ПОЛИТИКА
информационной безопасности
ООО «Инфомаксимум»

г. Саранск
2026 год

1. Общие положения

1.1. Назначение документа

Настоящая Политика информационной безопасности ООО «Инфомаксимум» (далее - **Политика**) определяет единые принципы, цели, область действия, распределение ответственности и основные направления обеспечения информационной безопасности в Обществе с ограниченной ответственностью «Инфомаксимум» (далее - Общество).

1.2. Политика является документом верхнего уровня. Детальные организационные, процессные и технические требования устанавливаются стандартами, регламентами, процедурами, инструкциями и иными локальными нормативными актами Общества.

1.3. Нормативная основа

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Трудовой кодекс Российской Федерации;
- договорные обязательства Общества перед клиентами.

1.4. Методологическая основа

- ISO/IEC 27001:2022;
- ISO/IEC 27002:2022;
- ISO/IEC 27005:2022;
- ГОСТ Р 50922-2006.

1.5. Статус документа

Положения Политики обязательны для руководства, работников Общества, а также для иных лиц, получивших доступ к информационным активам Общества в рамках договорных или иных законных отношений.

2. Термины и определения

Информационная безопасность (ИБ)	–	состояние защищенности информации, при котором обеспечены ее конфиденциальность, целостность и доступность.
Система управления информационной безопасностью (СУИБ)	–	часть системы управления Общества, обеспечивающая создание, внедрение, поддержание и постоянное улучшение ИБ на основе оценки рисков.
Высшее руководство	–	генеральный директор Общества или лицо его замещающее по приказу или доверенности.
Информационный актив	–	информация, информационная система, сервис, программное обеспечение (ПО), оборудование, учетная запись, носитель информации, облачный ресурс или иной ресурс, представляющий ценность для Общества.
Информация клиентов	–	информация, включая персональные данные, которую Общество получает, хранит или обрабатывает при оказании услуг клиентам, в том числе в облачных сервисах Общества и при сопровождении ПО в информационных системах клиентов.
Конфиденциальная информация	–	информация, доступ к которой ограничен законодательством Российской Федерации, договорами или решением Общества.

Риск ИБ – влияние неопределенности на цели ИБ, выражаемое сочетанием последствий события и вероятности его наступления.

Аппетит к риску – объем и вид риска, который Общество готово принять.

Владелец риска – работник, наделенный ответственностью и полномочиями управлять риском.

Остаточный риск – риск, сохраняющийся после применения мер обработки.

Исключение – утвержденное отступление от требования документа по ИБ на ограниченный срок, принятое на основании оценки риска.

Инцидент ИБ – событие или совокупность событий, которые нарушили или с высокой вероятностью могут нарушить конфиденциальность, целостность или доступность информации либо работу информационных систем.

Средство защиты информации (СЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Привилегированная учетная запись – учетная запись с правами администрирования информационных систем, инфраструктуры, СЗИ, средств резервного копирования или журналирования либо с доступом к конфиденциальной информации в объеме, превышающем пользовательский. Права локального администратора на рабочем месте работника к привилегированным учетным записям для целей Политики не относятся; требования к ним устанавливает Положение об ИБ.

ИИ-сервис – сервис на основе моделей искусственного интеллекта, включая чат-интерфейсы и программные интерфейсы, используемый для обработки информации.

ИИ-агент – ИИ-сервис, который по заданию работника самостоятельно выполняет действия в информационных системах Общества: создает и изменяет код, запускает сборку, работает с файлами и хранилищами и т.п.

Владелец информационного актива – руководитель подразделения, отвечающий за ценность, классификацию и условия использования актива.

Владелец системы – назначенный работник, отвечающий за бизнес-применение конкретной информационной системы и требования к ней, включая модель доступа.

Служба ИБ – подразделение или работник(и) Общества, на которое возложены функции по организации и контролю обеспечения ИБ.

3. Принципы информационной безопасности

3.1. Общество руководствуется следующими принципами:

– **Законность и соответствие требованиям** - меры ИБ реализуются с учетом законодательства, договорных обязательств и применимых внутренних документов.

– **Риск-ориентированный подход** - решения по мерам ИБ принимаются с учетом значимости активов, угроз, уязвимостей и потенциального ущерба.

– **Защита информации по критичности** - уровень защиты определяется значимостью, критичностью и режимом доступа к информации.

– **Необходимость и достаточность** - применяются разумные и достаточные меры защиты, соразмерные рискам и задачам бизнеса.

– **Разграничение доступа** - доступ предоставляется по принципам служебной необходимости, минимально достаточных привилегий и ролевого управления доступом.

– **Ответственность владельцев** - владельцы активов и систем участвуют в классификации, определении требований защиты и согласовании доступа.

– **Безопасность на всем жизненном цикле** - требования ИБ учитываются при создании, изменении, эксплуатации и выводе из эксплуатации систем и активов.

– **Непрерывность и устойчивость** - критичные процессы и системы должны поддерживаться с учетом задач устойчивости и восстановления.

– **Осведомленность работников** - работники должны знать и соблюдать применимые требования ИБ.

– **Постоянное улучшение** - система управления ИБ подлежит регулярному контролю и пересмотру.

4. Цели Политики

4.1. Целями Политики являются:

– установление единых рамок управления информационной безопасностью в Обществе;

– защита информации и информационных активов Общества от внутренних и внешних угроз;

– обеспечение устойчивого и безопасного функционирования информационной инфраструктуры;

– снижение рисков информационной безопасности бизнеса, клиентов, работников и партнеров;

– обеспечение выполнения применимых правовых, договорных и внутренних требований ИБ;

– создание основы для разработки стандартов, регламентов и процедур по ИБ.

5. Область действия

5.1. Политика распространяется:

– на все структурные подразделения и всех работников Общества, включая дистанционных работников;

– на все информационные активы Общества независимо от формы представления информации и места размещения;

– на все информационные системы, сервисы, сети, устройства, облачные и внешние ресурсы, используемые для деятельности Общества;

– на иных лиц, получающих доступ к активам Общества.

5.2. Требования Политики учитываются также при взаимодействии с контрагентами, клиентами и иными третьими лицами, если им предоставляется доступ к информации или системам Общества либо если они обрабатывают информацию Общества.

6. Объекты защиты

Категория	Состав
Информация клиентов	Информация, включая персональные данные, обрабатываемая в облачных сервисах Общества, при сопровождении ПО и при работе в информационных системах клиентов

Разрабатываемое ПО Общества и средства его создания	Исходный код, артефакты и образы сборки, средства разработки, сборки, хранения и распространения ПО
Персональные данные, обрабатываемые Обществом как оператором	Персональные данные работников и иных лиц
Коммерческая тайна	Информация, в отношении которой в Обществе введен режим коммерческой тайны
Аутентификационная и ключевая информация	Пароли, ключи доступа, криптографические ключи, токены, секреты, используемые в ПО и инфраструктуре
Информационные системы и инфраструктура	Серверы, облачные ресурсы, сети, рабочие места, носители, резервные копии, СЗИ
Сведения о мерах защиты	Информация об устройстве и настройках защиты информационных систем Общества
Иная служебная информация	Информация, используемая в деятельности Общества

7. Управление рисками и исключениями

7.1. Общество проводит регулярную оценку рисков и их обработку.

7.2. Оценка рисков и их обработка регламентируется Положением по управлению рисками и Регламентом оценки и обработки рисков ИБ.

7.3. Общество определяет аппетит к риску ИБ и критерии принятия риска, которые утверждаются и пересматриваются ежегодно в ходе анализа со стороны высшего руководства.

7.4. Служба ИБ организует оценку рисков ИБ.

7.5. Для каждого риска назначается Владелец риска и фиксируется в реестре рисков.

7.6. Реестр рисков ведет Служба ИБ.

7.7. Владелец риска принимает остаточный риск в пределах критериев принятия. Остаточный риск, превышающий критерии принятия, принимает высшее руководство.

7.8. Отступление от требования документов по ИБ допускается только в виде исключения, которое регламентируется Порядком оформления исключения.

7.9. Исключение не может разрешать нарушение законодательства Российской Федерации и ее субъектов, а также договорных требований клиентов.

7.10. Реестр исключений ведет Служба ИБ.

8. Модель ролей и обязанностей

8.1. В Обществе устанавливаются следующие ключевые роли:

- Высшее руководство;
- Служба ИБ;
- Ответственный за организацию обработки ПДн;
- Владельцы информационных активов и систем;
- Владельцы рисков;
- Служба ИТ;
- DevOps;
- Юристы;
- Руководители подразделений;
- Сотрудники.

8.2. Матрица ответственности (RACI) представлена в приложении 1.

8.3. Краткое описание ролей и их обязанностей

Высшее руководство:

- утверждает Политику и существенные изменения к ней;
- утверждает цели ИБ;
- утверждает аппетит к риску, критерии принятия риска;
- принимает риски;
- принимает решения об исключениях от требований ИБ;
- обеспечивает выделение необходимых ресурсов;
- проводит анализ ИБ со стороны руководства;
- осуществляет общее руководство системой управления ИБ.

Служба ИБ:

- является владельцем Политики, инициирует ее пересмотр и организует актуализацию Политики;
- организует функционирование системы управления ИБ;
- разрабатывает документацию по ИБ;
- организует оценку рисков;
- ведет реестры рисков, исключений, договорных требований по ИБ;
- организует обучение, контроль, внутренний аудит ИБ и реагирование на инциденты ИБ.

Ответственный за организацию обработки ПДн:

- организует выполнение требований законодательства о защите ПДн, в том числе обязательств по поручениям клиентов;
- участвует в реагировании на инциденты ИБ с ПДн.

Владельцы информационных активов и систем:

- определяют ценность и классификацию активов;
- определяют требования к защите, допустимый режим доступа и использования;
- определяют бизнес-требования к системе;
- согласуют роли доступа и предоставление доступа, включая привилегированный доступ;
- участвуют в периодическом пересмотре прав доступа.

Служба ИТ:

- реализуют и сопровождают технические меры ИБ во внутренней корпоративной ИТ-инфраструктуре;
- обеспечивают исполнение утвержденных решений по доступу во внутренней корпоративной ИТ-инфраструктуре;
- обеспечивают реализацию мер ИБ во внутренней корпоративной ИТ-инфраструктуре;
- ведут администрирование внутренней корпоративной ИТ-инфраструктуры и систем в пределах полномочий.

DevOps:

- реализуют и сопровождают технические меры ИБ в облачной инфраструктуре, процессах разработки и поставки ПО;
- обеспечивают исполнение утвержденных решений по доступу к сервисам и системам облачной инфраструктуры, процессов разработки и поставки ПО;
- обеспечивают реализацию мер ИБ в облачной инфраструктуре, процессах разработки и поставки ПО;
- ведут администрирование облачной инфраструктуры и систем в пределах полномочий.

Юристы:

- оказывают содействие и помощь службе ИБ при ведении реестра договорных требований по ИБ;
- организуют выполнение требований законодательства при оценке рисков, организации СУИБ и разработке документации.

Руководители подразделений:

- обеспечивают соблюдение и выполнение требований ИБ работниками подразделения;

– инициируют и подтверждают служебную необходимость предоставления, пересмотра и отзыва доступа работников к сервисам и системам;

– обеспечивают своевременное информирование об изменении статуса работников, влияющем на доступ;

– оказывают содействие расследованию инцидентов ИБ.

Сотрудники:

– обязаны соблюдать требования Политики и внутренних документов;

– используют предоставленные доступы только в служебных целях;

– незамедлительно сообщают о компрометации учетных данных, утрате устройств и иных признаках инцидентов ИБ;

– не передают учетные данные и средства аутентификации другим лицам;

– проходить обязательное обучение и инструктажи по ИБ.

9. Основные направления информационной безопасности

9.1. Общество определяет основные направления деятельности по обеспечению ИБ на организационные, технические и правовые.

9.2. Организационные меры ИБ:

- Назначение ответственных за ИБ;
- Классификация и управление активами;
- Управление доступом;
- Управление использованием ИИ-сервисов и ИИ-агентов;
- Обучение и повышение осведомленности работников в области ИБ;
- Организация физической безопасности инфраструктуры;
- Организация безопасной эксплуатации инфраструктуры;
- Управление инцидентами ИБ;
- Управление непрерывностью деятельности.

9.3. Технические меры ИБ:

- Защита от несанкционированного доступа;
- Защита от вирусов и иного вредоносного ПО;
- Криптографическая защита каналов передачи информации;
- Защита периметра корпоративной инфраструктуры;
- Мониторинг событий ИБ;
- Резервное копирование.

9.4. Правовые меры ИБ:

- Соответствие требованиям законодательства и договорным обязательствам;
- Включение требований ИБ в трудовые договоры и договоры с клиентами;
- Ответственность за нарушение требований ИБ.

10. Ответственность за нарушения требований

10.1. Нарушение требований Политики может повлечь применение мер ответственности в соответствии с законодательством Российской Федерации, локальными актами и условиями договоров.

11. Порядок пересмотра Политики

11.1. Политика пересматривается не реже **одного раза в год**.

11.2. Внеплановый пересмотр осуществляется при существенных изменениях в законодательстве, бизнес-процессах, организационной структуре, информационной инфраструктуре, модели угроз, результатах инцидентов или контрольных мероприятий.

11.3. Инициатором пересмотра может выступать владелец Политики или высшее руководство.

11.4. Изменения утверждаются высшим руководством в порядке, установленном для внутренних локальных актов Общества.

12. Заключительные положения

12.1. Политика вступает в силу с даты утверждения.

12.2. В случае противоречия между настоящей Политикой и документами более низкого уровня применяется настоящая Политика, если иное не вытекает из законодательства.