



## ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

Политика Федерального государственного бюджетного образовательного учреждения высшего образования «Брянский государственный технический университет» в области конфиденциальности – один из приоритетных факторов, определяющих концепцию, принципы и подходы в этой сфере для обеспечения защищенности образовательных, научных, исследовательских и иных процессов Университета, направленных на достижение целей, предусмотренных Уставом Университета, создающих условия безопасного цифрового развития Университета и обеспечивающих соответствие требованиям законодательства РФ в данной области.

Важнейшим инструментом обеспечения конфиденциальности является управление конфиденциальной информацией и рисками конфиденциальности, направленное на формирование действенного механизма защиты от разглашения конфиденциальной информации и, тем самым, получения экономических преимуществ от образовательной, научной, исследовательской, и инновационной деятельности Университета.

Концепция управления конфиденциальной информацией и рисками конфиденциальности включает в себя следующие методы:

- ✓ Обеспечение информационной безопасности Университета;
- ✓ Аутентификация и контроль доступа, организация обязательной аутентификации пользователей и управление доступом к системе;
- ✓ Защита персональных данных;
- ✓ Физическая защита, включающая в себя контроль доступа к серверам, хранилищам и другим информационным ресурсам, а также контроль целостности оборудования;
- ✓ Правовое обеспечение конфиденциальности, включающее в себя локальные нормативные акты, связанные с обеспечением конфиденциальности;
- ✓ Адаптация к возникающим угрозам и меняющемуся правовому ландшафту.

В основу реализации политики Университета в области конфиденциальности заложены следующие принципы:

- ✓ Целостность. Информация хранится в системе в полном объеме и не меняется без ведома владельца.
- ✓ Доступ - субъекты данных имеют доступ к своим данным и вносят исправления в любые неточности.
- ✓ Цель — данные используются только для указанной цели и не доступны ни для каких других целей.
- ✓ Безопасность — собранные данные защищены от любых возможных злоупотреблений;
- ✓ Конфиденциальность. Информацию не может посмотреть тот, у кого нет к ней доступа.

### Основные цели и задачи Университета в области конфиденциальности:

Управление конфиденциальностью ориентировано на достижение следующих целей:

- ✓ обеспечение безопасной информационной среды для функционирования и развития процессов Университета;
- ✓ снижение уровня рисков и угроз информационной безопасности до уровня, позволяющего осуществлять устойчивое цифровое развитие Университета.

Для достижения данных целей необходимо решение следующих задач:

- ✓ обеспечение информационной безопасности процессов Университета в условиях возрастающего уровня угроз, включая оперативный мониторинг и оценку состояния защищенности в Университете; повышение эффективности защиты от спланированных целенаправленных компьютерных атак;
- ✓ повышение информационной безопасности образовательных систем;
- ✓ применение новых современных методов для защищенной цифровизации Университета; организация апробации и применения новых методов защиты информации от современных угроз;
- ✓ применение безопасных цифровых технологий при внедрении отечественных разработок и развитие собственного конкурентоспособного программного обеспечения Университета;
- ✓ соответствие требованиям государства в области информационной безопасности путем обеспечения заданного уровня информационной безопасности информационных банков, баз данных и программного обеспечения в соответствии с требованиями действующего законодательства.

Конечным результатом реализации поставленных целей и задач рассматривается получение конкурентных преимуществ от образовательной, научной, исследовательской, и инновационной деятельности Университета, а также повышение эффективности от взаимодействия с внешними организациями, повышение компетенций работников в целях минимизации рисков конфиденциальности.

Ректор



О.И. Фелонин