Приложение к приказу учреждения образования «Могилевский государственный университет имени А.А. Кулешова»
«13» 09 2021 № 615-од

Политика информационной безопасности в учреждении образования «Могилевский государственный университет имени А.А. Кулешова»

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика разработана в соответствии с Постановлением Совета безопасности Республики Беларусь от 18.03.2019г. №1 «Концепция информационной безопасности Республики Беларусь».

1.2. Настоящая Политика является документом, доступным любому работнику учреждении образования «Могилевский государственный университет имени А.А. Кулешова» (далее – Университет) и пользователю информационных ресурсов Университета, и представляет собой официально принятую 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.

1.3. Руководство Университета осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности. Соблюдение требований информационной безопасности позволит упорядочить бизнес-процессы Университета, привести к соответствию правовым нормам, улучшить имидж и деловую репутацию.

1.4. Предъявляемые требования информационной безопасности соответствуют политике и миссии Университета и предназначены для снижения рисков, связанных с информационной безопасностью.

1.5. Стратегия Университета в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности законодательства Республики Беларусь в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных;

1.6. Необходимые требования обеспечения информационной безопасности Университета должны неукоснительно соблюдаться работниками и обучающимися в Университете.

1.7. Работники Университета, не ознакомленные с настоящей Политикой, не допускаются к работе с информационными системами (система, предназначенная для хранения, поиска и обработки информации) и ресурсами (массивы документов в информационных системах) Университета.

1.8. Настоящая Политика распространяется на все бизнес-процессы Университета и обязательна для применения всеми работниками Университета, а также пользователями её информационных ресурсов без исключения.

1.9. Дополнительно к данной политике могут быть разработаны отдельные документы, детализирующие положения Политики применительно к одной или нескольким информационным системам, видам и технологиям деятельности Университета.

ГЛАВА 2. СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

2.1. Бизнес-процесс – последовательность технологически связанных операций по осуществлению уставной деятельности Университета и конкретного вида обеспечивающей деятельности Университета.

2.2. Информационная безопасность (ИБ) – в настоящей Политике состояние защищенности технологических и бизнес-процессов Университета, объединяющих в своем составе работников Университета, технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере.

2.3. Информационная система Университета – совокупность программно-аппаратных комплексов Университета, применяемых для обеспечения бизнес-процессов Университета.

2.4. Инцидент информационной безопасности – это появление одного или нескольких нежелательных рисковых событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

2.5. Конфиденциальная информация (далее – КИ) – информация, в отношении которой Университетом установлен режим конфиденциальности.

2.6. Модель угроз – описательное представление свойств или характеристик угроз безопасности информации.

2.7. Модель нарушителя – описательное представление опыта, знаний, доступных ресурсов возможных нарушителей ИБ, необходимых им для реализации угрозы ИБ, и возможной мотивации действий.

2.8. Ответственное подразделение – отдел информационных технологий Университета. Основные функции в указанной сфере – внедрение настоящей Политики, разработка, внедрение и поддержка систем обеспечения информационной безопасности.

2.9. Пользователь информационной системы – физическое лицо, обладающее возможностью доступа к информационной системе Университета.

2.10.Режим конфиденциальности информации – организационно-технические мероприятия по защите информации, позволяющие обладателю КИ при любых обстоятельствах обеспечить её сохранность и конфиденциальность, включающие в себя:

2.10.1. перечень КИ определяется в Приложении №1 к данной Политике;

2.10.2. ограничение доступа к КИ путем установления порядка обращения с этой информацией и контроля над соблюдением такого порядка;

2.10.3. учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;

2.10.4. регулирование отношений по использованию КИ работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров и соглашений.

2.11.Рисковое событие информационной безопасности – это событие, повлекшее или способное повлечь за собой репутационные и финансовые потери Университета и произошедшее по причине ошибочности или сбоя процессов, действий людей и систем, а также по причине внешних событий.

2.12.Угроза информационной безопасности – любой риск, влияющий на нарушение одного (или нескольких) свойств информации – целостности, конфиденциальности, доступности объектов защиты.

ГЛАВА 3. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ

3.1. Основными объектами защиты системы информационной безопасности в Университете являются:

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

3.1.2. работники Университета и их представители, студенты и другие лица, являющиеся пользователями информационных систем Университета;

3.1.3. информационная инфраструктура, включающая системы хранения, 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.

ГЛАВА 4. ЦЕЛИ И ЗАДАЧИ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Целью деятельности по обеспечению информационной безопасности Университета является снижение угроз информационной безопасности.

4.2. Основные задачи деятельности по обеспечению информационной безопасности Университета:

4.2.1. своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем университета;

4.2.2. предотвращение инцидентов информационной безопасности;

4.2.3. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

4.2.4. защиту от вмешательства в процесс функционирования систем Университета посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

4.2.5. разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам университета – обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих должностных обязанностей;

4.2.6. обеспечение аутентификации пользователей, имеющих допуск в информационные сети и участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

4.2.7. защиту от несанкционированной модификации используемых в системах Университета программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;

4.2.8. защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

ГЛАВА 5. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Под антропогенными угрозами ИБ в Университете понимаются:

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

5.1.2. ошибки в действиях работников Университета;

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

5.1.4. угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Университета и контрольных органов;

5.2. Под техногенными угрозами ИБ в Университета понимается:

5.2.1. угрозы объективных физических процессов техногенного характера;

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

5.2.3. сбои в работе или разрушение систем, созданных человеком, находящихся вне зоны ответственности Университета.

5.3. Под природными угрозами ИБ в Университете понимаются:

5.3.1. угрозы объективных физических процессов природного характера;

5.3.2. стихийных природных явлений;

5.3.3. состояний окружающей среды, не обусловленных напрямую деятельностью человека;

5.3.4. угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

ГЛАВА 6. МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. В качестве потенциальных внутренних нарушителей Университетом рассматриваются:

6.1.1. зарегистрированные пользователи информационных систем Университета (работники и обучающиеся);

6.1.2. работники, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Университета, но имеющие доступ в здания и помещения;

6.1.3. работники, обслуживающие технические средства корпоративной информационной системы Университета;

6.1.4. руководители различных уровней Университета.

6.2. В качестве потенциальных внешних нарушителей Университетом рассматриваются:

6.2.1. бывшие работники Университета и выпускники;

6.2.2. сторонние организации или их представители задействованные в разработке и сопровождении программного обеспечения и взаимодействующие по вопросам технического обеспечения Университета;

6.2.3. сторонние организации или их представители, предоставляющие собственные ресурсы в пользование Университета;

6.2.4. посетители информационных ресурсов Университета;

6.2.5. посетители зданий и помещений Университета;

6.2.6. члены преступных организаций, работники спецслужб или лица, действующие по их заданию;

6.2.7. лица, случайно или умышленно проникшие в информационную

систему Университета из внешних телекоммуникационных сетей (хакеры).

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

6.3.1. нарушитель скрывает свои несанкционированные действия от других работников Университета;

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

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

6.3.4. внешний нарушитель может действовать в сговоре с внутренним нарушителем.

ГЛАВА 7. ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Стратегия Университета в части противодействия угрозам ИБ заключается в реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Университета, до специализированных мер информационной безопасности по каждому выявленному в Университете риску.

7.2. При планировании мероприятий по обеспечению информационной безопасности в Университете осуществляются:

7.2.1. определение и распределение ролей работников Университета, связанного с обеспечением информационной безопасности (ролей информационной безопасности);

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

7.2.3. управление рисками информационной безопасности.

7.3. В рамках реализации деятельности по обеспечению информационной безопасности в Университете осуществляются:

7.3.1. Управление инцидентами информационной безопасности, включающее, но не исключительно:

7.3.1.1. учет всех подлежащих защите информационных систем;

7.3.1.2. сбор информации о событиях информационной безопасности;

7.3.1.3. выявление и анализ инцидентов информационной безопасности;

7.3.1.4. расследование инцидентов информационной безопасности;

7.3.1.5. оперативное реагирование на инцидент информационной безопасности;

7.3.1.6. минимизация негативных последствий инцидентов информационной безопасности;

7.3.1.7. оперативное доведение до руководства Университета информации о наиболее значимых инцидентах информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;

7.3.1.8. взаимодействие с компетентными органами безопасности по выявленным инцидентам;

7.3.1.9. выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;

7.3.1.10.пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;

7.3.1.11.повышение уровня знаний работников Университета в вопросах обеспечения информационной безопасности;

7.3.1.12.обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем Университета и информации, обрабатываемой в них;

7.3.1.13.обеспечение бесперебойной работы автоматизированных систем и сетей связи;

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

7.3.1.15.применение средств защиты от вредоносных программ;

7.3.1.16.обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем Университета, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);

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

7.3.1.18.подготовка работников Университета, ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности.

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

7.4.2.1. применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме – пассивная защита;

7.4.2.2. применение мер и технических средств, создающих помехи при попытке несанкционированного получения информации – активная защита;

7.4.2.3. применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации – поиск.

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

7.5.1. контроль правильности реализации и использования мер защиты;

7.5.2. контроль изменений конфигурации систем и подсистем Университета;

7.5.3. мониторинг факторов рисков и соответствующий их пересмотр;

7.5.4. контроль реализации и исполнения требований работниками Университета действующих внутренних нормативных документов по обеспечению информационной безопасности Университета.

7.5. В целях совершенствования деятельности по обеспечению информационной безопасности в Университете осуществляется периодическое и, при необходимости, оперативное уточнение и пересмотр целей и задач обеспечения информационной безопасности.

ГЛАВА 8. ОРГАНИЗАЦИОННАЯ ОСНОВА ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. В целях выполнения задач по обеспечению информационной безопасности Университета, в соответствии с рекомендациями Республики Беларусь и международных стандартов по безопасности в Университете должны быть определены следующие роли:

8.1.1. ответственное подразделение;

8.1.2. работник Университета.

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

8.3. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Университета осуществляются и координируются Ответственным подразделением. Задачами Ответственного подразделения являются:

8.3.1. установление потребностей Университета в применении мер обеспечения информационной безопасности, определяемых требованиями нормативных актов законодательства и локальными правовыми актами;

8.3.2. соблюдение действующего законодательства, нормативных правовых актов в области обеспечения безопасности и технической защиты информации;

8.3.3. 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;

8.3.4. осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (планов, методик и т.д.), затрагивающих вопросы информационной безопасности Университета;

8.3.5. обучение, контроль и непосредственная работа с работниками Университета в области обеспечения информационной безопасности;

8.3.6. планирование применения и эксплуатации средств обеспечения информационной безопасности на объектах и системах в Университете;

8.3.7. выявление и предотвращение реализации угроз информационной безопасности;

8.3.8. выявление и реагирование на инциденты информационной безопасности;

8.3.9. информирование в установленном порядке ответственных лиц об угрозах и рисковых событиях информационной безопасности;

8.3.10. прогнозирование и предупреждение инцидентов информационной безопасности;

8.3.11. пресечение несанкционированных действий нарушителей информационной безопасности;

8.3.12. обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;

8.3.13. мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности, защитных мер и видов деятельности по обеспечению информационной безопасности Университета;

8.3.14. контроль обеспечения информационной безопасности Университета, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной

безопасности;

8.3.15. информирование руководства Университета и руководителей структурных подразделений об угрозах информационной безопасности, влияющих на деятельность Университета.

8.4. Финансирование работ по реализации положений настоящей Политики осуществляется в рамках выделяемых средств на информатизацию Университета.

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

8.5.1. соблюдение требований информационной безопасности, устанавливаемых нормативными документами Университета;

8.5.2. выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;

8.5.3. выявление и реагирование на инциденты информационной безопасности;

8.5.4. информирование в установленном порядке ответственных лиц о выявленных угрозах и рисковых событиях информационной безопасности;

8.5.5. прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;

8.5.6. мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;

8.5.7. информирование своего непосредственного руководителя и Ответственное подразделение о выявленной угрозе в информационной среде Университета.

ГЛАВА 9. ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ

9.1. Общее руководство обеспечением информационной безопасности Университета осуществляет начальник Ответственного подразделения.

9.2. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Университета возложена на Ответственное подразделение.

9.3. Неисполнение или некачественное исполнение работниками Университета, обучающимися и пользователями информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также привлечение виновных к дисциплинарной ответственности, степень которых определяется установленным в Университете порядком либо требованиями действующего законодательства.

ГЛАВА 10. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПОЛОЖЕНИЙ ПОЛИТИКИ

10.1.Общий контроль за состоянием информационной безопасности Университета осуществляется проректором Жуковой Э.В.

10.2.Текущий контроль за соблюдением настоящей Политики осуществляет Ответственное подразделение. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Университета, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

ГЛАВА 11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1.Требования настоящей Политики могут дополняться и уточняться нормативными документами Университета.

11.2.Внесение изменений и (или) дополнений в настоящую Политику осуществляется на периодической и внеплановой основе:

11.2.1. периодическое внесение изменений и (или) дополнений в настоящую Политику должно осуществляться не реже одного раза в 24 месяца;

11.2.2. внеплановое внесение изменений и (или) дополнений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

Ответственным за внесение изменений в настоящую Политику является Начальник Ответственного подразделения.

Приложение №1

Перечень конфиденциальной информации
в учреждении образования «Могилевский государственный университет имени А.А. Кулешова»

1. Любая информация на любых носителях о хозяйственной и финансовой деятельности Университета, в том числе:

1.1. о запланированных и осуществленных финансовых операциях Университета;

1.2. ключи доступа и сертификаты для систем криптографической защиты информации:

1.2.1. системы клиент-банк;

1.2.2. системы бухгалтерского учета 1С: Предприятие;

1.2.3. системы электронного документооборота Directum;

1.2.4. автоматизированной системы управления Кадры;

1.2.5. автоматизированной системы управления Студент;

1.2.6. автоматизированной системы управления Абитуриент;

1.2.7. системы образовательного портала Moodle;

1.2.8. корпоративная почта.

1.3. пароли доступов:

1.3.1. к информационным ресурсам Университета, вне зависимости от их местонахождения;

1.3.2. к файловым ресурсам Университета, вне зависимости от их местонахождения;

1.3.3. пользователей информационных ресурсов Университета;

1.3.4. к серверному оборудованию Университета, вне зависимости от их местонахождения.

2. Любая информация о деятельности Университета, которая обозначена как конфиденциальная:

2.1. документы Университета на любом носителе, которые отмечены грифом «Секретно» или «Для служебного использования».

3. Информация о договорах с работниками Университета.

4. Персональные данные работников и обучающихся Университета.