Учреждение образования
«Гродненский государственный
аграрный университет»

УТВЕРЖДЕНО
Приказом ректора УО «ГГАУ»
от 09.04.2025 № 171

ПОЛОЖЕНИЕ
об информационной безопасности УО «ГГАУ»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

Политика информационной безопасности (далее - Политика) учреждения образования «Гродненский государственный аграрный университет» (далее - Университет) определяет цели и задачи системы информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется Университет в своей деятельности.

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 Республики Беларусь в области информатизации, безопасности и защиты информации.

Политика определяет общие цели и принципы деятельности по защите Университета от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на информационные системы (далее - ИС), а также минимизации рисков информационной безопасности (далее - ИБ).

Настоящий документ не охватывает вопросы защиты информации, отнесенной к государственным секретам.

Положения Политики доводятся до ознакомления и являются обязательными для работников структурных подразделений Университета, организующих и обеспечивающих эксплуатацию ИС при выполнении своих служебных обязанностей, абитуриентов и обучающихся Университета, взаимодействующих с ИС в процессе поступления и обучения в Университете, иных пользователей ИС, физических или юридических лиц, выступающих в качестве информационных посредников, и операторов ИС.

Политику в актуальном состоянии осуществляет отдел информационных технологий (далее - ОИТ).

ГЛАВА 2
ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

Целями защиты информации является защита Университета от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС, а также минимизация рисков ИБ.

Основными задачами Университета в части обеспечения безопасности информации в ИС являются:

реализация требований законодательства Республики Беларусь в части информационной безопасности ИС 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, а также посредством принятия соответствующих внутренних нормативных и организационно-методических документов информационной безопасности Университета;

минимизация ущерба, который может быть нанесен Университету из-за нарушений ИБ;

разграничение доступа пользователей к ИС (предоставление доступа пользователям только к тем информационным ресурсам и выполнению только тех операций в ИС, которые необходимы пользователям для выполнения своих служебных обязанностей);

обеспечение аутентификации пользователей;

обеспечение защиты от несанкционированной модификации используемого в ИС программного обеспечения (далее - ПО), а также защиты ИС от внедрения несанкционированных программ, включая вредоносное ПО;

обеспечение резервирования и архивирования информационных ресурсов;

обеспечение криптографической защиты информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, при ее передаче посредством сетей электросвязи общего пользования;

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

выявление, предупреждение и пресечение возможности противоправной и иной деятельности работников и обучающихся Университета;

реализация программ по осведомленности и обучению работников Университета о возможных факторах рисков ИБ и мерах противодействия.

ГЛАВА 3
ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

ИБ Университета базируется на принципах конфиденциальности, целостности, подлинности, доступности и сохранности информации в ИС Университета.

Необходимый уровень безопасности достигается путем реализации мер, направленных на минимизацию возможного ущерба за счет:

профилактики нарушения ИБ;

своевременного обнаружения нарушений ИБ;

эффективного восстановления нормального состояния ресурсов и функционирования ИС.

Обеспечение целостности и конфиденциальности информации и информационных ресурсов ИС достигается:

управлением доступом пользователей к информации;

резервным копированием информации и резервированием инфраструктуры;

контролем действий пользователей, влияющими на работоспособность ИС;

наличием антивирусной защиты в составе системы защиты информации (далее - СЗИ);

средствами криптографической защиты информации (при необходимости).

Доступность информационных ресурсов и услуг ИС пользователям обеспечивается:

резервированием аппаратных и программных средств ИС;

наличием регулярно актуализируемых и проверенных на практике планов обеспечения непрерывной работы и восстановления ИС;

Подлинность пользователя ИС достигается за счет средств аутентификации ИС.

Сохранность информационных ресурсов и услуг ИС достигается за счет системы хранения данных и реализации резервного копирования.

Работникам Университета предоставляется уровень доступа к объектам ИБ Университета в объеме, необходимом для выполнения своих должностных обязанностей.

Работы в серверных помещениях должны производиться по согласованию с ответственным подразделением по ИБ и под контролем ответственного лица по структурному подразделению.

ГЛАВА 4
ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИС

Подключение компьютеров к ИС Университета производится сотрудниками ОИТ на основании заявки в устной либо письменной форме.

Все работы в пределах Университета выполняются в соответствии с должностными обязанностями только на компьютерах, разрешенных к использованию в Университете.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием имени пользователя и пароля.

Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим.

Запрещается хранить пароль на бумажном или ином носителе. Держать пароль в пределах компьютера, в виде наклеенных стикеров на мониторе, столе, клавиатуре и т.п.

Каждый сотрудник обязан немедленно уведомить ОИТ обо всех случаях предоставления доступа третьим лицам к ресурсам ИС Университета.

Доступ третьих лиц к ИС Университета должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к ИС Университета должен быть четко определен, контролируем и защищен.

Доступ к сети Интернет

Сотрудникам Университета разрешается использовать сеть Интернет только в служебных целях.

Запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности.

Сотрудники Университета перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов.

Запрещен доступ в Интернет через сеть Университета для всех лиц, не являющихся сотрудниками Университета, включая членов семьи.

Системный администратор (инженер-программист) Университета имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет.

Пользователи ИС должны:

осуществлять любые действия в ИС, к которым предоставлен доступ, после авторизации с использованием персональной учетной записи, зарегистрированной в ИС Университета;

использовать персональные компьютеры исключительно для тех целей, для которых они были предоставлены;

немедленно уведомлять ответственное лицо по структурному подразделению или ответственное подразделение за ИБ о возможной компрометации паролей авторизованного доступа к ИС;

блокировать доступ к ИС при уходе с рабочего места для предотвращения использования ИС неавторизованными пользователями. В Университете действует локальная политика, которая автоматически блокирует рабочее место при бездействии пользователя в течение 30 минут.

Любое использование оборудования для целей, не связанных со служебной деятельностью либо целями обучения, расценивается как несанкционированное использование оборудования.

Несанкционированная деятельность субъектов ИБ может обнаруживаться любыми незапрещенными законодательством способами и должна незамедлительно пресекаться.

Рекомендуемые правила пользования электронной почтой

Содержание электронных сообщений должно строго соответствовать корпоративным стандартам в области деловой этики.

Запрещается использование корпоративной электронной почты в личных целях.

Сотрудникам Университета запрещается использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.

Использование сотрудниками Университета публичных почтовых ящиков электронной почты осуществляется только при согласовании с системным администратором (инженером-программистом) Университета.

Сотрудники Университета для обмена документами с партнерами должны использовать только свой официальный адрес электронной почты.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.

Ниже перечислены недопустимые действия и случаи использования электронной почты:

рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

групповая рассылка всем пользователям Университета сообщений/писем;

рассылка рекламных материалов, не связанных с деятельностью Университета;

подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

поиск и чтение сообщений, направленных другим лицам (независимо отспособа их хранения);

пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным илиспособствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам в области этики.

Управление сетью

ОИТ Университета контролируют содержание всех потоков данных проходящих через сеть Университета.

Сотрудникам Университета запрещается:

нарушать информационную безопасность и работу сети Университета;

сканировать порты или систему безопасности;

контролировать работу сети с перехватом данных;

получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;

передавать информацию о сотрудниках или списки сотрудников Университета посторонним лицам;

создавать, обновлять или распространять компьютерные вирусы и прочие вредоносное программное обеспечение.

За несоблюдение вышеперечисленных правил, сотрудники университета могут быть привлечены к дисциплинарной, гражданской, административной либо уголовной ответственности.

ГЛАВА 5
ОТВЕТСТВЕННОСТЬ ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙБЕЗОПАСНОСТИ

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

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

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

Руководители структурных подразделений несут ответственность заознакомление подчиненных работников с правилами по обеспечению информационной безопасности, осуществление контроля за их исполнением, своевременное извещение ОИТ обо всех подозрительных ситуациях при работе с ИС.

Пользователи ИС обязаны соблюдать правила по обеспечению информационной безопасности, своевременно извещать руководителя подразделения обо всех подозрительных ситуациях при работе с ИС.

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.

ГЛАВА 6
ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

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.

ГЛАВА 7
ПОРЯДОК ОРГАНИЗАЦИИ ДИСТАНЦИОННОЙ РАБОТЫ

Сотрудникам Университета предоставляется доступ для дистанционной работы при помощи технологии VPN.

Организацию и согласование удаленного доступа при помощи технологии VPN к ИС Университета осуществляет ОИТ.

Для обеспечения дистанционной работы при помощи технологии VPN с ИС Университета, ОИТ вправе создавать дополнительные средства (методы) аутентификации работников Университета.

ГЛАВА 8
ПОРЯДОК ПЕРЕСМОТРА ДОКУМЕНТА

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.