|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДАЮ  Ректор      ФИО  «   »     2025 г. |

**Политика**

**в области информационной безопасности**

**университета**

г. Город

Год г.

Оглавление

**1. Общее положение** 3

**2. Нормативные ссылки** 3

**3. Термины, определения, обозначения и сокращения** 4

**4. Основные принципы обеспечения ИБ** 6

**5. Цели и задачи информационной безопасности Университета** 7

**6. Объекты защиты** 7

**7. Ответственность за нарушения в области ИБ** 8

1. **Общее положение**
   1. Назначение

Настоящая Политика является основополагающим документом, предназначенным для выражения позиции (далее – Университет) в области информационной безопасности, определяет систему взглядов, принципов и подходов в этой области для обеспечения защищенности образовательных, научных, финансово-хозяйственных и иных процессов Университета, направленных на достижение целей, предусмотренных Уставом Университета, создания условий безопасного цифрового развития Университета и обеспечения соответствия требованиям законодательства Российской федерации в данной области.

Настоящая Политика разработана в соответствии с требованиями законодательства Российской федерации в области информационной безопасности, с учетом применимых международных стандартов, передового опыта и лучших практик.

* 1. Область действия

Настоящая Политика обязательна для исполнения работниками Университета

* 1. Период действия и порядок внесения изменений

Настоящая Политика является локальным нормативным документом постоянного действия.

Настоящая Политика утверждается, изменяется и признается утратившей силу в Университете в соответствии с приказом Университета.

1. **Нормативные ссылки**

Настоящая Политика разработана с учетом следующих документов:

- Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ;

- Федеральный закон «О коммерческой тайне» от 29.07.2004 года №98-ФЗ;

- Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ;

1. **Термины, определения, обозначения и сокращения**

В настоящей политике используются следующие термины:

1. автоматизированная система: система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;
2. аудит информационной безопасности: системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определёнными критериями и показателями безопасности;
3. информационные технологии: процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
4. информационная безопасность Университета: состояние защищенности информационных активов Университета в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т. п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов Университета. Защищенность достигается обеспечением совокупности свойств информационной безопасности - конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры Университета;
5. информационные активы Университета: активы Университета, имеющие отношение к его информационной сфере и представляющие ценность для нее с точки зрения достижения уставных целей;
6. инцидент информационной безопасности: действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов Университета;
7. мониторинг информационной безопасности Университета: постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности Университета, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, нформационные технологические процессы, информационные услуги и пр.;
8. политика информационной безопасности Университета: комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в Университете для обеспечения информационной безопасности;
9. риск: Мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы;
10. роль в Университете: заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом в Университете. К субъектам относятся персонал Университета, его партнеры, обучающиеся, а также инициируемые от их имени действия над объектами. Объектами являются аппаратные и программные средства, информационные ресурсы, услуги и процессы, составляющие автоматизированную систему;
11. угроза: опасность, предполагающая возможность потерь (ущерба);
12. управление информационной безопасностью Университета: совокупность целенаправленных действий, осуществляемых в рамках Политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер);
13. уязвимость: недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Университета при реализации угроз в информационной сфере.

В настоящем положении используются следующие сокращения:

АС - автоматизированная система;

ИБ - информационная безопасность;

ИС - информационная система;

ЛВС - локальная вычислительная сеть;

НСД - несанкционированный доступ;

ОС - операционная система;

РФ - Российская Федерация;

СКЗИ - средство криптографической защиты информации;

СУБД - система управления базами данных;

ЭВМ - электронная вычислительная машина;

ЭЦП - электронная цифровая подпись;

ИСПДн - информационная система персональных данных.

1. **Основные принципы обеспечения ИБ**

Основными принципами обеспечения ИБ являются следующие:

* 1. Постоянное и всестороннее исследование информационных активов Университета и технологий с целью выявления уязвимостей.
  2. Оперативное выявление потенциальных проблем, которые могут повлиять на безопасность Университета, с последующим обновлением моделей угроз и нарушителя.
  3. Разработка и внедрение соответствующих защитных мер, учитывая характер обнаруженных угроз, их совместимость с существующими технологическими процессами и финансовыми ресурсами. При этом следует избегать усложнения достижения уставных целей Университета и увеличения сложности для пользователей.
  4. Контроль эффективности применяемых защитных мер.
  5. Использование индивидуального и ясного распределения ролей и ответственности среди персонала Университета в соответствии с принципом персональной ответственности за проводимые операции.

1. **Цели и задачи информационной безопасности Университета**
   1. Основными целями защиты информации Университета являются:

* повышение стабильности функционирования Университета в целом;
* достижение адекватности мер по защите от реальных угроз ИБ;
* предотвращение или снижение ущерба от инцидентов ИБ.
  1. Основными задачами деятельности по обеспечению ИБ Университета являются:
* выполнение требований законодательства по обеспечению ИБ;
* контроль выполнения установленных требований и поддержанию информационной безопасности с учетом требований системы менеджмента качества;
* разработка и совершенствование регламентирующих документов Университета в области обеспечения информационной безопасности;
* выявление, оценка и прогнозирование угроз информационной безопасности;
* организация антивирусной защиты информационных активов;
* защита информации от НСД и утечки по техническим каналам связи.

1. **Объекты защиты**
   1. В рамках обеспечения информационной безопасности объектами защиты в Университете является информация, обрабатываемая в Университете, вне зависимости от формы представления; информационные активы, включая, но не ограничиваясь следующим перечнем:

* автоматизированные рабочие места, средства обработки информации и мобильные технические средства;
* информационные системы, системы хранения данных, программное обеспечение и отдельные технические решения;
* информационно-технологическая инфраструктура, информационно-телекоммуникационные сети и системы связи;
* информационные сервисы (ИТ-услуги), оказываемые Университету или в интересах Университета;
* решения по цифровизации Процессов Университета.
  1. Защищаемая информация делится на следующие виды:
* информация, составляющая коммерческую тайну, научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны (определяется Перечнем защищаемых сведений, составляющих коммерческую тайну Университета в соответствии с Федеральным Законом «О коммерческой тайне»);
* персональные данные – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (в соответствии с Трудовым кодексом и другими законодательными актами РФ);
* иная информация, не относящаяся ни к одному из указанных выше видов, которая определена как защищаемая Приказами и распоряжениями руководства Университета.

1. **Ответственность за нарушения в области ИБ**

Работники Университета должны выполнять требования и правила информационной безопасности при работе с информацией и информационными активами Университета и его Деловых партнёров.

Требования распорядительных документов и правил обеспечения информационной безопасности обязательны для всех без исключения работников Университета и должны учитываться во взаимоотношениях с Деловыми партнерами.

Руководство Университета возлагает ответственность на руководителей структурных подразделений, представительств и филиалов Университета за организацию повседневной деятельности и выделение необходимых ресурсов для обеспечения информационной безопасности как неотъемлемой составляющей Процессов Университета; за своевременную идентификацию значимых информационных активов, назначение ответственных за информационные активы и управление доступа к ним; за предъявление установленных требований информационной безопасности к работникам Университета и Деловым партнерам, использующим информационные активы Университета, и контроль за их выполнением.

При использовании сети Интернет, при общении в социальных сетях и мессенджерах, использовании электронной почты, других средств телекоммуникаций и мобильных технических средств работникам Университета рекомендуется проявлять осмотрительность и сдержанность, чтобы не допускать рисков личной безопасности, а также избегать непреднамеренной утечки рабочей информации.

Каждый работник Университета за несоблюдение требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

Работники Деловых партнёров, использующие информационные активы Университета, а также предоставленную Университетом информацию, несут ответственность в соответствии с договорными отношениями с Университетом, а также применимым законодательством.