УТВЕРЖДЕНО
Приказ генерального директора
БелНИИТ «Транстехника»
07.03.2024 № 43

ПОЛОЖЕНИЕ
о политике информационной безопасности

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности Республиканского унитарного предприятие БелНИИТ «Транстехника» (далее – Политика) разработана в соответствии с требованиями Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66.

Нормативной правовой основой Политики служат:

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

Указ Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации»;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»;

иные нормативные правовые акты Республики Беларусь в области информатизации, безопасности и защиты информации, международные стандарты в области информационной безопасности продуктов и систем информационных технологий.

2. Политика определяет общие цели и принципы деятельности по защите БелНИИТ «Транстехника» от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на информационные системы (далее – ИС), а также минимизации рисков информационной безопасности (далее – ИБ).

3. Настоящей политикой не регулируются отношения в области защиты информации, отнесенной к государственным секретам.

4. Положения Политики является обязательными для работников - БелНИИТ «Транстехника».

5. Политика подлежит актуализации в связи с изменением в законодательстве Республики Беларусь в области защиты информации.

ГЛАВА 2
ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОИ БЕЗОПАСНОСТИ

6. Требования об обеспечении информационной безопасности обязательны к соблюдению всеми работниками БелНИИТ «Транстехника».

7. Стратегия БелНИИТ «Транстехника» в части противодействия угрозам ИБ заключается в реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства БелНИИТ «Транстехника», до специализированных мер информационной безопасности по каждому выявленному риску в БелНИИТ «Транстехника».

8. Основными объектами защиты системы информационной безопасности в БелНИИТ «Транстехника» являются:

информационные ресурсы, содержащие служебную тайну и конфиденциальную информацию, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы, независимо от формы и вида ее представления;

работники БелНИИТ «Транстехника» и их представители, являющиеся пользователями информационных систем.

9. Целями защиты информации является защита БелНИИТ «Транстехника» от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС, а также минимизация рисков ИБ.

10. При планировании мероприятий по обеспечению информационной безопасности в БелНИИТ «Транстехника» осуществляются:

определение и распределение функций и задач работников БелНИИТ «Транстехника», связанного с обеспечением информационной безопасности;

оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности;

управление рисками информационной безопасности.

11. В рамках реализации деятельности по обеспечению информационной безопасности в БелНИИТ «Транстехника» осуществляются:

реализация требований законодательства Республики Беларусь в части информационной безопасности ИС и мер контроля их защищенности;

минимизация ущерба, который может быть нанесен БелНИИТ «Транстехника» из-за нарушений ИБ;

разграничение доступа пользователей к ИС (предоставление доступа пользователям только к тем информационным ресурсам и выполнению только тех операций в ИС, которые необходимы пользователям для выполнения своих трудовых обязанностей);

обеспечение аутентификации пользователей;

обеспечение защиты от несанкционированной модификации используемого в ИС программного обеспечения (далее – ПО), а также защиты ИС от внедрения несанкционированных программ, включая вредоносное ПО;

обеспечение криптографической защиты информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, при ее передаче посредством сетей электросвязи общего пользования;

учет всех подлежащих защите информационных систем;

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 БелНИИТ «Транстехника» информации о наиболее значимых инцидентах информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;

взаимодействие с уполномоченными государственными органами безопасности по выявленным инцидентам;

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;

повышение уровня знаний работников БелНИИТ «Транстехника» по вопросам обеспечения информационной безопасности;

обеспечение бесперебойной работы автоматизированных систем и сетей связи;

обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;

применение средств защиты от вредоносных программ;

обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;

12. В целях проверки деятельности по обеспечению информационной безопасности в БелНИИТ «Транстехника» осуществляются:

контроль правильности реализации и использования мер защиты;

контроль изменений конфигурации систем и подсистем БелНИИТ «Транстехника»;

мониторинг факторов рисков и соответствующий их пересмотр;

13. В целях совершенствования деятельности по обеспечению информационной безопасности в БелНИИТ «Транстехника» осуществляется периодическое и, при необходимости, оперативное уточнение и пересмотр целей и задач обеспечения информационной безопасности.

ГЛАВА 3
УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

14. Под антропогенными угрозами ИБ в БелНИИТ «Транстехника» понимается:

угрозы, вызванные ошибками в проектировании информационной системы и ее элементов;

ошибки в действиях персонала и т.п.;

умышленные действия, связанные с корыстными, идейными или иными устремлениями людей;

угрозы, связанные с нестабильностью и противоречивостью требований государственных органов и иных организаций БелНИИТ «Транстехника» и контрольных органов;

15. Под техногенными угрозами ИБ в БелНИИТ «Транстехника» понимается:

угрозы объективных физических процессов техногенного характера;

техническое состояние окружения объекта угрозы или его самого, не обусловленное напрямую деятельностью человека;

сбои в работе или разрушение систем, созданных человеком, находящихся вне зоны ответственности БелНИИТ «Транстехника».

16. Под природными угрозами ИБ в БелНИИТ «Транстехника» понимается:

угрозы объективных физических процессов природного характера;

стихийных природных явлений и иных состояния природной среды.

ГЛАВА 4
МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

17. В качестве потенциальных внутренних нарушителей БелНИИТ «Транстехника» рассматриваются:

пользователи информационных систем БелНИИТ «Транстехника»;

работники, обслуживающий технические средства корпоративной информационной системы БелНИИТ «Транстехника»;

руководители различных уровней.

В качестве потенциальных внешних нарушителей БелНИИТ «Транстехника» рассматриваются:

бывшие работники БелНИИТ «Транстехника»;

сторонние организации или их представители, предоставляющие собственные ресурсы в пользование БелНИИТ «Транстехника»;

посетители зданий и помещений БелНИИТ «Транстехника»;

лица, случайно или умышленно проникшие в информационную систему БелНИИТ «Транстехника» из внешних телекоммуникационных сетей (хакеры).

В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

нарушитель скрывает свои несанкционированные действия от других работников БелНИИТ «Транстехника»;

несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства, и методы для достижения стоящих перед ним целей;

внешний нарушитель может действовать в сговоре с внутренним нарушителями.