

УТВЕРЖДАЮ

Директор УП «МИНСКИНЖПРОЕКТ»

_____ А.П. Говорко

«_____» _____ 2021

ПОЛОЖЕНИЕ

о политике информационной безопасности

1. Политика информационной безопасности (далее – Политика) УП «МИНСКИНЖПРОЕКТ» (далее – Предприятие) разработана в соответствии с требованиями нормативных правовых актов, регламентирующими защиту информации, и является основополагающим документом предприятия в сфере информационной безопасности (далее – ИБ).

2. Политика представляет собой изложение целей и задач обеспечения ИБ.

3. Предприятие стремится выбирать меры обеспечения ИБ, с учетом финансовых, материальных и иных затрат на их реализацию, вероятности возникновения угроз ИБ и объема возможных потерь от их реализации.

4. Под информационной безопасностью понимается состояние информационной системы (далее – ИС) и ее инфраструктуры, направленное на сохранение конфиденциальности, целостности, подлинности, доступности информации.

5. Под нежелательными воздействиями на ИС предприятия понимаются:

5.1. преднамеренные действия злоумышленников;

5.2. ошибочные и преднамеренные действия пользователей и администраторов;

5.3. проявления ошибок в системном и прикладном программном обеспечении;

5.4. сбои и отказы оборудования.

6. В предприятии защите подлежат все ИС, в которых обрабатывается информация.

7. ИБ достигается реализацией соответствующего набора организационных, правовых и технических мер управления ИБ.

ЦЕЛИ ОБЕСПЕЧЕНИЯ ИБ

8. Основными целями Политики являются:

8.1. обеспечение безопасности ИС предприятия, информационных ресурсов, связанных с производственными и иными процессами;

8.2. соответствие ИБ требованиям национального законодательства, международных норм (стандартов);

8.3. эффективное управление ИБ и непрерывное совершенствование системы управления ИБ;

8.4. достижение соразмерности мер по защите от угроз ИБ;

8.5. повышение деловой репутации и корпоративной культуры предприятия;

8.6. своевременное обеспечение пользователей и администраторов актуальной информацией о рисках и угрозах в сфере ИБ.

ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИБ

9. Защита информации является неотъемлемой составной частью основной деятельности всех структурных подразделений предприятия и достигается проведением комплекса правовых, организационных, технических и методических мероприятий, направленных на предотвращение или преодоление угроз безопасности информации в зависимости от условий деятельности и решаемых на конкретном периоде задач.

10. Для достижения целей обеспечения ИБ предприятия должны решаться следующие задачи:

10.1. соблюдение требований нормативных правовых актов Республики Беларусь, регламентирующих порядок обработки и хранения информации;

10.2. прогнозирование и своевременное выявление источников угроз безопасности информации, причин и условий, способствующих реализации угроз, оценка рисков, создание механизма оперативного реагирования на угрозы ИБ;

10.3. предотвращение действий, направленных против нарушения конфиденциальности, целостности, доступности, подлинности и сохранности информации;

10.4. предотвращение доступа неавторизованных пользователей и разграничение доступа зарегистрированных пользователей к ИС;

10.5. защита от несанкционированной модификации и контроль целостности используемых в ИС программных средств;

10.6. регистрация действий пользователей и администраторов в системных журналах и периодический контроль корректности их действий;

10.7. обеспечение аутентификации пользователей;

10.8. обнаружение и деактивация вредоносных программ;

10.9. согласованность действий по обеспечению ИБ, с применением экономически целесообразных мер;

10.10. совершенствование системы управления ИБ;

10.11. повышение работниками предприятия осведомленности в вопросах обеспечения ИБ;

10.12. анализ функционирования систем обеспечения ИБ, контроль защитных мер, оценка их эффективности;

10.13. минимизация и локализация ущерба, наносимого интересам предприятия реализацией угроз ИБ и принятие соответствующих мер по их предотвращению.

11. Перечень ИС, отнесенных к соответствующим классам типовых информационных систем, а также отдельно стоящих электронных вычислительных машин, используемых на предприятии, обязанности пользователей, порядок взаимодействия с внешними ИС, а также другие вопросы в сфере ИБ определяются отдельными локальными нормативными правовыми актами предприятия.

12. Для обеспечения конфиденциальности информации в гражданско-правовых договорах, которые предусматривают возможность приема и (или) передачи информации предприятия, неподлежащей разглашению, предусматриваются условия о конфиденциальности.