Политика информационной безопасности ФКП «БОЗ»

1. Назначение Политики информационной безопасности.

Политика информационной безопасности ФКП «БОЗ» — это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в ФКП «БОЗ».

Политика информационной безопасности относятся к административным мерам обеспечения ИБ и определяют стратегию ФКП «БОЗ» в области ИБ.
Политика информационной безопасности регламентируют эффективную работу СЗИ. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политика ИБ реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политику, должны быть утверждены на ФКП «БОЗ».

2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

- Постоянный и всесторонний анализ информационного пространства ФКП «БОЗ» с целью выявления уязвимостей информационных активов;
- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ ФКП «БОЗ», корректировка моделей угроз и нарушителя;
- Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для
- Обеспечения ИБ, не должны усложнять достижение уставных целей ФКП «БОЗ», а также повышать трудоемкость технологических процессов обработки информации;
- Контроль эффективности принимаемых защитных мер;

- Персонификация и адекватное разделение ролей и ответственности между сотрудниками ФКП «БОЗ», исходя из принципа персональной и единоличной ответственности за совершаемые операции.

3. Соответствие Политики информационной безопасности действующему законодательству

Правовую основу Политики составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

4. Ответственность за реализацию Политики информационной безопасности

Ответственность за разработку мер обеспечения защиты информации несёт АИБ.

Ответственность за реализацию Политики возлагается:

- В части, касающейся разработки и актуализации правил внешнего доступа -на АИБа;
- В части, касающейся контроля доведения правил Политики до сотрудников ФКП «БОЗ», а также иных лиц (см. область действия настоящей Политики) — на АИБа;
- В части, касающейся исполнения правил Политики — на каждого сотрудника ФКП «БОЗ», согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей Политики.

5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе.

- Обучение сотрудников ФКП «БОЗ» в области ИБ проводится согласно плану, утвержденному Генеральным директором предприятия.

- Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности».
- Допуск персонала к работе с защищаемыми ИР ФКП «БОЗ» осуществляется только после его ознакомления с настоящей Политикой, а также после ознакомления пользователей с «Порядком работы пользователей» ФКП «БОЗ», а также иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящей Политики подтверждается подписями сотрудников в журналах ознакомления.
- Допуск персонала к работе с информацией ФКП «БОЗ» осуществляется после ознакомления с «Порядком организации работы с материальными носителями»,
- «Порядком организации работы с электронными носителями». Правила допуска к работе с ИР лиц, не являющихся сотрудниками ФКП «БОЗ», определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

6. Учетные записи.

Настоящая Политика определяет основные правила присвоения учетных записей пользователям информационных активов ФКП «БОЗ».

Регистрационные учетные записи подразделяются на:

- Пользовательские — предназначенные для идентификации/ аутентификации пользователей информационных активов ФКП «БОЗ»;
- Системные — используемые для нужд операционной системы;
- Служебные — предназначенные для обеспечения функционирования отдельных процессов или приложений.
- Каждому пользователю информационных активов ФКП «БОЗ» назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

- В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.
- Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.
- Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.
- Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

7. Использование паролей.

Настоящая Политика определяет основные правила парольной защиты на ФКП «БОЗ». Положения Политики закрепляются в «Порядке по организации парольной защиты»

8. Защита автоматизированного рабочего места.

- Настоящая Политика определяет основные правила и требования по защите информации ФКП «БОЗ» от неавторизованного доступа, утраты или модификации.
- Положения данной Политики определяются в соответствии с используемым техническим решением.