КРАТА
АКЦИОНЕРНОЕ ОБЩЕСТВО "ПИГМЕНТ"

Утверждаю

Генеральный директор
ООО «УК «КРАТА»
_____ Утробин А.Н.
«29» 06 2023г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «Пигмент»

г.Тамбов | 2023г.

Оглавление

1 Введение

1.1. Настоящая Политика информационной безопасности АО «Пигмент» (далее – Политика) определяет систему взглядов на проблему обеспечения информационной безопасности (ИБ).
1.2. Политика устанавливает основополагающие принципы и задачи построения системы обеспечения информационной безопасности, а также определяет высокоуровневые требования как к процессам системы управления информационной безопасностью (далее – СУИБ), так и к защитным мерам системы ИБ АО «Пигмент» (далее – Предприятие).
1.3. Деятельность Предприятия при обеспечении ИБ основывается на требованиях законодательства Российской Федерации и норм права в части обеспечения информационной безопасности и других законодательных актах, определяющих права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативных, отраслевых и ведомственных документах, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

2 Область действия

2.1. Действие данной Политики распространяется на все подразделения Предприятия. Положения данной Политики обязательны для применения всеми работниками и руководством Предприятия.
2.2. Действие данной Политики не распространяется на защиту информации, требования по защите которой определяются нормативными актами Российской Федерации в области защиты государственной тайны.
2.3. Положения данной Политики должны учитываться при разработке распорядительно-нормативных документов Предприятия по обеспечению информационной безопасности.

3 Термины и сокращения

3.1. Сокращения

АРМ	Автоматизированное рабочее место
АСУ	Автоматизированная система управления
ИБ	Информационная безопасность
ИР	Информационный ресурс
ИС	Информационная система
ИТ	Информационные технологии
СИБ	Система информационной безопасности
СУИБ	Система управления информационной безопасностью

3.2. Термины

Актив - все, что имеет ценность для Предприятия и находится в его распоряжении.

Примечание.

К активам Предприятия могут относиться:

- работники (персонал), финансовые (денежные) средства, *объекты информационной инфраструктуры, включая автоматизированные системы, программное обеспечение,* средства вычислительной техники, телекоммуникационные средства и пр.;
- различные виды информации — платежная, финансово-аналитическая, служебная, управляющая и пр.;
- производственные процессы (производственно-технологические процессы, информационные технологические процессы);
- продукты и услуги, предоставляемые клиентам.

Безопасность - состояние защищенности интересов (целей) Предприятия в условиях угроз.

Информационная безопасность (ИБ) - безопасность, связанная с угрозами в информационной сфере.

Инцидент информационной безопасности (инцидент ИБ) - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, т.е. реализацию нарушения свойств ИБ информационных активов Предприятия.

Примечание.

Нарушение может вызываться источниками угроз ИБ: либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами, например, пожаром

или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов.

ИТ-актив - все аппаратные и программные элементы ИТ-инфраструктуры, обеспечивающие деятельность бизнес-среды.

ИТ-инфраструктура - организационно-техническое объединение программных, вычислительных и телекоммуникационных средств, связей между ними и эксплуатационного персонала, обеспечивающее предоставление информационных, вычислительных и телекоммуникационных ресурсов, возможностей и услуг работникам (подразделениям) предприятия (организации), необходимых для осуществления профессиональной деятельности и решения соответствующих бизнес-задач.

ИТ-сервис - комплекс сложных индивидуализированных технологичных услуг для решения бизнес-задач потребителя по повышению эффективности, безопасности и бесперебойности деятельности компании-потребителя, основанный на взаимодействии личном и/или с применением удаленных технологий.

Политика информационной безопасности (политика ИБ) - документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для Предприятия в целом.

Система информационной безопасности (СИБ) - совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Система управления информационной безопасности (СУИБ) - часть системы Предприятия, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

Угроза информационной безопасности (угроза ИБ) - угроза нарушения свойств ИБ – доступности, целостности или конфиденциальности информационных активов Предприятия.

Ущерб - утрата активов, повреждение (утрата свойств) активов и(или) инфраструктуры организации или другой вред активам и(или) инфраструктуре Предприятия, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

Аппаратное средство - материальная часть вычислительной системы, включающая в себя электрические и электронные элементы (например, приборы и схемы), электромеханические элементы (например, дисководы) и механические элементы (например, стойки).

[ГОСТ Р 51904–2002]

Программно-аппаратное средство - сочетание технических устройств и машинных команд или используемых вычислительной машиной данных, постоянно хранящихся на техническом устройстве в виде постоянного программного средства. Данное программное средство не может изменяться только средствами программирования.

[ГОСТ Р ИСО/МЭК 12207–99]

Программное средство - программное обеспечение и связанные с ним документы, вновь созданные, модифицированные или сгруппированные для удовлетворения требованиям контракта.

[ГОСТ Р 51904–2002]

4 Цели и задачи

4.2. Целью обеспечения ИБ Предприятия является поддержание приемлемого уровня защищенности его интересов при воздействии угроз в информационной сфере. Приемлемый уровень защищенности интересов Предприятия в информационной сфере характеризуется отсутствием недопустимых для бизнеса рисков, связанных с информацией и информационной инфраструктурой.
4.3. Указанная цель достигается посредством решения следующих задач:

- выявление угроз информационной безопасности и уязвимостей объектов защиты;
- обеспечение соответствия требованиям законодательства Российской Федерации;
- обеспечение конституционных прав граждан по сохранению личной тайны и обеспечению безопасности персональных данных;
- обеспечение режима коммерческой тайны;
- обеспечение безопасности информации не являющейся коммерческой тайной, но требующей защиты;
- обеспечение необходимого уровня защищенности используемых Предприятием технологических процессов в зависимости от их значимости для реализации целей бизнеса Предприятия;
- планирование, реализация и контроль использования защитных мер ИБ, прогнозирование развития событий на основе мониторинга и анализа инцидентов ИБ;
- координация всех видов деятельности Предприятия в целях обеспечения ИБ, в том числе и через инициирование/согласование/принятие соответствующих внутренних документов ИБ Предприятия, реализацию программ по осведомленности и обучению персонала Предприятия.
- минимизация ущерба и быстрое восстановление видов деятельности Предприятия, пострадавших в результате кризисных ситуаций, участие в расследовании причин возникновения таких ситуаций и принятии соответствующих мер по их предотвращению;
- своевременное информирование руководства Предприятия о состоянии ИБ Предприятия.

5 Объекты информационной безопасности

5.1. К основным объектам защиты системы информационной безопасности относятся:

- информационные активы и информационные ресурсы, содержащие информацию, составляющую коммерческую и иную охраняемую законом тайну, персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы Предприятия, независимо от формы и вида ее представления;
- процессы обработки информации в информационных системах Предприятия – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей информационных систем и их обслуживающий персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, и другие объекты информационной инфраструктуры, каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены активы Предприятия и элементы информационной среды.

6 Объекты обеспечения информационной безопасности

6.1. В рамках обеспечения информационной безопасности объектами защиты на Предприятии являются информация, обрабатываемая на Предприятии, вне зависимости от формы представления; ИТ-активы, включая, но не ограничиваясь следующим перечнем:

- АРМ, средства обработки информации и мобильные технические средства;
- ИС, системы хранения данных, программное обеспечение и отдельные технические решения;
- АСУ, системы метрологии и промышленной автоматизации, в том числе измерительные системы;
- ИТ-инфраструктура, информационно-телекоммуникационные сети и системы связи;
- ИТ-сервисы (ИТ-услуги), оказываемые Предприятием или в интересах Предприятия;
- решения по цифровизации бизнес- и технологических (производственных) процессов.

7 Принципы обеспечения информационной безопасности

7.1. При осуществлении всех видов деятельности по обеспечению ИБ необходимо руководствоваться следующими общими принципами:

– **своевременность обнаружения проблем**, означающий, что должны своевременно обнаруживаться проблемы, потенциально способные повлиять на цели бизнеса Предприятия;

– **прогнозируемость развития проблем**, означающий, что на основе выявления причинно-следственных связей возможных проблем должно обеспечиваться прогнозирование их развития;

– **адекватность защитных мер**, означающий, что выбираемые защитные меры, должны быть адекватны модели угроз информационной безопасности и нарушителей;

– **эффективность защитных мер**, означающий, что используемые защитные меры, оптимальны с точки зрения минимизации затрат на их реализацию и достижения целей ИБ;

– **комплексность и системность**, означающий, что обеспечение ИБ должно предусматривать обоснованное и непрерывное использование взаимоувязанных программно-технических, организационных, правовых, нормативно-методических и других мер обеспечения ИБ, основанных на оценке рисков ИБ;

– **упреждающий характер защитных мер**, означающий, что деятельность по обеспечению ИБ должна быть направлена в первую очередь на предотвращение (по возможности) проявлений угроз ИБ;

– **согласованность защитных мер**, означающий, что защитные меры должны быть согласованы между собой и скоординированы по применению;

– **унифицированность решений по обеспечению ИБ**, означающий, что на Предприятии должны внедряться унифицированные решения в области ИБ, способствующие сокращению затрат и повышению отдачи от инвестиций в ИБ;

– **контролируемость защитных мер**, означающий, что должны применяться только те защитные меры, правильность работы которых может быть проверена;

– **персонификация и адекватное разделение ответственности**, означающий, что ответственность должностных лиц за решения, связанные с обеспечением ИБ, должна персонифицироваться. Ответственность должна быть адекватна степени влияния на цели бизнеса Предприятия;

– **информационная безопасность как неотъемлемое свойство ИТ-актива -** ***принцип заключается в следующем:***

- требования информационной безопасности учитываются на всех этапах жизненного цикла ИТ-актива, вне зависимости от уровня конфиденциальности информации, обрабатываемой в ИТ-активе;
- создание программных продуктов в интересах Предприятия осуществляется с применением методов безопасной разработки программного обеспечения;
- предпочтительными являются ИТ-активы с наибольшим покрытием требований информационной безопасности встроенными функциями (при прочих равных характеристиках);

- встроенные функции по информационной безопасности должны быть настроены и использоваться при эксплуатации ИТ-активов, включая программно-аппаратные средства, автоматизированные системы управления и т.д.;
- соответствие приобретаемого/внедряемого ИТ-актива требуемому уровню информационной безопасности подтверждается согласно существующими процедурами, с учетом требований применимого законодательства.

– **информационная безопасность как неотъемлемое свойство ИТ-сервиса (ИТ-услуги)** означает, что предлагаемые и оказываемые Предприятию или в интересах Предприятия ИТ-услуги и ИТ-сервисы должны разрабатываться и оказываться с учетом требований информационной безопасности.

- **совместимость** - подразумевает подбор компонентов для обеспечения информационной безопасности способом, гарантирующим их взаимную системную совместимость на информационном, программном, электромагнитном и эксплуатационном уровнях, а также совместимость с используемыми ИТ-решениями, информационными технологиями и с решениями по автоматизации технологических и производственных процессов Предприятия.
- **надежность** - использование компонентов и средств для обеспечения информационной безопасности, соответствующих требованиям по надежности, готовности и обслуживаемости.
- **адекватность и обоснованность решений** - принимаемые на Предприятии меры и применяемые средства информационной безопасности эффективны, результативны и соразмерны с величиной ИБ-рисков и угроз информационной безопасности, влияющих на цели Предприятия.
- **комплексность** - применение любых доступных законных методов, средств и мероприятий (включая законодательные и нормативно-правовые, организационно-административные, программно-технические, инженерно-технические, физические), направленных на снижение ИБ-рисков, пресечение угроз информационной безопасности и недопущение ущерба Предприятию, её Деловым партнёрам и работникам.
- **разделение и минимизация полномочий** - означает, что выполнение критичных операций проводится только посредством разделения действий (например, алгоритмического разделения, временного или ресурсного - в т.ч. двумя работниками). Исключение единоличного совершения критичной операции может быть организовано на уровне организационных мер и/или программно-технических средств за счет выделения полномочий или роли пользователя. Программно-технический способ разделений полномочий является предпочтительным относительно организационного. Должны осуществляться контроль реализации принципов разграничения критических полномочий в ИС, ограничение прав доступа, в зависимости от уровня согласованных полномочий. При необходимости должен осуществляться контроль конфликта полномочий - организационный, а также программно-аппаратный.

8 Оценка и обработка рисков

8.1. Предприятие идентифицирует, оценивает риски в области ИБ. Оценка производится с учетом вероятности возникновения и/или величины потерь. Результаты оценки дают возможность сформулировать соответствующие требования по ИБ и принять меры для защиты от этих рисков.

8.2. Оценка рисков по ИБ производится:

- в плановом порядке с установленной периодичностью;

- внепланово с целью:

  - учета изменений бизнес-требований и приоритетов;
  - принятия во внимание новых угроз и уязвимостей;
  - получения подтверждения о том, что реализованные средства сохранили свою эффективность.

8.3. Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

- применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
- уклонение от риска путём недопущения действий, которые могут быть его причиной;
- сознательное и объективное принятие риска;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

9 Ответственность

9.1. Управляющий директор Предприятия определяет приоритетные направления деятельности в области ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство СУИБ Предприятия.

9.2. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Предприятия закрепляется за начальником отдела информационной безопасности.

9.3. Все Руководители структурных подразделений Предприятия несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях.

9.4. Работники Предприятия несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в отдел ИБ.

9.5. Руководство Предприятия регулярно проводит совещания, посвящённые проблемам обеспечения информационной безопасности с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения.

9.6. Нарушение политики по ИБ и других нормативных документов по ИБ, действующих на предприятии, влечет за собой проведение внутреннего расследования и определение мер наказания за выявленное нарушение.