Приложение № 1
УТВЕРЖДЕНО
приказом генерального директора АО
«Тулаточмаш»

ПОЛИТИКА
информационной безопасности
АО «Тулаточмаш»

1 Область применения

Настоящая политика в соответствии с Федеральными законами «Об информации, информационных технологиях и защите информации», «О коммерческой тайне», «О персональных данных» и иными нормативно-правовыми актами Российской Федерации определяет систему взглядов на обеспечение безопасности информации и представляет собой систематизированное изложение целей и задач защиты информационной безопасности, которыми необходимо руководствоваться в своей деятельности, а также основных принципов обеспечения безопасности информации в АО «Тулаточмаш».

Политика обязательна для исполнения всеми работниками АО «Тулаточмаш» и является локальным нормативно-правовым актом, регламентирующим принципы обеспечения информационной безопасности на предприятии.

Политика учитывает современное состояние и ближайшие перспективы развития информационных технологий в АО «Тулаточмаш», а также цели, задачи и правовые основы их эксплуатации, режимы функционирования.

Законодательной основой настоящей Политики являются:
- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;
- 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»;
- Законодательство и национальные стандарты России, действующие в области защиты информации и создания операционных систем.

Политика разработана в соответствии с требованиями ГОСТ Р ИСО 9001-2015, ГОСТ РВ 0015-002-2012.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности

информации.

2 Термины и определения

Автоматизированная система обработки информации - организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно- структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей в деятельности АО «Тулаточмаш».

Безопасность информации - защищенность информации от нежелательного ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Вредоносные программы - программы или измененные программы объекта информатизации, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы.

Документ - зафиксированная на материальном носителе информация с реквизитами, позволяющими его идентифицировать.

Доступность информации - важнейшее свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

Злоумышленник - нарушитель, действующий намеренно из корыстных, идейных или иных побуждений.

Информация – сведения (сообщения, данные) о деятельности АО «Тулаточмаш», об иных предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах.

Информационная система - организационно упорядоченная совокупность документов (массивов документов), независимо от формы их представления, и информационных технологий, в том числе с использованием вычислительной техники и связи.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой

осуществляется с использованием средств вычислительной техники.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к информации, требование не передавать такую информацию третим лицам без согласия АО «Тулаточмаш».

Корпоративная информационная система – совокупность систем обработки информации АО «Тулаточмаш».

Нарушитель - лицо, которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных действий с данным ресурсом) по ошибке, незнанию или осознанно с умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства.

Несанкционированный доступ – возможность доступа лица к объекту в нарушение установленных в системе правил разграничения доступа.

Объект - пассивный компонент системы, единица ресурса информационной системы, доступ к которому регламентируется правилами разграничения доступа.

Объект защиты - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Организационные меры защиты - меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Пароль - слово (набор символов), которое считается известным узкому кругу лиц (одному лицу) и используется для ограничения доступа к информации, в помещение, на территорию;

Пользователь - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;

Разграничение доступа к ресурсам - порядок использования ресурсов системы, при котором лица получают доступ к объектам в строгом соответствии с установленными правилами.

Система информационной безопасности - совокупность специальных мер правового и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности.

Субъект - активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

Угроза безопасности информации - потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации;

Уязвимость автоматизированной системы - любая характеристика

автоматизированной системы, использование которой может привести к реализации угрозы;

Целостность информации - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Цель защиты информации - предотвращение или минимизация наносимого ущерба (прямого или косвенного, материального, морального или иного) субъектам информационных отношений посредством нежелательного воздействия на компоненты информационной системы, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

3 Объекты защиты

Объектами системы информационной безопасности в АО «Тулаточмаш» являются:

- информационная инфраструктура, включающая системы обработки, хранения 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 элементы информационной среды;
- процессы обработки информации в информационной системе АО «Тулаточмаш» информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;
- информационные ресурсы с ограниченным доступом, составляющие коммерческую тайну, персональные данные работников и иную информацию ограниченного распространения в целях обеспечения ее конфиденциальности.

3.1 Общие характеристики основных объектов защиты

Информационная среда является сосредоточенной структурой, которая имеет подключения к информационно-телекоммуникационным сетям информационного обмена.

К основным особенностям информационной среды АО «Тулаточмаш» относятся:

- разнообразие технических средств обработки информации, решаемых задач и типов обрабатываемых данных;
- объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;
- высокая значимость информационных потоков;
- разнообразие категорий пользователей и обслуживающего персонала системы.

Ключевым фактором является резкое возрастание уязвимости информации, в

результате одним из важнейших элементов информационной среды становится корпоративная информационная система, в которой обрабатываются и накапливаются значительные объемы информации, совместно используемой различными категориями пользователей.

3.2 Категории информационных ресурсов, подлежащих защите

Защите подлежит вся информация и информационные ресурсы, независимо от их представления и местонахождения в информационной среде АО «Тулаточмаш».

В АО «Тулаточмаш» циркулирует информация ограниченного характера, требующая защиты ее конфиденциальности, установленной Положением об обращении и защите конфиденциальной информации, утвержденной приказом генерального директора от 09.10.2018 № 495.

4 Цели и задачи обеспечения безопасности информации

4.1 Интересы затрагиваемых субъектов информационной системы

Субъектами информационной системы при обеспечении информационной безопасности АО «Тулаточмаш» являются:

- АО «Тулаточмаш» как собственник информационных ресурсов;
- подразделения АО «Тулаточмаш», участвующие в информационном обмене;
- руководители и работники структурных подразделений, в соответствии с возложенными на них функциями;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационной системе;
- другие юридические и физические лица, задействованные в обеспечении выполнения АО «Тулаточмаш» своих функций (разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и пр.).

Перечисленные субъекты информационной системы заинтересованы в обеспечении:

- своевременного доступа к необходимой им информации (ее доступности);
- достоверности (полноты, точности, адекватности, целостности) информации;
- конфиденциальности информации;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

4.2 Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационной системы от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация рисков.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих основных свойств информации:

- доступности информации для легальных пользователей (устойчивого функционирования информационной системы, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждения авторства) информации, хранимой и обрабатываемой в информационной системе и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне информации, хранимой, обрабатываемой и передаваемой по каналам связи.

4.3 Основные задачи системы обеспечения безопасности информации

Для достижения основной цели защиты и осуществления указанных свойств информации система информационной безопасности должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценку и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационной системы посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в корпоративной информационной системе программных и технических средств средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

4.4 Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач

достигаются:

- учетом всех подлежащих защите ресурсов информационной системы (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- подготовкой должностных лиц, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;
- наделением каждого работника минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам;
- четким знанием и строгим соблюдением всеми пользователями информационной системы требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам;
- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- эффективным контролем за соблюдением пользователями информационных ресурсов, требований по обеспечению безопасности информации;
- юридической защитой интересов при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

5 Основные угрозы безопасности информации

Основными источниками угроз безопасности информации являются:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационной системы (в том числе работников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;
- преднамеренные действия легально допущенных к информационным ресурсам

пользователей, которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;
- деятельность отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационной системы в целом и ее отдельных компонентов;
- удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних информационно-телекоммуникационных сетей общего пользования;
- ошибки, допущенные при разработке компонентов информационной системы и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств;
- аварии, стихийные бедствия.

Наиболее значимыми угрозами безопасности информации для АО «Тулаточмаш» является:
- нарушение конфиденциальности (разглашение, утечка) информации, а также сведений, составляющих коммерческую тайну, персональные данные;
- нарушение функциональности компонентов информационной системы, блокирование информации, нарушение технологических процессов, своевременного решения задач;
- нарушение целостности информационных, программных и других ресурсов, а также фальсификация документов.

6 Ответственность

6.1 Лица, чьи действия повлекли нарушения принципов политики информационной безопасности предприятия либо создавшие условия возможности нарушения принципов информационной безопасности, несут ответственность, в том числе материальную, в соответствии с трудовым, гражданским, административным, уголовным и иным законодательством Российской Федерации.

6.2 В целях профилактики, предотвращения, выявления и надлежащего реагирования на нарушение принципов настоящей Политики, а также привлечения к ответственности виновных лиц, уполномоченными сотрудниками службы безопасности принимаются необходимые меры в рамках своей компетенции.

Заместитель генерального директора
по безопасности С.В. Сологуб