БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА
Приказ ректора БГУ
_____ № _____

ПОЛИТИКА
информационной безопасности Белорусского государственного университета

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности (далее – Политика) Белорусского государственного университета (далее – БГУ) разработана в соответствии с требованиями Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66.

Нормативной правовой основой Политики служат:

Гражданский кодекс Республики Беларусь;

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»;

Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О концепции информационной безопасности Республики Беларусь»;

Указ Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации»;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»;

иные нормативные правовые акты Республики Беларусь в области информатизации, безопасности и защиты информации, международные стандарты в области информационной безопасности продуктов и систем информационных технологий.

2. Политика определяет общие цели и принципы деятельности по защите БГУ 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).

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

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

5. Политика должна актуализироваться в связи с изменением в законодательстве Республики Беларусь в области защиты информации, изменениями в организационной структуре или в информационной инфраструктуре БГУ, но не реже одного раза в год. Поддержание положений Политики в актуальном состоянии осуществляет отдел кибербезопасности Центра информационных технологий (далее – ЦИТ).

ГЛАВА 2
ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

6. Для целей Политики применяются термины в значениях, определенных в Положении о технической и криптографической защите информации, Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (за исключением термина «персональные данные»), Законе Республики Беларусь от 7 мая 2021 г. № 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 БГУ, объединяющих в своем составе работников и обучающихся БГУ, 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 БГУ;

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, лицами, 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 БГУ;

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), атака и актив, который подвергается атаке.

ГЛАВА 3
ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

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

8. Основными задачами БГУ 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 БГУ;

минимизация ущерба, который может быть нанесен БГУ 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 регистрации действий пользователей ИС в системных журналах и организация контроля этих действий путем анализа содержимого журналов;

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 БГУ;

планирование, реализация и контроль эффективности использования

защитных мер и СЗИ, создание механизма оперативного реагирования на угрозы ИБ;

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

ГЛАВА 4
СУБЪЕКТЫ И ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПОРЯДОК ИХ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

9. Субъектами информационной безопасности являются:

ответственные за ИБ в ИС – должностные лица БГУ или структурные подразделения, обеспечивающие ИБ в той или иной ИС, определенные в пунктах 37-52 настоящей Политики;

ответственное подразделение по защите сетевой и вычислительной инфраструктуры БГУ – структурное подразделение, организующее разработку, внедрение и функционирование технической системы ИБ, имеющее в составе специалистов, выполняющих функции администратора ИБ ИС. Ответственным подразделением по информационной безопасности БГУ является Центр информационных технологий БГУ;

ответственное лицо по структурному подразделению – работник БГУ, назначаемый руководителем структурного подразделения согласно приказу ректора от 13.03.2017 №54-В, обеспечивающий корректное и безопасное функционирование ИС, компьютеров и сети структурного подразделения и выполняющий функции системного администратора структурного подразделения. Информацию об ответственном лице с указанием электронных адресов и рабочих телефонов руководитель структурного подразделения предоставляет в ЦИТ в виде докладной записки в течение трех дней со дня его назначения;

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

10. При планировании и реализации мероприятий по обеспечению ИБ в БГУ осуществляются:

инвентаризация информационных ресурсов БГУ и уточнение состава ИС;

оценка важности (категорирование) информационных ресурсов и элементов ИС;

формирование методики оценки рисков (установление критериев рисков для ИС и информационных ресурсов БГУ и формирование методики обработки рисков);

проектирование, внедрение и поддержание в актуальном состоянии СЗИ;

разработка и поддержание в актуальном состоянии локальных правовых

актов БГУ по вопросам ИБ;

обучение пользователей ИС по вопросам ИБ.

11. Для проверки соответствия системы управления ИБ требованиям законодательства о защите информации, оценки степени (качества) защиты БГУ от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС проводятся периодические аудиты ИБ согласно документации системы защиты информации.

12. В процессе эксплуатации ИС осуществляются:

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

контроль за порядком использования ИС;

мониторинг функционирования ИС и СЗИ;

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

резервное копирование информации, содержащейся в ИС;

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

13. На основе анализа функционирования системы управления ИБ в ходе эксплуатации ИС осуществляется постоянная оценка соответствия уровня защищенности ИС установленным критериям риска.

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

14. Объектами ИБ являются:

информация, хранящаяся и обрабатываемая в ИС БГУ, а также передаваемая в БГУ при оказании услуг (классификация информации, хранящейся и обрабатываемой в ИС БГУ, 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.

15. Основными составляющими КПТС БГУ являются компоненты, входящие в состав корпоративной информационной сети БГУ:

центр обработки данных (далее – ЦОД);

коммуникационная инфраструктура;

информационные системы;

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

инфраструктуры;

автоматизированные рабочие места работников и студентов.

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

17. Порядок информационного взаимодействия субъектов с объектами информационной безопасности БГУ определяется локальными правовыми актами БГУ.

18. Порядок информационного взаимодействия объектов между собой определяется эксплуатационной (технической) документацией на ИС БГУ.

ГЛАВА 5
ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

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

20. 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.

21. Обеспечение целостности и конфиденциальности информации и информационных ресурсов ИС достигается:

управлением доступом пользователей к информации;

резервным копированием информации и резервированием инфраструктуры;

контролем действий пользователей, в частности действий, производимых с критическими ресурсами, влияющими на работоспособность ИС;

наличием антивирусной защиты в составе СЗИ;

средствами криптографической защиты информации (при необходимости).

22. 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;

наличием соглашения с оператором сети Интернет об уровне предоставления сервиса, содержащим описание услуги, права и обязанности сторон, согласованный уровень качества предоставления услуги (доступность,

надежность, безопасность и управляемость);

наличием документированных процедур, регламентирующих процессы жизненного цикла программно-технических средств, направленных на обеспечение непрерывности функционирования ИС.

23. Подлинность пользователя ИС достигается за счет средств аутентификации ИС.

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

25. Управление инцидентами ИБ осуществляется в соответствии с установленными правилами управления инцидентами ИБ в ИС.

26. Для всех критических ресурсов определяются правила, установленные Положением о копировании, резервировании и восстановлении информации.

27. Порядок и правила предоставления доступа к объектам информационной безопасности БГУ определяется локальными правовыми актами БГУ.

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

29. Физический доступ к КПТС (охраняемые зоны, периметры безопасности и т.п.) обеспечивается в соответствии с Инструкцией о порядке организации доступа в серверные помещения БГУ.

Технические средства защиты оборудования должны включать в себя источники бесперебойного питания, трансформаторы и кондиционеры.

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

31. Размещение ИС, обрабатывающих информацию ограниченного распространения, в виртуальной инфраструктуре центров обработки данных сторонних организаций, предоставляющих соответствующие услуги, должно производиться исключительно при условии выполнения данными организациями требований законодательства Республики Беларусь в сфере защиты информации и по согласованию с ЦИТ.

ГЛАВА 6
ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИС

32. Пользователи ИС должны:

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

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

использовать в своей деятельности легально приобретенное ПО;

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;

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.

33. 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.

ГЛАВА 7
ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ

34. В БГУ функционируют следующие ИС:

электронный почтовый сервис;

автоматизированная ИС «Студенты»;

автоматизированная ИС «Студгородок»;

автоматизированная ИС «Абитуриент»;

распределенная автоматизированная ИС «Персональный кабинет сотрудника БГУ»;

ИС «Телефония БГУ»;

ИС «Система сайтов БГУ»;

ИС «Система дистанционного обучения БГУ»;

автоматизированная ИС «Бухгалтерия»;

автоматизированная ИС «Управление организационно-штатной структурой и персоналом БГУ»;

ИС «СДО ДЕЛО»;

ИС «Электронная библиотека»;

система корпоративной видеоконференцсвязи;

главный сайт БГУ.

35. Для обеспечения работоспособности ИС используются системы виртуализации Microsoft Hyper-V и VMWare ESXi, OpenStack, структурированная кабельная система, сервера с операционной системой семейства Windows и семейства Linux. Для доступа к информационным

системам используются персональные компьютеры, находящиеся во внутренней сети БГУ с операционными системами семейства Windows и семейства Linux.

36. Для получения доступа к ИС и информационной сети БГУ сотрудник заполняет заявление, расположенное на внутреннем сайте intranet.bsu/cit в разделе «Регистрация».

37. Электронный почтовый сервис, доступный по адресу webmail.bsu.by, относится к классу 3-юл. Администрирование обеспечивает отдел администрирования сетевой инфраструктуры ЦИТ. Доступ имеют все пользователи информационной сети БГУ. Информационную безопасность данной ИС осуществляет ЦИТ.

38. Автоматизированная ИС «Студенты» относится к классу 3-ин. Администрирование обеспечивает отдел прикладного программного обеспечения ЦИТ. Доступ к редактированию информации в автоматизированной ИС «Студенты» предоставляется по заявлению, расположенному на внутреннем сайте intranet.bsu/cit в разделе «Доступ к информационным базам данных» и подписанному руководителем структурного подразделения и начальником Главного управления образовательной деятельности. Доступ получают пользователи информационной сети БГУ, которым в рамках выполнения должностных обязанностей необходима информация, содержащаяся в данной ИС. Права, предоставляемые пользователю ИС, определяются руководителем структурного подразделения и начальником Главного управления образовательной деятельности. Доступ к личному кабинету студента, который является частью ИС «Студенты», получают все обучающиеся БГУ. Информационную безопасность данной ИС осуществляет ЦИТ.

39. Автоматизированная ИС «Студгородок» относится к классу 3-ин. Администрирование обеспечивает Студенческий городок БГУ. Доступ к автоматизированной ИС «Студгородок» получают пользователи информационной сети БГУ, которым в рамках выполнения должностных обязанностей необходима информация, содержащаяся в данной ИС, по докладной записке на имя начальника Студенческого городка БГУ. Информационную безопасность данной ИС осуществляет Студенческий городок, и/или разработчики, и/или обслуживающая организация данной ИС при технической поддержке ЦИТ.

40. Автоматизированная ИС «Абитуриент» относится к классу 3-ин. Администрирование обеспечивает отдел прикладного программного обеспечения ЦИТ. Доступ к редактированию информации автоматизированной ИС «Абитуриент» предоставляется по заявлению, расположенному на внутреннем сайте intranet.bsu/cit в разделе «Доступ к информационным базам данных» и подписанному секретарем приемной комиссии и начальником ЦИТ. Доступ получают пользователи информационной сети БГУ, которым в рамках

выполнения должностных обязанностей необходима информация, содержащаяся в данной ИС либо согласно приказу ректора. Права, предоставляемые пользователю ИС, определяются секретарем приемной комиссии. Доступ к личному кабинету абитуриента, который является частью ИС «Абитуриент», получают пользователи, зарегистрировавшиеся на данном ресурсе. Информационную безопасность данной ИС осуществляет ЦИТ.

41. Распределенная автоматизированная ИС «Персональный кабинет сотрудника БГУ», доступная по внутреннему адресу cabinet.bsu.by, относится к классу 3-ин. Администрирование обеспечивает отдел администрирования программно-технической инфраструктуры ЦИТ. Доступ к распределенной автоматизированной ИС «Персональный кабинет сотрудника БГУ» имеют все сотрудники БГУ, которые являются пользователями информационной сети БГУ. Информационную безопасность данной ИС осуществляет ЦИТ.

42. ИС «Телефония БГУ» относится к классу 3-ин. Администрирование обеспечивает отдел эксплуатации информационно-коммуникационных систем ЦИТ. Доступ к автоматизированной ИС «Телефония БГУ» пользователи информационной сети БГУ получают по заявлению, расположенному на внутреннем сайте intranet.bsu/cit в разделе «Доступ к информационным базам данных» и подписанному руководителем структурного подразделения и начальником ЦИТ. Права, предоставляемые пользователю ИС, определяются начальником отдела эксплуатации информационно-коммуникационных систем ЦИТ. Информационную безопасность данной ИС осуществляет ЦИТ.

43. ИС «Система сайтов БГУ» относится к классу 5-гос. Администрирование технической и сетевой инфраструктуры ИС «Система сайтов БГУ» осуществляет отдел администрирования программно-технической инфраструктуры ЦИТ. Администрирование выделенных серверов структурного подразделения в ИС «Системы сайтов БГУ» обеспечивает ответственный по структурному подразделению. Информационную безопасность данной ИС осуществляют ответственные лица по структурному подразделению при технической поддержке ЦИТ.

44. ИС «Система дистанционного обучения БГУ» относится к классу 3-ин. Администрирование ИС «Система дистанционного обучения БГУ» обеспечивает отдел администрирования программно-технической инфраструктуры ЦИТ. Администрирование выделенного сайта структурного подразделения ИС «Системы дистанционного обучения БГУ» осуществляется ответственными по структурному подразделению. Доступ к ИС «Система дистанционного обучения БГУ» имеют все пользователи информационной сети БГУ. Информационную безопасность данной ИС осуществляет ЦИТ.

45. Автоматизированная ИС «Бухгалтерия» относится к классу 3-юл. Администрирование и эксплуатацию осуществляет Главное управление

бухгалтерского учета и финансов. Доступ к автоматизированной ИС «Бухгалтерия» получают пользователи, которым в рамках выполнения должностной обязанностей необходима информация, содержащаяся в данной ИС. ИБ данной ИС осуществляет отдел информатизации бухгалтерского учета, и/или разработчики, и/или обслуживающая организация при технической поддержке ЦИТ в части безопасности на сетевом уровне.

46. Автоматизированная ИС «Управление организационно-штатной структурой и персоналом БГУ» относится к классу 3-юл. Администрирование обеспечивает отдел прикладного программного обеспечения ЦИТ. Доступ к автоматизированной ИС «Управление организационно-штатной структурой и персоналом БГУ» (за исключением администрирования организационной и штатной структурой БГУ) получают пользователи информационной сети БГУ по заявлению, расположенному на внутреннем сайте intranet.bsu/cit в разделе «Доступ к информационным базам данных». Права, предоставляемые пользователю ИС, определяются начальником управления по работе с персоналом. Доступ к автоматизированной ИС «Управление организационно-штатной структурой и персоналом БГУ» получают пользователи информационной сети БГУ, которым в рамках выполнения должностных обязанностей необходима информация, содержащаяся в данной ИС, в соответствии с должностной инструкцией. Информационную безопасность данной ИС осуществляет ЦИТ.

47. ИС «СДО ДЕЛО» относится к классу 3-юл. Администрирование ИС осуществляется начальником управления организационной работы и документационного обеспечения. Доступ к ИС «СДО ДЕЛО» работники БГУ получают по докладной записке на имя начальника управления организационной работы и документационного обеспечения. Информационную безопасность данной ИС осуществляют управление организационной работы и документационного обеспечения и обслуживающая организация, и/или разработчики, и/или обслуживающая организация при технической поддержке ЦИТ.

48. ИС «Электронная библиотека» относится к классу 3-ин. Администрирование ИС обеспечивает фундаментальная библиотека БГУ. Доступ к ИС «Электронная библиотека» предоставляется всем пользователям информационной сети БГУ. Информационную безопасность данной ИС осуществляет фундаментальная библиотека, и/или разработчики, и/или обслуживающая организация при технической поддержке ЦИТ.

49. Система корпоративной видеоконференцсвязи относится к классу 3-ин. Администрирование ИС обеспечивает отдел сопровождения системного программного обеспечения и антивирусной защиты ЦИТ. Доступ к системе корпоративной видеоконференцсвязи предоставляется пользователям

информационной сети БГУ по докладной записке на имя начальника ЦИТ, подписанной руководителем структурного подразделения. Информационную безопасность данной ИС осуществляет ЦИТ.

50. Главный сайт БГУ, доступный по адресу bsu.by, относится к классу 5-гос. Администрирование обеспечивает Центр корпоративных коммуникаций БГУ. Право на редактирование главного сайта БГУ предоставляется пользователям информационной сети БГУ по докладной записке от руководителя структурного подразделения на имя начальника Центра корпоративных коммуникаций БГУ. Информационную безопасность данной ИС осуществляет Центр корпоративных коммуникаций, и/или разработчики, и/или обслуживающая организация при технической поддержке ЦИТ.

51. При разработке информационной системы, которая будет размещена в ЦОД БГУ либо в инфраструктуре БГУ, разработчики либо заинтересованное структурное подразделение обязаны разработать СЗИ в соответствии с действующим законодательством и согласовать с ЦИТ.

52. Структурные подразделения, которые являются владельцами разработанных информационных систем, которые размещены в ЦОД БГУ либо в инфраструктуре БГУ, обязаны разработать СЗИ в соответствии с действующим законодательством по согласованию с ЦИТ.

53. Технические аспекты защиты сетевой и вычислительной инфраструктуры ЦОД БГУ возлагаются на ЦИТ.

54. При увольнении работника все предоставленные пользователю права доступа к ресурсам ИС удаляются. При изменении трудовых отношений руководитель структурного подразделения уведомляет ЦИТ с помощью докладной записки о лишении прав доступа работника БГУ к ИС, указанным в пунктах 38, 40, 42, 46.

ГЛАВА 8
ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

55. Порядок взаимодействия объектов ИБ БГУ с ИС БГУ определяется локальными документами по каждому взаимодействию.

56. Обновление баз средств антивирусной защиты информации должно осуществляться с периодичностью, рекомендованной производителем антивирусного программного обеспечения.

57. Правила доступа к корпоративной информационно-коммуникационной сети регулируются приказом ректора от 20.06.2022 № 405-ОД.

58. Синхронизация времени программных средств коммутационного оборудования, компьютеров, серверов, центра обработки данных (далее – объектов БГУ) осуществляется ежедневно в автоматическом режиме.

59. Функционирование объектов БГУ должно осуществляться с синхронизацией времени с Интернет-ресурсом Белорусского государственного института метрологии belgim.by и обновлением системного, прикладного программного обеспечения и антивирусных баз с соответствующими ресурсами.

60. К авторизованным сервисам БГУ относятся:

обновление системного и прикладного ПО;

обновление встроенного ПО технических средств;

обновление антивирусных средств защиты информации;

синхронизация времени с источником надежного времени.

61. Взаимодействие объектов БГУ с иными ИС определяются соответствующими документами. Для взаимодействия объектов БГУ с иными ИС должны применяться СЗИ, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы при Оперативно-аналитическом центре при Президенте Республики Беларусь.

ГЛАВА 9
ПОРЯДОК ОРГАНИЗАЦИИ ДИСТАНЦИОННОЙ РАБОТЫ

62. Профессорско-преподавательскому составу БГУ предоставляется автоматический доступ для дистанционной работы с распределенной автоматической ИС «Персональный кабинет сотрудника БГУ» при помощи технологии VPN.

63. Для организации дистанционной работы при помощи технологии VPN руководители (начальники) структурных подразделений формируют списки работников, ИС и ресурсов (сервисов) БГУ с обоснованием необходимости дистанционной работы.

64. Организацию и согласование удаленного доступа при помощи технологии VPN к ИС БГУ осуществляет ЦИТ. Если есть возможность рисков ИБ БГУ, то ЦИТ вправе отказать в удаленном доступе к ИС БГУ.

65. Для обеспечения дистанционной работы при помощи технологии VPN с ИС БГУ и ресурсами (сервисами) БГУ, ЦИТ вправе создавать дополнительные средства (методы) аутентификации работников БГУ.