**1. КРАТКОЕ ИЗЛОЖЕНИЕ ПОЛИТИКИ**

Информация всегда должна быть защищена не зависимо от её формы и её способа распространения, передачи и хранения.

**2. ВВЕДЕНИЕ**

1. Настоящая Политика разработана в соответствии с законодательством Республики Беларусь и нормами права в части обеспечения информационной безопасности, и основывается в том числе на:

* международном стандарте ISO/IEC 27002 «Информационные технологии - Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью»;
* приказе оперативно-аналитического центра при Президенте Республики Беларусь № 62 «О некоторых вопросах технической и криптографической защиты информации».

1. Настоящая Политика является документом, доступным любому сотруднику университета и пользователю его ресурсов, и представляет собой официально принятую руководством НАЗВАНИЕ УНИВЕРСИТЕТА (далее – Университет) систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Университета.
2. Руководство Университета осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования образовательной деятельности, а также развития реализуемых университетом технологий и ожиданий сотрудников, студентов и других заинтересованных сторон. Соблюдение требований информационной безопасности позволит создать конкурентные преимущества Университету, обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.
3. Требования информационной безопасности, которые предъявляются Университетом, соответствуют интересам (целям) деятельности Университета и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере Университета имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности. Факторы рисков в информационной сфере Университета составляют значимую часть операционных рисков Университета, а также имеют отношение и к иным рискам основной и управленческой деятельности Университета.
4. Необходимые требования обеспечения информационной безопасности Университета должны неукоснительно соблюдаться персоналом Университета и другими сторонами как это определяется положениями внутренних нормативных документов Университета, а также требованиями договоров и соглашений, стороной которых является Университет.
5. Настоящая Политика распространяется на бизнес - процессы Университета и обязательна для применения всеми сотрудниками и руководством Университета, а также пользователями его информационных ресурсов.
6. Положения настоящей Политики должны быть учтены при разработке политик информационной безопасности в дочерних и аффилированных организациях.
7. Настоящая Политика является корпоративным документом по ИБ первого уровня.
8. Документами, детализирующими положения корпоративной Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Университета, являются частные политики по обеспечению ИБ (далее – Частные политики), которые являются документами по ИБ второго уровня, оформляются как отдельные внутренние нормативные документы Университета, разрабатываются и согласовываются в соответствии с установленным в Университете порядком, утверждаются Куратором.

**3. ОБЛАСТЬ ДЕЙСТВИЯ**

Основными объектами защиты системы информационной безопасности в Университете являются:

* + информационные ресурсы, содержащие коммерческую тайну, персональные данные физических лиц, информация ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Университета, независимо от формы и вида ее представления;
  + сотрудники Университета, являющиеся разработчиками и пользователями информационных систем Университета;
  + информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

**4. ЦЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Целью деятельности по обеспечению информационной безопасности Университета является снижение угроз информационной безопасности до приемлемого для Университета уровня.

Основные задачи деятельности по обеспечению информационной безопасности Университета:

* выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
* предотвращение инцидентов информационной безопасности;
* исключение либо минимизация выявленных угроз.

**5. ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные).

1. Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

К антропогенным угрозам относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Университета и контрольных органов, с действиями в руководстве и управлении (менеджменте), неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

1. Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

1. Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

1. Источники угроз по отношению к инфраструктуре Университета могут быть как внешними, так и внутренними.
2. По отношению к Университету нарушители могут быть разделены на внешних и внутренних нарушителей.

Внутренние нарушители.

В качестве потенциальных внутренних нарушителей Университетом рассматриваются:

* зарегистрированные пользователи информационных систем Университета;
* сотрудники Университета, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Университета, но имеющие доступ в здания и помещения;
* персонал, обслуживающий технические средства корпоративной информационной системы Университета;
* сотрудники самостоятельных структурных подразделений Университета, задействованные в разработке и сопровождении программного обеспечения;
* сотрудники самостоятельных структурных подразделений, обеспечивающие безопасность Университета;
* руководители различных уровней.

1. Внешние нарушители.

В качестве потенциальных внешних нарушителей Университетом рассматриваются:

* бывшие сотрудники Университета;
* представители организаций, взаимодействующих по вопросам технического обеспечения Университета;
* клиенты Университета;
* посетители зданий и помещений Университета;
* конкурирующие с Университета образовательные организации;
* члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию.

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

* нарушитель скрывает свои несанкционированные действия от других сотрудников Университета;
* 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, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;
  + внешний нарушитель может действовать в сговоре с внутренним нарушителем.

1. Требования об обеспечении информационной безопасности Университета обязательны к соблюдению всеми работниками Университета и пользователями информационных систем.
2. Руководство Университета приветствует и поощряет в установленном порядке деятельность работников Университета и пользователей информационных систем по обеспечению информационной безопасности.
3. Неисполнение или некачественное исполнение сотрудниками Университета и пользователями информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в Университете порядком либо требованиями действующего законодательства.
4. Стратегия Университета в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Университета, до специализированных мер информационной безопасности по каждому выявленному в Университете риску, основанных на оценке рисков информационной безопасности.
5. При планировании мероприятий по обеспечению информационной безопасности в Университете осуществляются:
6. Определение и распределение ролей персонала Университета, связанного с обеспечением информационной безопасности (ролей информационной безопасности).
7. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.
8. Менеджмент рисков информационной безопасности, включающий:

* анализ влияния на информационную безопасность Университета применяемых в деятельности Университета технологий, а также внешних по отношению к Университету событий;
* выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
* определение моделей угроз информационной безопасности;
* выявление, анализ и оценка значимых для Университета угроз информационной безопасности;
* выявление возможных негативных последствий для Университета, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Университета;
* идентификацию и анализ рисковых событий информационной безопасности;
* оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для Университета;
* обработку результатов оценки рисков информационной безопасности, базирующейся на методах управления операционными рисками, определенных в Университете;
* оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Университета в случае наступления рисковых событий;
* оценку влияния защитных мер на цели основной деятельности Университета;
* оценку затрат на реализацию защитных мер;
* рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;
* разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Университета и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;
* документальное оформление целей и задач обеспечения информационной безопасности Университета, поддержка в актуальном состоянии нормативно – методического обеспечения деятельности в сфере информационной безопасности.

1. В рамках реализации деятельности по обеспечению информационной безопасности в Университете осуществляются:
2. Менеджмент инцидентов информационной безопасности, включающий:

* 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 Университета информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
* 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 персонала Университета в вопросах обеспечения информационной безопасности;
* обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем Университета и информации, обрабатываемой в них;
* применение средств криптографической защиты информации;
* 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 на стадиях жизненного цикла автоматизированных систем Университета, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);
* контроль доступа в здания и помещения Университета.

1. Обеспечение защиты информации от утечки по техническим каналам, включающее:

* применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита;
* применение мер и технических средств, создающих помехи при несанкционированном получении информации - активная защита;
* применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

1. В целях проверки деятельности по обеспечению информационной безопасности в Университете осуществляются:

* контроль правильности реализации и эксплуатации защитных мер;
* контроль изменений конфигурации систем и подсистем Университета;
* мониторинг факторов рисков и соответствующий их пересмотр;
* контроль реализации и исполнения требований сотрудниками Университета действующих внутренних нормативных документов по обеспечению информационной безопасности Университета;
* контроль деятельности сотрудников и других пользователей информационных систем Университета, направленный на выявление и предотвращение конфликтов интересов.

1. В целях совершенствования деятельности по обеспечению информационной безопасности в Университете осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Университета).
2. В целях выполнения задач по обеспечению информационной безопасности Университета, в соответствии с рекомендациями международных стандартов по безопасности в Университете должны быть определены следующие роли:

* Куратор;
* Ответственное подразделение;
* Сотрудник Университета.

При необходимости могут быть определены и другие роли по информационной безопасности.

1. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Университета осуществляются и координируются Ответственным подразделением. Задачами Ответственного подразделения являются:
   * установление потребностей Университета в применении мер обеспечения информационной безопасности, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;
   * соблюдение действующего законодательства, нормативных актов органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации, нормативных актов по обеспечению информационной безопасности;
   * разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Университета, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;
   * осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности Университета;
   * обучение, контроль и непосредственная работа с персоналом Университета в области обеспечения информационной безопасности;
   * планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объекты и системы в Университете;
   * выявление и предотвращение реализации угроз информационной безопасности;
   * выявление и реагирование на инциденты информационной безопасности;
   * информирование в установленном порядке ответственных лиц об угрозах и рисковых событиях информационной безопасности;
   * прогнозирование и предупреждение инцидентов информационной безопасности;
   * пресечение несанкционированных действий нарушителей информационной безопасности;
   * поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение персонала;
   * типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на филиалы и представительства Университета;
   * обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;
   * мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности Университета;

* контроль обеспечения информационной безопасности Университета, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;
* информирование руководства Университета и руководителей его самостоятельных структурных подразделений Университета об угрозах информационной безопасности, влияющих на деятельность Университета.

1. Ответственное подразделение может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые сотрудником Ответственного подразделения, и может, при наличии обоснованной необходимости по согласованию с руководителями соответствующих подразделений, привлекать для работы в них сотрудников других самостоятельных структурных подразделений Университета на основе совмещения работы в группе со своими основными должностными обязанностями.
2. Финансирование работ по реализации положений настоящей Политики осуществляется как в рамках целевого бюджета Ответственного подразделения Университета, так и в рамках бюджетов бизнес - подразделений и подразделений ИТ-блока.
3. Основными функциями Куратора в вопросах информационной безопасности являются:

* назначение ответственных лиц в области ИБ,
* координация и внедрение информационной безопасности в Университете.

1. Основными задачами работников Университета при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению информационной безопасности Университета являются:

* соблюдение требований информационной безопасности, устанавливаемых нормативными документами Университета;
* выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;
* выявление и реагирование на инциденты информационной безопасности;
* информирование в установленном порядке ответственных лиц о выявленных угрозах и рисковых событиях информационной безопасности;
* прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;
* мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;
* информирование своего руководства и Ответственного подразделения о выявленной угрозе в информационной среде Университета.

**6. СФЕРЫ ОТВЕТСТВЕННОСТИ**

Общее руководство обеспечением информационной безопасности Университета осуществляет Куратор.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы обеспечения информационной безопасности Университета лежит на руководстве Ответственного подразделения.

Ответственность работников Университета за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с работниками Университета, а также положениями внутренних нормативных документов Университета.

**7. КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ**

1. Инциденты информационной безопасности не должны приводить серьёзным непредвиденным затратам или серьёзным срывам работы служб и деятельности Университета.
2. Потери из-за мошенничества должны быть известны и находится в рамках приемлемых ограничений.
3. Вопросы информационной безопасности не должны оказывать неблагоприятного влияния на учебный процесс или деятельность Университета.