Учреждение образования
«Белорусский государственный
университет транспорта»

Приложение

УТВЕРЖДЕНО
Приказ ректора университета
18.06.2024 № 735

ПОЛИТИКА

г. Гомель

информационной безопасности

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности (далее – Политика) в учреждении образования «Белорусский государственный университет транспорта» (далее – университет) определяет общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, в том числе и персональных данных, документально закрепленные собственником информационной системы университета.

2. Положения Политики служат основой для разработки локальных правовых актов, регламентирующих в университете вопросы защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.

3. Ответственность за соблюдение информационной безопасности несет каждый работник университета, при этом первоочередной задачей является обеспечение безопасности всех активов университета. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив университета. Главные цели университета не могут быть достигнуты без своевременного и полного обеспечения работников информацией, необходимой им для выполнения своих обязанностей.

4. Политика в университете определяется в соответствии со следующими нормативными правовыми актами:

Конституция Республики Беларусь;

Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее – Закон о защите персональных данных);

Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации».

5. 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).

6. Настоящий документ не охватывает вопросы защиты информации, отнесенной к государственным секретам. Защита данного вида информации регламентируется соответствующими нормативными правовыми актами.

7. Положения Политики доводятся под подпись и являются обязательными для работников структурных подразделений университета, организующих и обеспечивающих эксплуатацию ИС при выполнении своих трудовых обязанностей и обучающихся университета, взаимодействующих с ИС в процессе обучения в университете, иных пользователей ИС, физических или юридических лиц, выступающих в качестве информационных посредников, операторов информационных систем и связи.

8. Политика должна актуализироваться в связи с изменениями в законодательстве по вопросам защиты информации, изменениями в организационной структуре или в информационной инфраструктуре университета. Поддержание положений Политики в актуальном состоянии осуществляет Центр информационных систем и технического обеспечения (далее – ЦИСиТО).

ГЛАВА 2
ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

9. Для целей Политики применяются термины в значениях, определенных в Положении о технической и криптографической защите информации утвержденной Указом Президента Республики Беларусь от 16.04.2013 № 196, Законе Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (за исключением термина «персональные данные»), Законе Республики Беларусь от 7.05.2021 № 99-З «О защите персональных данных», а также следующие термины и их определения:

администрирование ИС – это предоставление пользователям соответствующих прав использования возможностей работы с ИС и обеспечение целостности данных;

активы – информация или ресурсы, которые должны быть защищены средствами системы защиты информации, используемыми в ИС;

анализ риска – систематическое использование информации для выявления источников и оценки степени риска;

атака – попытка нарушения ИБ или попытка обхода средств управления безопасностью ИС;

аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности;

доступность – свойство активов ИС, заключающееся в возможности их использования по требованию субъекта, имеющего соответствующие полномочия, за приемлемое время;

информационная безопасность – состояние защищенности информации и бизнес-процессов университета, объединяющих в своем составе работников и обучающихся университета, от внешних и внутренних угроз в информационной сфере;

информационная система – совокупность банков данных, информационных технологий и комплекса программно-технических средств (далее – КПТС), применяемых для обеспечения бизнес-процессов университета;

инцидент информационной безопасности – одно или ряд нежелательных или непредвиденных событий в области ИБ, при которых имеется значительная вероятность компрометации функционирования деловых процессов или реализации угрозы ИБ;

комплекс программно-технических средств – совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий;

контролируемая зона – территория вокруг объекта информатизации, здание, часть здания, в пределах которого исключено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих разрешения на постоянный или разовый доступ на объект;

конфиденциальность – свойство информации, обрабатываемой ИС, быть недоступной и закрытой от раскрытия и использования пользователями, логическими объектами или процессами ИС, которые не имеют соответствующих полномочий;

критический ресурс – объекты информационной сети, несанкционированный доступ к которым может повлечь за собой доступность информационных систем;

пользователь ИС – физическое лицо, обладающее правом доступа к ИС;

риск ИБ – потенциальная возможность реализации угроз ИБ, которая может повлечь нарушение или прекращение функционирования ИС;

система защиты информации (далее – СЗИ) – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации в ИС университета;

событие ИБ – идентифицированное возникновение состояния ИС, услуги или сети, указывающее на возможное нарушение ИБ или отказ средств защиты, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью;

целостность – свойство сохранения полноты состава и неизменности активов ИС;

угроза – описание возможности воздействия на ИС в понятиях источник угроз (нарушитель), актив, который подвергается атаке.

ГЛАВА 3
НАЗНАЧЕНИЕ, ПРИЧИНЫ И ЦЕЛИ ПОЛИТИКИ

10. Назначение настоящей Политики заключается в повышении осведомленности пользователей в области рисков, связанных с информационными ресурсами университета, определении степени ответственности и обязанностей работников по обеспечению информационной безопасности в университете, обеспечении регулярного контроля за соблюдением положений настоящей Политики и проведении периодических проверок соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки ректору университета.

11. Целями и причинами защиты информации являются:

сохранение конфиденциальности информационных ресурсов;

обеспечение непрерывности доступа к информационным ресурсам университета для поддержки процессов;

защита целостности деловой информации с целью поддержания возможности университета по оказанию услуг высокого качества и принятию эффективных управленческих решений;

защита университета от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС, а также минимизация рисков ИБ.

12. Основными задачами университета в части обеспечения безопасности информации в ИС являются:

реализация требований законодательства 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 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 трудовых обязанностей);

обеспечение аутентификации пользователей;

обеспечение регистрации действий пользователей ИС в системных журналах;

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;

планирование, реализация и контроль эффективности использования защитных мер и СЗИ, создание механизма оперативного реагирования на угрозы ИБ;

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

ГЛАВА 4
ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕЙ ПОЛИТИКИ

13. Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации университета. Соблюдение настоящей Политики обязательно для всех работников университета, включая филиалы. В договорах с третьими лицами, получающими доступ к информации университета, должна быть оговорена обязанность третьего лица по неразглашению сведений, содержащих конфиденциальную информацию об университете, которая станет ему доступна в процессе выполнения своих обязанностей по договору.

14. Университету принадлежат на праве собственности (в том числе на праве интеллектуальной собственности) вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления деятельности в соответствии с действующим законодательством.

Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования университета, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех подразделений и персонала университета.

ГЛАВА 5
ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ

15. Перечень информационных систем (информационных ресурсов), находящихся на балансе университета:

программное средство 1С Предприятие по ведению бухгалтерского, кадрового учета. Отнесена к соответствующему классу 4-юл типовых информационных систем;

программный комплекс собственной разработки Управление образованием (АСУ ВУЗ);

почтовый сервер домена bsut.by;

программа реконструкции механизма дорожно-транспортного происшествия "PC-crash";

программа для статистического анализа данных, процедур и методов statistica ultimate acad;

программа для расчета заработной платы работников Мапсофт. Отнесена к соответствующему классу 4-спец типовых информационных систем;

программа по расчету смет и процентовок SXW. Отнесена к соответствующему классу 4-спец типовых информационных систем;

программный комплекс Credo (Кредо) для учреждения высшего образования;

программа "Каноэ";

программа "Аркит";

веб-сайт (портал) учреждения образования «Белорусский государственный университет транспорта». Отнесена к соответствующему классу 5-гос типовых информационных систем.

ГЛАВА 6
ОТВЕТСТВЕННОСТЬ ЗА ИНФОРМАЦИОННЫЕ АКТИВЫ

16. В отношении всех собственных информационных активов университета, активов, находящихся под контролем университета, а также активов, используемых для получения доступа к инфраструктуре университета, должна быть определена ответственность соответствующего работника университета.

ГЛАВА 7
КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ, ПОРЯДОК ИХ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

17. Субъектами информационной безопасности являются:

ответственные за ИБ в ИС – должностные лица университета или структурные подразделения, обеспечивающие ИБ и определенные приказом ректора университета по каждой ИС;

ответственное подразделение по защите сетевой и вычислительной инфраструктуры университета – структурное подразделение, организующее разработку, внедрение и функционирование технической системы ИБ,

имеющее в составе специалистов, выполняющих функции администратора ИБ ИС. Ответственным подразделением по информационной безопасности университета является Центр информационных систем и технического обеспечения университета;

ответственное лицо по структурному подразделению – работник университета, назначаемый руководителем структурного подразделения, обеспечивающий корректное и безопасное функционирование ИС, компьютеров и сети структурного подразделения и выполняющий функции системного администратора структурного подразделения;

пользователи ИС – работники, обучающиеся, абитуриенты университета, использующие ИС для решения задач, возникающих в процессе выполнения должностных обязанностей, обучения или поступления в университет.

18. При планировании и реализации мероприятий по обеспечению ИБ в университете осуществляются:

проектирование, внедрение и поддержание в актуальном состоянии СЗИ;

разработка и поддержание в актуальном состоянии локальных правовых актов университета по вопросам ИБ;

разграничение, при необходимости, доступа пользователей при работе на ПЭВМ;

обучение пользователей ИС по вопросам ИБ.

19. В процессе эксплуатации ИС осуществляются:

контроль за соблюдением требований, установленных локальными правовыми актами университета в области ИБ;

контроль за порядком использования ИС;

мониторинг функционирования ИС и СЗИ;

протоколирование (ведение log-файлов) действий пользователей;

выявление угроз (анализ журналов аудита), которые могут привести к сбоям, нарушению функционирования ИС;

регулярное создание резервных копий информации, в соответствии с Распоряжением первого проректора от 29.02.2024 № 16 «О защите данных»;

выявление и фиксация инцидентов ИБ, принятие мер по своевременному реагированию на инциденты ИБ, выполнению мероприятий по недопущению инцидентов ИБ;

при увольнении работника все предоставленные пользователю права доступа к ресурсам ИС удаляются. Ответственными за удаление доступа к ресурсам ИС являются:

– ответственный по информационной безопасности подразделения, к которому относится увольняемый работник;

– работники, назначенные приказом ректора по представлению начальника ЦИСиТО ответственными за информационные системы (ресурсы), обслуживаемые ЦИСиТО, с обязательной записью в журнал

регистрации удаления доступа пользователя к информационным системам (ресурсам).

20. В случае несоответствия заданным критериям или их изменения производится корректировка СЗИ ИС.

21. Объектами ИБ являются:

информация, хранящаяся и обрабатываемая в ИС университета, а также передаваемая в университете при выполнении работ, оказании услуг (классификация информации, хранящейся и обрабатываемой в ИС университета, представлена в разделе Перечень информационных систем);

КПТС, включающий технические, программные и программно-аппаратные средства обработки, передачи и отображения информации, в том числе каналы передачи данных и информационного обмена, средства технической и криптографической защиты информации.

22. Основными составляющими КПТС университета являются компоненты, входящие в состав корпоративной информационной сети университета:

коммуникационная инфраструктура;

информационные системы;

программное обеспечение, в том числе обеспечивающее функционирование центра обработки данных и коммуникационной инфраструктуры;

автоматизированные рабочие места работников и студентов.

23. КПТС должен располагаться в помещениях, исключающих несанкционированный доступ к ним и обеспечивающих их бесперебойную круглосуточную эксплуатацию в климатических условиях, указанных в документации на эксплуатацию.

24. Порядок информационного взаимодействия субъектов с объектами информационной безопасности университета определяется локальными правовыми актами университета.

25. Порядок информационного взаимодействия объектов между собой определяется эксплуатационной (технической) документацией на ИС университета.

ГЛАВА 8
ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Работники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация университета.

26. Аппаратное обеспечение.

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (например, манипуляторы типа «мышь», клавиатуры), коммуникационное оборудование (например, факс-модемы, сетевые

адаптеры и концентраторы), для целей настоящей Политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное университетом, является его собственностью и предназначено для использования исключительно в рабочих целях.

Данные не должны быть скомпрометированы в случае халатности или небрежности, приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

При записи какой-либо информации на носитель для передачи его контрагентам необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных.

Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты, и прочие переносные устройства не относятся к числу устройств, имеющих надежные механизмы защиты данных. На подобных устройствах не рекомендуется хранить конфиденциальную информацию.

27. Программное обеспечение.

Все программное обеспечение, установленное на предоставленном университетом компьютерном оборудовании, является собственностью университета и должно использоваться исключительно в рабочих целях.

Работникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено руководителю.

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты с актуальными базами данных сигнатур (регулярное обновление).

Работники университета не должны блокировать антивирусное программное обеспечение.

ГЛАВА 9
ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

28. Электронные сообщения (удаленные или не удаленные) могут быть доступны или получены государственными органами для их использования в качестве доказательств в процессе судебного разбирательства. Поэтому содержание электронных сообщений должно строго соответствовать корпоративным стандартам в области деловой этики.

Строго конфиденциальная информация университета не подлежит пересылке третьим лицам по электронной почте.

Доступ к электронной почте предоставляется работникам университета для выполнения своих трудовых обязанностей только с использованием официальных почтовых ящиков (доменное имя bsut.by). Использование бесплатных почтовых сервисов (Gmail, Яндекс.Почта, Mail.ru и т.п.) в рабочих целях является недопустимым.

Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма, и факсимильные сообщения.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей.

Ниже перечислены недопустимые действия и случаи использования электронной почты:

рассылка сообщений личного характера;

рассылка рекламных материалов, не связанных с деятельностью университета;

подписка на рассылку, участие в дискуссиях и подобные услуги в личных целях;

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

пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует 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.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью.

29. При просмотре входящих писем:

внимательно проверять адрес отправителя и получателя;

не доверять письмам, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;

не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они заменены на слова, длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com, и т.д.);

внимательно относится к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками

ГЛАВА 10
ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИС

30. Пользователи 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;

использовать в своей деятельности легально приобретенное ПО;

использовать флеш-накопители, внешние жесткие диски и т. д. на рабочих местах только после предварительной проверки содержимого на предмет вредоносного ПО ответственными за соблюдение политики безопасности в подразделениях;

использовать доступные механизмы ИБ для защиты конфиденциальности и целостности собственной информации, когда это требуется;

устанавливать и использовать пароли в соответствии с требованиями локальных правовых актов по вопросам ИБ;

не хранить пароли в открытом доступе, в текстовых или иных файлах на локальных дисках;

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.

31. Любое использование оборудования для целей, не связанных с трудовой деятельностью либо целями обучения, расценивается как несанкционированное использование оборудования.

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

ГЛАВА 11
СООБЩЕНИЕ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, МЕРЫ РЕАГИРОВАНИЯ

32. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

33. Ответственные лица за ИБ обязаны составить докладную записку об известных случаях нарушения политики безопасности на имя ректора университета, предварительно согласовав ее с начальником ЦИСиТО. На

основании докладной записки проводится проверка с принятием необходимых мер реагирования.

34. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения работник обязан:

проинформировать специалистов университета;

не пользоваться зараженным компьютером;

не подсоединять этот компьютер к компьютерной сети университета до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование специалистами университета.

35. Нарушение политики информационной безопасности является нарушением Правил внутреннего трудового распорядка университета.

ГЛАВА 12
УПРАВЛЕНИЕ СЕТЬЮ

36. Обязательное изменение заводских реквизитов доступа (логин и пароль) для монтируемого сетевого оборудования. Выполняется работниками, ответственными за информационную безопасность подразделения, на баланс которого это оборудование поступает.

37.Работникам университета запрещается:

нарушать информационную безопасность и работу сети университета;

запрещено самовольное подключение компьютерного оборудования к сети университета, изменение свойств подключения к сети уже подключенного оборудования;

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 работниках или списки работников университета посторонним лицам;

создавать, обновлять или распространять компьютерные вирусы и прочее разрушительное программное обеспечение.

ГЛАВА 13
ЗАЩИТА И СОХРАННОСТЬ ДАННЫХ

38. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

Необходимо регулярно делать резервные копии всех основных рабочих данных и программного обеспечения.

39. Работники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп и к которым они имеют санкционированный доступ.

40. Все процедуры по внесению изменений в информационные системы и сервисы должны быть документированы и согласованы с проректором по учебной работе и проректором, курирующим вопросы безопасности, режима и кадров.

Начальник Центра информационных систем и технического обеспечения А.В.Рычков