго соблюдает применимое законодательство, требования нормативных правовых и технических документов в области ИБ.

Принцип управляемости

Процессы обеспечения и совершенствования ИБ должны быть управляемыми, т. е. необходимо осуществлять мониторинг, измерение параметров и своевременно корректировать процессы.

Принцип персональной ответственности

Ответственность за обеспечение ИБ возлагается на каждого сотрудника в пределах его полномочий.

Ответственность за нарушение Политики

Сотрудники Софтлайн обязаны выполнять требования и правила ИБ при работе с информацией и информационными активами Группы, её партнёров и контрагентов.

Высокие корпоративные стандарты и правила обеспечения ИБ Софтлайн обязательны для всех без исключения сотрудников Группы и должны учитываться во взаимоотношениях с партнерами и контрагентами.

При использовании сети Интернет, при общении в социальных сетях и мессенджерах, использовании электронной почты, других электронных средств и платформ коммуникаций сотрудникам Софтлайн следует проявлять осмотрительность и сдержанность.

Каждый сотрудник Софтлайн за несоблюдение требований ИБ несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с применимым законодательством.

Сотрудники партнёров и контрагентов, использующие информационные активы Софтлайн, а также предоставленную им информацию, несут ответственность в соответствии с договорными положениями, а также применимым законодательством.

Приложение. Перечень минимальных требований по выполнению политики в ПАО Софтлайн и ее дочерних и зависимых компаниях

Настоящее приложение к Политике ИБ содержит перечень минимальных требований по выполнению Политики в ПАО Софтлайн и ее ДЗО, включая требования о разработке и внедрению собственной политики ИБ и иных нормативных документов в сфере ИБ. Ответственность за выполнение минимальных требований в ДЗО несут Генеральные директора ДЗО.

Организационные меры

Софтлайн выполняют следующие организационные меры защиты ИБ:

- Разрабатывает, утверждает на уровне руководства и регулярно обновляет политику ИБ, соответствующую политике безопасности Софтлайн, а также иным применимым стандартам и требованиям с учетом специфики ДЗО.
- Реализует процедуры доступа в соответствии с принципом минимально достаточных прав.
- Разрабатывает и обеспечивает соблюдение политик парольной защиты для всех пользователей и сервисных учётных записей. Политика парольной защиты включает в себя определение требований к сложности паролей, периодичности их смены и хранения.
- Назначает приказами генерального директора организации ответственных лиц за ИБ, безопасность обработки персональных данных, а также обеспечение безопасности персональных данных в информационных системах персональных данных (ИСПДн). Эти лица несут ответственность за соблюдение требований ИБ и защиту персональных данных в соответствии с законодательством.
- Организует регулярное обучение по информационной безопасности для всех категорий сотрудников. Темы обучения должны охватывать актуальные угрозы: предотвращения фишинговых атак, безопасное использование корпоративных ресурсов, работу с персональными данными, соблюдение внутренних политик ИБ и т. п.
- Организует регулярное тестирование сотрудников на знание требований информационной безопасности. Результаты тестирования должны использоваться для выявления пробелов в знаниях и дальнейшего обучения.
- Обеспечивает регулярное и своевременное информирование сотрудников о новых угрозах, инцидентах ИБ, изменениях в политиках или процедурах компании. Это может включать информационные рассылки, публикации на корпоративном портале, проведение вебинаров и т. п.
- Обеспечивает информирование новых работников об имеющихся требованиях по информационной безопасности на этапе приема на работу.

Технические меры защиты

Софтлайн выполняют следующие технические меры защиты ИБ:

- Внедряет меры по защите от вредоносного программного обеспечения, включающие установку и регулярное обновление антивирусного программного обеспечения на всех рабочих станциях и серверах.
- Осуществляет проверку всего входящего почтового трафика на предмет вредоносных вложений и ссылок.
- Обеспечивает регулярную автоматическую установку обновлений безопасности программного обеспечения для рабочих станций и серверов. В случае невозможности автоматической установки обновления должны быть установлены вручную с последующим контролем.
- Обеспечивает создание и хранение резервных копий критически важных систем и данных в изолированной среде. Выполняет регулярную проверку возможности восстановления из резервных копий для обеспечения доступности данных в случае возникновения инцидентов.
- Внедряет средства контроля сетевого трафика (межсетевые экраны) для обеспечения безопасности сетевых ресурсов.
- Использует криптографические методы защиты информации при взаимодействии с информационными системами Софтлайн для обеспечения конфиденциальности и целостности данных.

УТВЕРЖДЕНО

Генеральный директор ПАО Софтлайн В. Лавров

Совет директоров ПАО Софтлайн (Протокол № 05/25 от 21 мая 2025 г.)