

Общество с ограниченной ответственностью «ФотоЭЦП»

199034, г. Санкт-Петербург, линия 9-я В.О., дом 4, литер А, помещение 5-Н, р.м. 13

ПОЛИТИКА
информационной безопасности
Общества с ограниченной ответственностью «ФотоЭЦП»

1. Назначение и правовая основа политики информационной безопасности

1.1. Настоящая Политика информационной безопасности Общества с ограниченной ответственностью «ФотоЭЦП» (далее – Общество) определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих Положений, Правил, Инструкций.

1.2. Настоящая Политика является документом, доступным любому сотруднику Общества и пользователю его ресурсов, и представляет собой официально принятую руководством Общества систему взглядов на проблему обеспечения информационной безопасности.

1.3. Руководство Общества осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства, а также ожиданий сотрудников, клиентов, партнёров Общества и других заинтересованных сторон. Обеспечение информационной безопасности – необходимое условие для успешного осуществления деятельности Общества. Нарушения в данной области могут привести к серьезным последствиям, включая потерю доверия со стороны сотрудников, клиентов, партнёров Общества и других заинтересованных сторон.

1.4. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения безопасности защищаемой информации, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим средствам разведки и технической защиты информации, и основывается, в том числе, на:

- Доктрине информационной безопасности Российской Федерации (утвержденной Указом Президента Российской Федерации 05.12.2016 года № 646);
- Федеральном законе от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральном законе от 27.07.2006 года № 152-ФЗ «О персональных данных».
- Федеральном законе от 06.04.2011 года № 63-ФЗ «Об электронной подписи».

1.5. Необходимые требования обеспечения информационной безопасности Общества должны неукоснительно соблюдаться сотрудниками и рабочим персоналом Общества и другими сторонами как это определяется положениями внутренних нормативных документов Общества, а также требованиями договоров и соглашений, стороной которых является Общество.

1.6. Настоящая Политика распространяется на процессы Общества и обязательна для применения всеми сотрудниками и руководством Общества, а также пользователями его информационных ресурсов.

2. Термины и определения

В настоящей Политике использованы термины с соответствующими определениями законодательства Российской Федерации и норм права в части обеспечения информационной безопасности, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

2.1. **Информация** - сведения (сообщения, данные) независимо от формы их представления.

2.2. **Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2.3. **Информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

2.4. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.5. **Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.6. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.7. **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

2.8. **Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.9. **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.10. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.11. **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных

данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.12. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

2.14. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.15. Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.16. Режим обработки персональных данных - организационно-технические мероприятия по защите персональных данных, позволяющие Оператору персональных данных при существующих или возможных обстоятельствах обеспечить целостность, доступность и конфиденциальность персональных данных, избежать неоправданных расходов, и реализующие меры по охране персональных данных, включающие в себя:

- определение перечня персональных данных в соответствии с целями и задачами обработки, требованиями Федерального закона от 27.07.2006 года №152 «О персональных данных»;
- ограничение доступа к персональным данным путем установления порядка обращения с ними и контроля за соблюдением такого порядка;
- определение класса информационной системы, в которой осуществляется обработка персональных данных;
- учет лиц, получивших доступ к персональным данным, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию персональных данных работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров и соглашений.

2.17. Рисковое событие информационной безопасности - это событие, обусловленное операционным риском, повлекшее или способное повлечь за собой потери Общества и произошедшее по причине ошибочности или сбоя процессов Общества, действий людей и систем, а также по причине внешних событий.

2.18. Угроза информационной безопасности - операционный риск, влияющий на нарушение одного (или нескольких) свойств информации - целостности, конфиденциальности, доступности.

2.19. Уязвимость – любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

3. Цели и задачи, принципы обеспечения информационной безопасности

3.1 Целями деятельности по обеспечению информационной безопасности Общества являются:

- снижение угроз информационной безопасности до приемлемого для Общества уровня;
- защита персональных данных, обрабатываемых в информационной системе Общества; защита информационной системы от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи;
- минимизация уровня рисков.

3.2 Основные задачи деятельности по обеспечению информационной безопасности Общества:

- отнесение информации к категории несекретной, ограниченного распространения, коммерческой и другим видам тайн, иной конфиденциальной информации, информации персонального характера подлежащей защите от неправомерного использования;
- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам Общества, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования Общества с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Общества, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного предотвращения и локализации ущерба, наносимого неправомерными действиями физических и (или) юридических лиц.

3.3 Построение системы обеспечения безопасности информации Общества и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- **законности** – соблюдение законодательства по защите информации, защите персональных данных и законных интересов всех участников информационного обмена;
- **системности** – подход к вопросам организации информационной безопасности должен быть логическим и последовательным: в первую очередь категорирование обрабатываемой информации, информационной системы, оценка риска информационной безопасности исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику Общества;

- **эффективности** – реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению информационной безопасности должны сводить риски к приемлемому уровню, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;
- **целесообразности** – соблюдение соразмерности затрат на обеспечение защиты информации и потенциальных потерь при реализации угроз;
- **непрерывности** – принцип функционирования системы информационной безопасности, учитывающий, что злоумышленники в любой момент времени ищут возможность обхода защитных мер, прибегая для этого к легальным и нелегальным методам;
- **взаимодействию и координации** – осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи структурных подразделений Общества, информационных технологий и подразделений-пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания информационных систем, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными государственными органами. Эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться подготовленными сотрудниками Общества;
- **совершенствованию** – совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;
- **приоритетности** – категорирование (ранжирование) информации и всех информационных ресурсов Общества по степени важности и оценка реальных, а также потенциальных угроз информационной безопасности;
- **информированности и персональной ответственности** – пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации, информационных сервисов индивидуально идентифицирующих и аутентифицирующих пользователей и иницилируемые ими процессы;
- **обязательность контроля** – контроль за деятельностью пользователей, а также мониторинг работы информационной системы должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия.

4. Объекты информационной безопасности

4.1 Основными объектами защиты системы информационной безопасности в Общества являются:

- персональные данные, информационные ресурсы обрабатывающие персональные данные, сведения ограниченного распространения, независимо от формы и вида их представления;

- информационные ресурсы, содержащие персональные данные физических лиц;
- сотрудники Общества, являющиеся пользователями информационных ресурсов (систем) Общества;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее 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;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) информационной системы Общества, с помощью которых производится обработка защищаемой информации;
- помещения, предназначенные для обработки персональных данных, сведений конфиденциального (персонального) характера;
- помещения, в которых расположены средства обработки защищаемой информации;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

4.2 Подлежащая защите информация может находиться:

- на бумажных носителях;
- в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);
- передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;
- в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;
- записываться и воспроизводиться с помощью программных и технических средств (диктофоны, видеоманитофоны и др.).

4.3 Среда информационного обмена обеспечивается, в том числе, общедоступными информационными ресурсами.

5. Угрозы информационной безопасности

5.1 Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

- несанкционированное распространение (передача) персональных данных;
- утрата сведений, составляющих конфиденциальную информацию, персональные данные Общества и иную защищаемую информацию, а также искажение такой информации;
- утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);

- недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;

- отсутствие планирования и контроля;
- низкая степень надежности программного обеспечения;
- недостаточная осведомленность персонала, низкая квалификация персонала и пользователей в области информационных технологий.

5.2 В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Общества и его нормальное функционирование:

- финансовые потери, связанные с утечкой или разглашением защищаемой информации;
- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
- ущерб от дезорганизации деятельности Общества и потери, связанные с невозможностью выполнения им своих обязательств;
- моральные потери (ущерб репутации Общества).

6. Меры обеспечения информационной безопасности

6.1 Требования об обеспечении информационной безопасности Общества и обработке персональных данных обязательны к соблюдению всеми работниками Общества и пользователями информационных систем.

6.2 Руководство Общества приветствует и поощряет в установленном порядке деятельность работников Общества и пользователей информационных систем по обеспечению информационной безопасности.

6.3 Неисполнение или некачественное исполнение сотрудниками Общества и пользователей информационных систем обязанностей по обеспечению информационной безопасности и обработке персональных данных может повлечь применение к виновным административных мер воздействия, степень которых определяется установленным в Обществе порядком либо требованиями действующего законодательства.

6.4 Система обеспечения безопасности информационных ресурсов должна соответствовать экономической целесообразности.

6.5 Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, технических, криптографических, программных средств и мер по защите информации в процессе документооборота, при работе работников с персональными данными, конфиденциальными документами и сведениями, при обработке информации в информационных системах различного уровня и назначения, при передаче по каналам связи, при ведении деловых переговоров.

6.6 Управление рисками информационной безопасности в Общества включает в себя:

- анализ влияния на информационную безопасность Общества применяемых в деятельности Общества технологий, а также внешних по отношению к Общества событий;
- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
- определение моделей угроз, выявление, анализ и оценка значимых для Общества угроз информационной безопасности;
- выявление возможных негативных последствий для Общества, наступающих в результате проявления рисков информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Общества;
- идентификацию и анализ рисков событий информационной безопасности;
- оценку величины рисков информационной безопасности и выявление рисков, неприемлемых для Общества;
- оценку влияния защитных мер на цели основной деятельности Общества;
- оценку затрат на реализацию защитных мер.

6.7 Организационные меры обеспечения информационной безопасности включают в себя:

- организацию контроля доступа в здания и помещения Общества, предназначенные для обработки сведений конфиденциального и персонального характера;
- разработку и осуществление разрешительной системы допуска работников к работам с документами и персональными данными;
- заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности, обработки персональных данных и сохранность конфиденциальной информации (персональных данных);
- установление единого порядка хранения и обращения персональных данных, конфиденциальной информации (носителей информации);
- координацию работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи;
- проведение периодического обучения и повышения квалификации работников Общества в области информационной безопасности;
- минимизацию данных конфиденциального (персонального) характера, доступных работникам;
- обеспечение физической сохранности автоматизированной системы и дополнительного оборудования;
- практическую проверку функционирования мер защиты обработки персональных данных и конфиденциальной информации.

6.8 Технические меры обеспечения информационной безопасности включают в себя:

- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам информационных систем Общества и информации, обрабатываемой в них;

- применение программных, программно-аппаратных средств криптографической защиты информации;
- обеспечение бесперебойной работы информационной системы обработки персональных данных и сети связи;
- обеспечение возобновления работы информационных ресурсов и сети связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- применение средств обнаружения вторжений;
- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
- предотвращения несанкционированного изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;
- проверку машинных и ручных протоколов выполнения работ со стороны пользователей;
- применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме (пассивная защита).

6.9 Управление инцидентами информационной безопасности в Общества включает в себя:

- сбор информации о событиях информационной безопасности;
- выявление и анализ инцидентов информационной безопасности;
- расследование инцидентов информационной безопасности;
- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства Общества информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности.

7. Структура управления политикой информационной безопасности

7.1 В целях выполнения задач по обеспечению информационной безопасности Общества, в Обществе определены следующие роли:

- Руководитель Общества.
- Ответственный за обработку персональных данных.
- Администратор сети.
- Руководители структурных подразделений
- Работники Общества.

7.2 При необходимости могут быть определены и другие роли по информационной безопасности.

7.3 Общее руководство обеспечением информационной безопасности Общества осуществляет руководитель Общества.

7.4 Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Общества лежит на **ответственном за обработку персональных данных**.

7.5 Ответственность преподавательского состава и работников Общества за невыполнение настоящей Политики определяется законодательством Российской Федерации, а также положениями внутренних нормативных документов (локальных актов) Общества.

7.6 Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Общества осуществляются и координируются ответственным за обработку персональных данных.

7.7 Задачи ответственного за обработку персональных данных и преподавательского состава Общества по обеспечению информационной безопасности определяются законодательством Российской Федерации и локальными актами Общества.

7.8 Руководитель Общества может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые ответственным за обработку персональных данных, и может, при необходимости привлекать для работы в них ответственных сотрудников других подразделений Общества на основе совмещения работы в группе со своими основными должностными обязанностями.

7.9 Финансирование работ по реализации положений настоящей Политики осуществляется в рамках бюджета Общества.

8. Контроль за соблюдением положений Политики

8.1 Общий контроль состояния информационной безопасности Общества осуществляется Руководителем Общества.

8.2 Контроль соблюдения настоящей Политики осуществляет ответственный за обработку персональных данных на основе проведения внутреннего аудита информационной безопасности.

8.3 Контроль осуществляется путем проведения мониторинга и управлением инцидентов информационной безопасности Общества, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

9. Заключительные положения

9.1 Требования настоящей Политики могут развиваться другим внутренними нормативными документами Общества, которые дополняют и уточняют ее.

9.2 В случае изменения действующего законодательства и иных нормативных актов, а также Устава Общества настоящая Политика и изменения к

ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Общества. В этом случае ответственный за обработку персональных данных обязан незамедлительно инициировать внесение соответствующих изменений.

9.3 Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

- периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 12 месяцев;
- внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.