Учреждение образования
«Витебский государственный
университет имени П.М. Машерова»

УТВЕРЖДЕНО

Приказ ректора ВГУ имени
П.М. Машерова

«28» мая 2024 г. № 143

г. Витебск

Политика информационной
безопасности ВГУ имени
П.М. Машерова

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности (далее – Политика) ВГУ имени П.М. Машерова (далее – Университет) определяет цели и задачи системы информационной безопасности и представляет собой совокупность действующих правил, процедур и требований в области защиты информации для информационной системы (далее – ИС).

Система защиты информации (далее – СЗИ) предназначена для обеспечения конфиденциальности, целостности, доступности, подлинности и сохранности информации, обрабатываемой в информационной системе.

Политика разработана в соответствии с требованиями Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», Указа Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации», Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации», приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449», иных актов законодательства и определяет общие направления деятельности по поддержанию необходимого уровня информационной безопасности, включающего обеспечение конфиденциальности, целостности, сохранности, подлинности и доступности информации в университете.

2. Настоящая Политика разработана с целью регламентирования единых подходов и требований по обеспечению информационной безопасности субъектами информационных отношений университета при осуществлении своей деятельности и направлена на решение следующих задач:

реализация требований законодательства в части информационной безопасности информационных систем и мер контроля их защищенности;

определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований Политики, в том числе с

использованием программных, программно-аппаратных средств технической и криптографической защиты информации;

своевременное выявление и оценка причин, условий и характера угроз информационной безопасности и дальнейшее прогнозирование развития событий на основе мониторинга инцидентов информационной безопасности;

планирование, реализация и контроль эффективности использования защитных мер и средств защиты информации, создание механизма оперативного реагирования на угрозы информационной безопасности;

реализация программ по осведомленности и обучению работников университета о возможных факторах рисков информационной безопасности и мерах противодействия.

3. Положения настоящей Политики распространяются на все структурные подразделения университета и учитываются при взаимодействии с другими субъектами информационных отношений.

4. Иные локальные правовые акты ВГУ имени П.М. Машерова, регулирующие отдельные вопросы в сфере информационной безопасности, должны соответствовать требованиям настоящей Политики.

5. В настоящей Политике не рассматриваются вопросы обеспечения безопасности информации, содержащей сведения, составляющие государственные секреты.

2. ЦЕЛИ И ЗАДАЧИ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6. Целями защиты информации в ИС является обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации, обрабатываемой в информационной системе.

Доступность должна достигаться:

резервированием данных, технических и инженерных средств, телекоммуникационного оборудования и каналов передачи информации;

использованием отказоустойчивых технологий и решений.

Конфиденциальность и подлинность должна достигаться:

применением средств межсетевого экранирования и разграничения доступа к информации и функциям управления;

применением средств криптографической защиты информации;

аудитом событий безопасности;

разграничением прав доступа к информации;

многоуровневой идентификацией и аутентификацией сотрудников Университета, пользователей информационной системы и системных процессов.

Целостность должна достигаться:

применением механизмов контроля целостности данных;

применением средств антивирусной защиты;

применением средств криптографической защиты информации.

Сохранность должна достигаться:

применением средств резервного копирования и восстановления хранимых данных и программных средств.

7. Основными задачами деятельности по обеспечению информационной безопасности являются:

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

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

обеспечение защиты от вмешательства в процесс функционирования информационных систем посторонними лицами;

предоставление доступа к информационным ресурсам только зарегистрированным пользователям;

разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам университета;

обеспечение доступа пользователям только к тем ресурсам и к выполнению только тех операций с ними, которые необходимы им для исполнения своих должностных обязанностей;

обеспечение аутентификации пользователей, имеющих допуск в информационные сети и участвующих в информационном обмене;

обеспечение защиты от несанкционированной модификации используемых в системах университета программных средств, а также защиты систем от внедрения несанкционированных программ, включая компьютерные вирусы;

обеспечение защиты информации от утечки по техническим каналам связи при ее обработке, хранении и передаче по каналам связи.

3. ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

8. Система защиты информации университета основывается на следующих принципах:

8.1. Комплексность:

обеспечение безопасности информационных активов от возможных угроз всеми доступными законными средствами, методами и мероприятиями;

обеспечение безопасности информационных активов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования;

способность системы информационной безопасности к развитию и совершенствованию в соответствии с изменениями условий функционирования университета;

Комплексность достигается:

обеспечением соответствующего режима и охраны университета;

организацией отдельного делопроизводства с ориентацией на защиту информации, распространение и (или) предоставление которой ограничено;

мероприятиями по подбору, расстановке и обучению персонала;

широким использованием технических средств безопасности и защиты информации;

совокупностью правовых, организационных и инженерно-технических мероприятий;

внутренним контролем.

8.2. Своевременность – упреждающий характер мер обеспечения информационной безопасности.

8.3. Непрерывность – целостность и постоянство обеспечения информационной безопасности.

8.4. Активность – предполагает проведение защиты с достаточной степенью настойчивости.

8.5. Законность – предполагает разработку системы информационной безопасности на основе действующего законодательства.

8.6. Обоснованность – используемые возможности и средства защиты должны быть реализованы на современном уровне развития науки и техники и быть обоснованы с точки зрения заданного уровня безопасности.

8.7. Экономическая целесообразность и сопоставимость возможного ущерба и затрат на обеспечение безопасности – во всех случаях стоимость системы информационной безопасности университета должна быть меньше размера возможного ущерба от любых видов риска.

8.8. Специализация – эксплуатация технических средств и реализация мер безопасности должны осуществляться профессионально подготовленными работниками.

8.9. Взаимодействие и координация – означает осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений университета, сторонних специализированных организаций, координацию их усилий для достижения поставленных целей, а также сотрудничество с заинтересованными организациями, взаимодействие с органами государственного управления, в том числе правоохранительными органами.

8.10. Совершенствование – предусматривает совершенствование мер и средств защиты на основе отечественного, зарубежного и собственного опыта, появления новых технических средств.

8.11. Централизация управления – предполагает самостоятельное функционирование системы безопасности по единым правовым, организационным, функциональным и методологическим принципам.

8.12. Системность – реализация системы защиты информации должна быть обоснована и базироваться на системном подходе, учитывающем все основные факторы, оказывающие или способные оказать влияние на информационную безопасность университета.

4. СУБЪЕКТЫ И ОБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

9. Субъектами информационных отношений при обеспечении информационной безопасности являются:

ВГУ имени П.М. Машерова – в качестве обладателя информации и собственника (владельца) программно-технических средств, информационных ресурсов, информационных систем и информационных сетей;

государственные органы, другие государственные организации, иные юридические лица, организации, не являющиеся юридическими лицами, физические лица, в том числе индивидуальные предприниматели, иностранные и международные организации – в качестве пользователей информации, информационных систем и (или) информационных сетей, информационных посредников, операторов информационных систем, поставщиков программного обеспечения и программно-технических средств, исполнителей услуг технической поддержки, гарантийного и сервисного обслуживания программного обеспечения и программно-технических средств;

работники университета осуществляющие деятельность, связанную с поиском, получением, передачей, сбором, обработкой, накоплением, хранением, распространением и (или) предоставлением информации, пользованием информацией, созданием и использованием информационных технологий, информационных сетей и информационных систем, формированием информационных ресурсов, организацией и обеспечением защиты информации, в соответствии с актами законодательства, локальными правовыми актами университета, иными организационно-распорядительными документами, регламентами, правилами, инструкциями в пределах возложенных на них обязанностей;

обучающиеся Университета, иные физические лица, получившие доступ к предоставляемым Университетом услугам (работам);

Работники университета при использовании информационных технологий, информационных систем и информационных сетей университета обязаны:

соблюдать права и законные интересы университета и других лиц;

своевременно и точно выполнять указания работников центра информационных технологий по вопросам обеспечения информационной безопасности;

не использовать информационные ресурсы университета для получения личной коммерческой выгоды, осуществления коммерческой деятельности, участия в форумах, рассылки рекламы, если это не связано с исполнением возложенных обязанностей, а также просмотра (выгрузки) материалов порнографического и деструктивного характера, компьютерных игр, иных развлекательных материалов;

не совершать каких-либо действий, прямо или косвенно направленных на нарушение нормальной работы информационных ресурсов;

передавать третьим лицам свой пароль или работать под чужим регистрационным именем.

10. Объектами информационных отношений при обеспечении информационной безопасности являются:

поступающая (получаемая), накапливаемая, хранящаяся, обрабатываемая, распространяемая и (или) предоставляемая в процессе деятельности университета информация;

информационная инфраструктура, включающая информационные ресурсы, информационные системы и информационные сети университета и места их расположения;

процессы, методы, отношения при осуществлении поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, пользования информации, защиты информации, предоставлении программного обеспечения и программно-технических средств, оказании услуг технической поддержки, гарантийного и сервисного обслуживания программного обеспечения и программно-технических средств.

5. ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

11. Основные направления деятельности по обеспечению защиты объектов информационной системы:

обеспечение защиты средств вычислительной техники от вредоносного программного обеспечения;

использование криптографических алгоритмов защиты информации, интегрированных в программное обеспечение (ПО), в том числе самих носителей информации;

отключение функций автозагрузки внешних машинных носителей информации при их подключении к средствам вычислительной техники;

определение перечня разрешенного ПО, регламентация и контроль порядка его установки и использования;

регламентация порядка использования внешних машинных носителей информации, мобильных технических средств.

12. Основные направления деятельности по управлению доступом и идентификацией пользователей:

использование объектов информационной системы с правами пользовательских учетных записей;

обеспечение централизованного управления (создания, активации, блокировки, уничтожения) учетными записями пользователей для доступа к объектам информационной системы;

ограничение возможности использования общих учетных записей пользователей для доступа к объектам информационной системы;

разграничение доступа пользователей к объектам информационной системы;

обеспечение идентификации и аутентификации пользователей информационных систем;

своевременное блокирование (уничтожение) неиспользуемых учетных записей пользователей;

обеспечение доступа пользователей к объектам информационной системы на основе ролей;

блокировка доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя или по его запросу;

обеспечение изменения атрибутов безопасности сетевого оборудования, ПО, установленных по умолчанию;

ограничение количества неуспешных попыток доступа к объектам информационной системы;

обеспечение контроля соблюдения правил генерации и смены паролей пользователей;

обеспечение управления физическим доступом в помещения, а также к шкафам с СВТ, сетевым и другим оборудованием;

предоставление уникальных учетных записей привилегированных пользователей для авторизованного доступа к сетевому оборудованию;

предоставление временных учетных записей пользователей для авторизованного доступа в целях обслуживания объектов информационной системы неуполномоченными сотрудниками (сторонними организациями), обеспечение их контроля и отключения;

предоставление пользователям авторизованного доступа при подключении к объектам информационной системы из-за ее пределов.

13. Основные направления деятельности по защите почтовых серверов:

использование услуг хостинга уполномоченных поставщиков интернет-услуг;

обеспечение в реальном масштабе времени автоматической антивирусной проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживания обнаруженных вредоносных программ;

обеспечение спам-фильтрации почтовых сообщений;

обеспечение фильтрации почтовых сообщений с использованием списков нежелательных отправителей почтовых сообщений;

блокирование массовой рассылки почтовых сообщений.

14. Основные направления деятельности по обеспечению менеджмента сети:

обеспечение сегментации (изоляции) сети доступа в Интернет от сети передачи данных ИС;

обеспечение сегментации (изоляции) сети доступа в Интернет сторонних пользователей от сети передачи данных ИС;

ограничение входящего и исходящего трафика (фильтрация) определенных приложений и сервисов (мессенджеры, социальные сети, онлайн-маркеты, анонимайзеры и др.);

ограничение входящего и исходящего трафика (фильтрации) ИС только необходимыми соединениями (использование межсетевого экрана);

отключение неиспользуемых портов сетевого оборудования;

обнаружение и предотвращение вторжения в ИС (IPS/IDS);

обеспечение доступа пользователей в сеть Интернет с применением технологии проксирования сетевого трафика;

использование объектами информационной системы локальной системы доменных имен (DNS-сервер), в том числе для доступа в сеть Интернет, либо системы доменных имен, расположенной на территории Республики Беларусь.

15. Основные направления деятельности по обеспечению менеджмента уязвимостей:

периодическое, но не менее одного раза в год осуществление контроля отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы;

обеспечение исправления выявленных уязвимостей объектов информационной системы.

16. Основные направления деятельности по обеспечению аудита безопасности:

разработка и внедрение плана реагирования на инциденты информационной безопасности;

организация взаимодействия с центром информационных технологий по вопросам управления событиями (инцидентами) информационной безопасности;

назначение ответственных за информационную безопасность;

обеспечение централизованного сбора и хранения не менее одного года информации о функционировании средств защиты информации, сетевого оборудования, систем, сервисов (лог-файлы запросов пользователей к локальным системам доменных имен, лог-файлы системы проксирования подключения к сети Интернет, лог-файлы работы серверов печати и др.) о действиях пользователей, а также о событиях информационной безопасности;

периодическое, но не менее одного раза в неделю осуществление мониторинга (просмотр, анализ) событий информационной безопасности, функционирования объектов информационной системы;

обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования и системного ПО, средствам защиты информации и событиям безопасности;

осуществление контроля за внешними подключениями к ИС.

17. Основные направления деятельности по обеспечению безопасности информации в локальных сетях, подключенных к сети Интернет:

осуществление предоставления доступа к сервисам сети Интернет в той степени, которая необходима для исполнения возложенных обязанностей;

определение правил работы с сервисами сети Интернет (электронная почта, передача файлов, доступ к информационным ресурсам, социальным сетям и публичным системам мгновенных сообщений);

определение специалистов по администрированию сети, их прав и обязанностей;

определение прав и обязанностей пользователей;

определение ответственных за обеспечение защиты информации;

определение порядка и перечня используемого программного обеспечения;

определение порядка применения средств защиты информации;

осуществление необходимых мероприятий по разграничению доступа к средствам защиты информации и обработки информации;

определение порядка смены атрибутов безопасности (паролей) пользователей;

определение порядка действий при возникновении нештатной ситуации (сбои, повреждения, отказы) с информационными ресурсами;

определение порядка резервирования и уничтожения информации;

определение порядка контроля, учета использования ресурсов сети Интернет пользователями с использованием технических, программно-аппаратных и программных средств;

обеспечение межсетевого экранирования с использованием собственных возможностей и (или) возможностей уполномоченных поставщиков интернет-услуг;

обеспечение идентификации абонентских устройств в локальной сети;

обеспечение блокирования неконтролируемого обмена информацией между рабочими местами пользователей в локальной сети;

исключение использования на рабочих местах в локальной сети постороннего программного обеспечения, ресурсов сети Интернет, предназначенных для сокрытия действий пользователя;

исключение подключения рабочего места в локальной сети к сетям связи общего пользования через другие каналы доступа (сотовый телефон, модем);

осуществление сбора и хранения данных авторизации и статистики использования сети Интернет пользователями в течение 1 года;

обеспечение возможности анализа использования сети Интернет пользователями (с использованием собственных возможностей или поставщиков интернет-услуг).

18. Иные направления деятельности по обеспечению информационной безопасности:

определение состава и содержания информации, подлежащей резервированию (в том числе конфигурационных файлов сетевого оборудования, лог-файлов служб и сервисов);

обеспечение резервирования информации;

обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин;

информирование сотрудников об угрозах информационной безопасности и мерах по их предотвращению, обучение сотрудников правилам безопасной работы с объектами информационной системы,

использования почтовых сервисов ИС, работы в Интернете, определения фишинговых сообщений и т.п., в том числе с проведением практических занятий.

6. ОТВЕТСТВЕННОСТЬ ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

19. Ректор университета обязан организовать на должном уровне информационную безопасность университета и создать необходимые для этого условия.

20. Реализацию настоящей Политики и иных вопросов обеспечения информационной безопасности, планирование по информационной безопасности, контроль нештатных ситуаций и инцидентов в области защиты информации осуществляет центр информационных технологий.

21. Центр информационных технологий выполняет мониторинг защищенности информационных ресурсов, разрабатывает локальные правовые акты, иные организационно-распорядительные документы, правила, инструкции, регламенты по обеспечению информационной безопасности, контролирует соблюдение требований информационной безопасности всеми субъектами информационных отношений.

Расследование случаев нарушений информационной безопасности осуществляет центр информационных технологий с привлечением при необходимости специалистов иных подразделений и уполномоченных организаций.

22. Руководители структурных подразделений несут ответственность за ознакомление подчиненных работников с правилами по обеспечению информационной безопасности, осуществление контроля за их исполнением, своевременное извещение центра информационных технологий обо всех подозрительных ситуациях при работе с информационными ресурсами.

23. Пользователи информационных систем обязаны соблюдать правила по обеспечению информационной безопасности, своевременно извещать руководителя подразделения обо всех подозрительных ситуациях при работе с информационными ресурсами.

24. Нарушения требований настоящей Политики и иных организационно-распорядительных документов, регламентирующих порядок обеспечения информационной безопасности, а равно несоблюдение работниками мер, предусмотренных системой обеспечения информационной безопасности, является основанием для привлечения их к дисциплинарной ответственности и применения иных мер правового характера.

7. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ИНЫМИ (ВНЕШНИМИ) ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

25. Взаимодействие с иными информационными системами (в случае предполагаемого взаимодействия) должно быть организовано с учетом требований согласно приложению 4 к Положению о порядке технической и криптографической защиты информации в информационных системах,

предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденному приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66.

8. ПОРЯДОК ПЕРЕСМОТРА ДОКУМЕНТА

26. Пересмотр и внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

Плановый пересмотр Политики должен выполняться не реже одного раза в год.

Внеплановый пересмотр Политики выполняется в следующих случаях:

– изменения законодательства в области защиты информации;

– изменения технических нормативных правовых актов в области защиты информации;

– решения руководства Университета о пересмотре Политики.