

	степенью вероятности могут привести к компрометации в бизнес-процессах и создают угрозы для информационной безопасности;
ИОР	информация ограниченного распространения;
ИС	информационная система;
ЛКС БГУИЯ	локальная компьютерная сети БГУИЯ;
ЛПА	локальный правовой акт;
МНИ	машинные носители информации;
ПК	персональный компьютер;
ПО	программное обеспечение;
Пользователь ИС	субъект ИС ЛКС БГУИЯ, осуществляющий деятельность в рамках предоставленных им прав и наделённых обязанностей;
Ресурс ИС	именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;
СВТ	средства вычислительной техники;
СКЗИ	средства криптографической защиты информации;
СНИ	съёмные носители информации;
СУБД	система управления базами данных.

6. Основные нормы, требования и принципы, изложенные в Политике ИБ, а также других локальных правовых актах (далее – ЛПА) БГУИЯ, регламентирующих вопросы ИБ, являются обязательными для выполнения всеми структурными подразделениями и работниками Университета.

7. Все владельцы объектов, подлежащих защите, обязаны обеспечить их защиту в соответствии с требованиями ИБ и должны быть обеспечены БГУИЯ необходимыми для этого ресурсами.

ГЛАВА 2 ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИБ. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИБ

8. Обеспечение ИБ является одним из составных элементов комплексной безопасности Университета. Под обеспечением информационной безопасности понимается деятельность, направленная на обеспечение защищённого состояния объектов информации, в том числе объектов автоматизированных и телекоммуникационных систем.

9. Деятельность БГУИЯ по обеспечению ИБ должна быть направлена на: снижение уровня рисков нарушения ИБ, и как следствие, ассоциированных с ними рисков бизнес-процессов;

предотвращение материального, физического, репутационного или иного ущерба Университету посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки, хранения и передачи;

выполнение требований законодательства Республики Беларусь в области ИБ и защиты информации.

10. Указанные цели достигаются посредством обеспечения и постоянного поддержания следующих значимых свойств ИБ:

- конфиденциальность;
- целостность;
- доступность;
- сохранность.

11. Для достижения основных целей обеспечения ИБ в БГУИЯ применяются организационные, технические и физические меры обеспечения ИБ, направленные на:

- своевременное выявление и устранение источников угроз ИБ, уязвимостей объектов, подлежащих защите, а также причин и условий, способствующих нанесению ущерба в области ИБ;

- снижение рисков нарушения ИБ до приемлемого уровня;

- исключение либо минимизация возможностей реализации угроз ИБ;

- предотвращение инцидентов ИБ, а в случае их возникновения – своевременное реагирование;

- минимизацию последствий реализованных угроз ИБ;

- защиту информации распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (далее – информация ограниченного распространения).

12. Организационные меры предусматривают проведение мероприятий по: созданию систем защиты информации;

- подготовке административно-распорядительных и иных документов, касающихся безопасности функционирования и использования информационных ресурсов, определения режима доступа к ним, порядка и условий обслуживания технических средств и программного обеспечения и пр.;

- обеспечению соблюдения работниками Университета требований Политики ИБ;

- реализации ответственными лицами управленческих функций по организации защиты информации;

- контролю выполнения принятых решений по вопросам информационной безопасности.

13. Технические меры защиты информации подразумевают применение программных, программно-аппаратных средств защиты информации способных решать отдельные задачи по технической защите информации.

14. Физические меры защиты информации предназначены для воспрепятствования физическому проникновению посторонних лиц в помещения, в которых размещаются объекты БГУИЯ, подлежащие защите.

Доступ посторонним лицам в помещения, отнесенные к объектам защиты должен быть ограничен. Технический персонал сторонних организаций, осуществляющий эксплуатацию и ремонт оборудования БГУИЯ,

должен проводить ремонтно-наладочные и профилактические работы в помещениях Университета только в присутствии работников БГУИЯ, имеющих право находиться в указанных помещениях для выполнения своих должностных обязанностей.

ГЛАВА 3 ОБЪЕКТЫ, ПОДЛЕЖАЩИЕ ЗАЩИТЕ, И ИХ КЛАССИФИКАЦИЯ

15. Основным объектом защиты информации является информационная система «Локальная компьютерная сеть БГУИЯ» (далее – ИС) с ее физической и логической инфраструктурой.

16. В порядке, установленном Приказом Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ) № 195 от 12.11.2021 г. (далее – Приказ), ИС отнесена Владельцем к классу 3-ин типовых информационных систем, т.к. в ИС обрабатывается информация, распространение и (или) предоставление которой ограничено, в частности, персональные данные, за исключением специальных персональных данных. ИС имеет подключение к открытым каналам передачи данных.

17. Информационные ресурсы, размещенные в ИС, защищаются в соответствии с Политикой ИБ вне зависимости от физической среды, в которой они зафиксированы и хранятся (серверы, жесткие диски, запоминающие устройства и иные носители информации).

18. Защитой обеспечивается:

информация, распространение и (или) предоставление которой ограничено, не отнесенная к государственным секретам, хранящаяся и обрабатываемая на информационных ресурсах Университета;

общедоступная информация, хранящаяся и обрабатываемая на информационных ресурсах БГУИЯ;

данные ИС (резервные копии, конфигурационные файлы, данные аудита и др.);

общесистемное, прикладное, специальное программное обеспечение (далее – ПО), входящее в состав ИС;

сетевое и серверное оборудование, средства защиты информации ИС.

19. К объектам защиты информации также относятся:

персональные компьютеры (далее – ПК), серверы, сетевое оборудование и другие технические средства, используемые при работе в ИС для сбора, хранения, обработки и передачи информации, в том числе подключаемые к ним съемные носители;

помещения, в которых размещены технические средства ИС.

20. Вся информация, создаваемая и обрабатываемая с использованием ПК, на рабочем месте пользователя ИС является собственностью Университета.

21. Для обработки информации распространение и (или) предоставление которой ограничено, не отнесенная к государственным секретам в БГУИЯ создана и аттестована ИС.

ГЛАВА 4 ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УНИВЕРСИТЕТА

22. Общее руководство процессом обеспечения информационной безопасности Университета осуществляет ректор БГУИЯ.

23. Организацию мероприятий по обеспечению информационной безопасности и контроль за соблюдением требований ИБ осуществляет начальник отдела информационных сетей и обслуживания компьютерной техники (далее – ответственный за ИБ).

24. Руководители всех структурных подразделений БГУИЯ обеспечивают ознакомление сотрудников своих подразделений с ЛПА, регламентирующими вопросы обеспечения ИБ, Университета под роспись и обеспечивают контроль за их исполнением.

25. Пользователи ИС обязаны:

знать и выполнять, в части их касающейся, требования ЛПА Университета, регламентирующие вопросы ИБ;

использовать доступные защитные механизмы в интересах выполнения требований ИБ;

знать основные источники угроз ИБ и содержание основных мероприятий по их нейтрализации (минимизации последствий);

незамедлительно уведомлять непосредственных руководителей, а также ответственного за ИБ о фактах нарушения требований ИБ.

26. В БГУИЯ должны быть определены и в установленном порядке утверждены процедуры реагирования на инциденты ИБ (выявленные нарушения требований ИБ), описывающие последовательность и содержание принимаемых мер.

27. При взаимодействии с внешними организациями (поставщиками оборудования, работ, услуг т.п.), где подразумевается возможность доступа к ИОР, требования по обеспечению ИБ должны регламентироваться положениями, включаемыми в договоры (соглашения о конфиденциальности) с ними.

28. Обязанности работников Университета по выполнению требований ИБ должны включаться в обязательства о неразглашении информации ограниченного распространения.

29. Все принимаемые на работу в БГУИЯ лица должны проходить процедуры (с обязательным документированием результатов процедур), включающие:

30. ознакомление с ЛПА Университета, регламентирующими вопросы обеспечения ИБ и работу с информацией ограниченного распространения, в

объеме, необходимом для исполнения работником своих должностных обязанностей;

31. заключение обязательства с БГУИЯ о неразглашении информации.

ГЛАВА 5 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

32. В качестве обязательного условия безопасного использования информационных ресурсов Политикой ИБ устанавливаются требования по созданию и функционированию системы идентификации и аутентификации пользователей.

33. Все пользователи для доступа (авторизации) к ресурсам ИС, должны пройти процедуру идентификации и аутентификации.

34. Для учётных записей пользователей ИС должна реализовываться парольная политика со следующими требованиями к сложности пароля:

длина пароля не менее 8 символов;

обязательное удовлетворение 3 из 4 следующих требований к паролю:

использование цифр от 0 до 9;

использование заглавных букв латинского алфавита;

использование строчных букв латинского алфавита;

использование знаков, отличных от букв и цифр.

35. Организация идентификации и аутентификации пользователей к ресурсам ИС осуществляется с учетом требований настоящей Политики ИБ и действующих ЛПА.

ГЛАВА 6 ОРГАНИЗАЦИЯ УПРАВЛЯЕМОГО РОЛЕВОГО ДОСТУПА

36. Организация управляемого ролевого доступа работников Университета к ресурсам ИС включает в себя:

назначение ролей работникам БГУИЯ;

распределение прав и обязанностей работников БГУИЯ согласно назначенным ролям;

управление доступом работников БГУИЯ к ресурсам ИС согласно назначенным ролям;

контроль деятельности работников БГУИЯ в рамках назначенных ролей, прав и обязанностей.

37. Назначение ролей работникам БГУИЯ проводится на основании существующих бизнес-процессов и выполняемых работниками обязанностей, определенных должностными инструкциями, с целью исключения концентрации полномочий и снижения риска нарушений ИБ, связанных с потерей значимых свойств ИБ.

38. В интересах исключения концентрации полномочий и обеспечения эффективного контроля целесообразно осуществлять разделение функций

обеспечения ИБ, функций системного администрирования и администрирования СУБД между разными ролями.

39. В интересах снижения риска нарушений ИБ, в рамках одной роли не целесообразно совмещать функции разработки, сопровождения и эксплуатации ИС (ее отдельных элементов) с функциями контроля их выполнения.

40. Для каждой роли определяются конкретные доступные ресурсы ИС, а также допустимые операции с ними.

41. Одновременное назначение пользователю (группе пользователей) нескольких ролей допускается при условии выполнения требований, изложенных в пунктах 6.3-6.5 настоящей Политики ИБ.

42. Ответственными за назначение ролей являются руководители структурных подразделений.

43. При увольнении или изменении трудовых обязанностей работников Университета, имевших доступ к ИС, выполняются соответствующие документированные процедуры пересмотра (отмены) прав доступа.

44. При назначении на должность (приеме на работу) или изменении должностных обязанностей работника, допускаемого к ресурсам ИС и объектам, подлежащим защите, его профессиональные навыки, квалификация и компетентность должны соответствовать назначаемым ролям и быть достаточными для понимания и надлежащего выполнения требований ИБ.

45. Распределение прав и обязанностей работников БГУИЯ в соответствии с назначенными ролями должно строиться таким образом, чтобы в случае любого нарушения ИБ круг виновных лиц был известен или сведен к минимуму.

46. В интересах управления доступом работников БГУИЯ к ресурсам ИС, в обязательном порядке осуществляются идентификация, аутентификация и авторизация пользователей ИС.

47. Действия всех пользователей ИС осуществляются под уникальными идентификаторами (учетными записями). Для пользователей, которым одновременно назначены разные роли в одной системе, допускается использование различных для каждой роли идентификаторов.

48. В БГУИЯ должны разрабатываться и применяться защитные меры, направленные на обеспечение защиты от несанкционированного доступа, повреждения или нарушения целостности информации, необходимой для идентификации, аутентификации и авторизации пользователей ИС.

49. Работники Университета должны быть осведомлены о порядке действий в случае компрометации (подозрения на компрометацию) информации, необходимой для авторизации в ИС.

50. Пользователи ИС обязаны осуществлять доступ к ресурсам, подлежащим защите, только в рамках назначенных ролей, прав и обязанностей.

51. Пользователям ИС запрещено осуществлять любые попытки доступа к активам, к которым они не авторизованы, в том числе и от имени других авторизованных пользователей.

52. Использование встроенной (создаваемой по умолчанию) учетной записи привилегированного администратора должно быть регламентировано и контролироваться ответственным за ИБ.

53. Процедуры управления доступом работников БГУИЯ к ресурсам ИС осуществляется с учетом требований настоящей Политики ИБ и ЛПА.

ГЛАВА 7 ОБЕСПЕЧЕНИЕ ИБ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

54. Доступ к электронной почте предоставляется работникам БГУИЯ для выполнения служебных обязанностей.

55. Электронные письма, создаваемые и сохраняемые с использованием электронной почты БГУИЯ, являются собственностью Университета.

56. Справочники, базы данных адресов электронной почты работников и структурных подразделений являются служебной информацией и не подлежат передаче за пределы БГУИЯ (допускается передача отдельных адресов электронной почты работникам субъектам информационных отношений для взаимодействия по служебным вопросам).

57. Пользователю электронной почты запрещается:

использовать электронные почтовые ящики, не принадлежащие БГУИЯ (размещенные на зарубежных серверах или общедоступных почтовых сервисах), для ведения служебной переписки;

открывать письма без предварительного анализа на предмет подозрительной тематики и адресов (бессвязные наборы букв, символов, иероглифов и т.п.);

открывать письма рекламного характера, предлагающие получить выигрыш в денежной и другой форме, призывающие к получению прибыли (часто в ограниченные временные рамки: «легкие деньги», «быстрый заработок»);

открывать или запускать файлы (приложения), полученные по электронной почте, которые предварительно не были затребованы для получения, кроме служебной переписки и от известных адресатов;

использовать рабочий адрес электронной почты для регистрации на различных интернет-ресурсах, не связанных со служебной деятельностью;

предоставлять иным лицам возможность пользоваться выделенным адресом электронной почты работников и структурных подразделений БГУИЯ;

рассылать сообщения личного характера.

58. Почтовые серверы должны быть сконфигурированы так, чтобы осуществлялась автоматическая проверка входящих электронных писем на

наличие вредоносных программ и защиты от нежелательных электронных сообщений (спама).

59. Организация работы с электронной почтой осуществляется с учетом требований настоящей Политики ИБ и ЛПА.

ГЛАВА 8 ОБЕСПЕЧЕНИЕ ИБ СРЕДСТВАМИ АНТИВИРУСНОЙ ЗАЩИТЫ

60. В ИС Университета должны применяться меры по предотвращению, обнаружению и регистрации фактов внедрения вредоносных программ.

61. На всех СВТ, которые потенциально могут подвергаться воздействию вредоносных программ, должны применяться сертифицированные в национальной системе сертификации средства антивирусной защиты, если иное не предусмотрено технологическими процессами.

62. В случае невозможности установки на СВТ средств антивирусной защиты, должны быть приняты компенсационные меры, обеспечивающие соответствующий уровень защиты программой среды.

63. Вновь устанавливаемое или обновляемое ПО подлежит обязательной предварительной проверке на отсутствие вирусов. После установки или обновления ПО должна выполняться повторная антивирусная проверка.

64. Процедуры установки и обновления средств антивирусной защиты должны максимально автоматизироваться.

65. Установка и обновление средств антивирусной защиты, а также предварительное тестирование устанавливаемых обновлений антивирусных баз производится ответственным за ИБ.

66. В интересах соблюдения установленных в БГУИЯ единых правил и требований, управление средствами антивирусной защиты, а также контроль их состояния и обновления средств антивирусной защиты, сбор информации об инцидентах, связанных с вирусным заражением, должны осуществляться централизованно.

67. В целях защиты от вредоносных программ в БГУИЯ дополнительно должны быть реализованы следующие меры:

запрет использования ПО, не включенного в список разрешенного, который определяется путем утверждения перечня разрешенного ПО;

организация антивирусной проверки всех входящих и исходящих сообщений электронной почты;

защита от реализации угроз, связанных с получением файлов из МНИ, подключаемых к ИС, а также файлов из сети Интернет и/или из любого другого внешнего источника.

68. Выполнение установленных правил антивирусной защиты является обязательным для каждого работника БГУИЯ. Контроль выполнения

требований по антивирусной защите возлагается на руководителей структурных подразделений Университета и ответственного за ИБ.

69. Обеспечение ИБ средствами антивирусной защиты осуществляется с учетом требований настоящей Политики ИБ и ЛПА.

ГЛАВА 9 ОБЕСПЕЧЕНИЕ ИБ ПРИ ИСПОЛЬЗОВАНИИ РЕСУРСОВ СЕТИ ИНТЕРНЕТ, ВЗАИМОДЕЙСТВИИ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

70. Использование ресурсов глобальной компьютерной сети Интернет осуществляется в целях, устанавливаемых БГУИЯ, к которым, как правило, относятся:

получение и распространение информации, связанной с Университетом (в т.ч. путем использования официального сайта БГУИЯ в сети Интернет;

организация внешних каналов связи;

осуществление информационно-аналитической работы в интересах БГУИЯ;

обеспечение канала взаимодействия ИС с иными информационными системами;

обмен электронными почтовыми сообщениями с использованием почтового сервера БГУИЯ только в рамках исполнения служебных обязанностей;

поиск персонала;

профессиональная подготовка персонала;

проведение аудио и видеоконференций;

подписка к доступу электронных баз данных, электронным библиотекам на платной основе;

осуществление взаимодействия с банками;

получение или оказание информационных услуг;

диалог в режиме реального времени (чат) и размещение объявлений;

для связи с поставщиками:

получение сведений о необходимых товарах (работах, услугах) и их поставщиках;

предоставление сведений о потребностях Университета в товарах (работах, услугах);

размещение заказов на необходимые Университету товары (работы, услуги) (без учета заказов, отправленных по электронной почте);

оплата поставляемых товаров (работ, услуг);

получение электронной продукции;

для связи с потребителями:

предоставление сведений об услугах БГУИЯ;

получение заказов на услуги БГУИЯ;

для взаимодействия с государственными органами (организациями):

получение информации о деятельности государственных органов (организаций);

представление государственной статистической отчетности, налоговых деклараций и других документов;

получение государственных услуг в электронном виде без необходимости использования бумажного документооборота при получении таких услуг;

участие в процедурах закупок товаров (работ, услуг).

71. Не допускается использование ресурсов сети Интернет в целях, отличных от установленных БГУИЯ и запрещенных законодательством целям.

72. Взаимодействие с информационными системами других организаций должно осуществляться на основе установленных для таких систем регламентов или предварительно заключенных между сторонами договоров (соглашений), в которых перечисляются необходимые требования (условия) (или даны ссылки на них) по обеспечению ИБ и защиты активов информационных систем от угроз со стороны внешних подключений.

73. Использование сети Интернет и взаимодействие ИС с иными информационными системами должно осуществляться с обязательным соблюдением следующих мер обеспечения ИБ и защиты активов ИС от угроз со стороны внешних подключений:

для доступа к ресурсам сети Интернет должны использоваться только протоколы (сетевые сервисы), соответствующие требованиям по обеспечению ИБ;

должны быть реализованы защитные меры, направленные на противодействие атакам и распространению нежелательных электронных сообщений (спама);

доступ в/из сети Интернет должен производиться только через специализированные программные и/или программно-аппаратные средства;

должна осуществляться фильтрация сетевых пакетов в соответствии с задаваемыми правилами на основе IP-адресов отправителя и получателя, разрешенных портов, протоколов и приложений;

должно осуществляться управление сетевым доступом к сегментам ИС;

должна быть реализована трансляция сетевых адресов для сокрытия топологии ИС;

должны применяться средства обнаружения и предотвращения вторжений с использованием известных шаблонов атак;

должна быть реализована защита от атак типа «отказ в обслуживании»;

должно осуществляться обновление баз сигнатур подсистемы обнаружения вторжений;

должна проводиться антивирусная фильтрация трафика, получаемого из сети Интернет;

для обмена информацией ограниченного распространения со сторонними информационными системами должны использоваться защищённые каналы передачи информации, организованный с

использованием СКЗИ, имеющих сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь; должна проводиться регистрация событий ИБ с заданным уровнем детализации.

74. В интересах обеспечения ИБ при использовании ресурсов сети Интернет санкционируются:

перечень сервисов и ресурсов сети Интернет, доступных для пользователей ИС;

предоставление пользователям ИС прав пользования сервисами и ресурсами сети Интернет в объеме, необходимом для выполнения ими должностных обязанностей.

75. Для публичных информационных ресурсов Университета, размещаемых в сети Интернет, должны быть обеспечены доступность и целостность информации, а также контроль содержания размещаемой на них информации.

76. Организация доступа к информационным ресурсам БГУИЯ через сеть Интернет должна осуществляться через выделенные сегменты корпоративной сети передачи данных с изолированными физическими сетевыми интерфейсами, при одновременном обеспечении скрытности структуры внутренней сети Университета и невозможности доступа нарушителей к ней извне.

77. Контроль за использованием ресурсов сети Интернет возлагается на руководителей структурных подразделений и ответственного за ИБ.

78. Организация работы с ресурсами сети Интернет осуществляется с учетом требований настоящей Политики ИБ и ЛПА.

ГЛАВА 10 ОБЕСПЕЧЕНИЕ ИБ ПРИ ИСПОЛЬЗОВАНИИ СЪЕМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

79. При работе с ИС разрешается использование только служебных съемных носителей информации (далее – СНИ) или носителей информации, прошедших предварительную проверку с использованием сертифицированного средства антивирусной защиты.

80. Служебное СНИ закрепляется за конкретным работником УО БГУИЯ под подпись в журнале регистрации.

81. Проверка СНИ работников производится сотрудниками отдела ТСО не реже раза в неделю, СНИ обучающихся – перед началом работы с ИС при помощи средства антивирусной защиты на компьютере Университета. Контроль за выполнением проверки СНИ обучающимися осуществляет техник, за которыми закреплен компьютерный класс, или работник из числа профессорско-преподавательского состава.

82. Пользователям запрещается:

передавать служебные СНИ сторонним лицам;

принимать и хранить на СНИ файлы от сторонних источников, предварительно не проверенные антивирусным ПО;

копировать и переносить рабочие документы (материалы) со служебных СНИ на веб-ресурсы либо другие носители информации, не относящиеся к деятельности Учреждения, если это не вызвано служебной необходимостью;

подключать СНИ к СВТ, в которых не установлено антивирусное ПО и не обновлены базы сигнатур.

ГЛАВА 11 ОБЕСПЕЧЕНИЕ ИБ ПРИ ИСПОЛЬЗОВАНИИ СКЗИ

83. Для обеспечения таких значимых свойств ИБ как конфиденциальность и целостность, в Университете могут применяться СКЗИ.

84. Решение о необходимости использования СКЗИ в БГУИЯ принимается на основании результатов анализа и оценки рисков нарушения ИБ, а также с учетом особенностей, используемых технологических процессов ИС и требований законодательства в области ИБ .

85. СКЗИ, используемые в Университете, должны реализовываться на основе алгоритмов, соответствующих национальным и международным стандартам, и иметь сертификат соответствия, выданный в соответствии с Национальной системой подтверждения соответствия Республики Беларусь.

86. Пользователи СКЗИ, являющиеся работниками Университета, несут ответственность за:

сохранность и конфиденциальность своего личного ключа подписи, а также носителя ключевой информации;

состав и характер информации, передаваемой с использованием СКЗИ.

87. Управлению криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение) осуществляется в соответствии с требованиями эксплуатационной документации на СКЗИ.

ГЛАВА 12 МОНИТОРИНГ И АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

88. С целью постоянного наблюдения за состоянием ИБ, обнаружения и регистрации отклонений, реализованных защитных мер от требований ИБ, а также оценки полноты и качества их реализации, в БГУИЯ организуется и проводится мониторинг ИБ.

89. Организация мониторинга ИБ осуществляется ответственным за ИБ, другим уполномоченным лицом с возможным привлечением работников иных структурных подразделений Университета (по согласованию с их руководителями).

90. В рамках мониторинга ИБ проводится комплекс мероприятий, направленных на:

выявление новых потенциальных или действительных угроз ресурсам ИС, а также уязвимостей в ИС с целью принятия своевременных мер по снижению рисков;

контроль и оценку состояния ИБ ИС;

проверку действительной реализации защитных мер, их соответствие требованиям ИБ;

регулярный анализ журналов аудита ИБ.

91. При проведении аудита ИБ, как правило, используются стандартные процедуры документальной проверки, опрос работников и анализ журналов регистрации инцидентов ИБ.

ГЛАВА 13 ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ ИБ

92. По мере совершенствования законодательства, развития систем автоматизации, внедрения новых услуг, связанных с передачей информации посредством ИС, Политика может пересматриваться или дополняться.

93. Актуализация Политики ИБ проводится при необходимости, но не реже одного раза в три года с целью приведения в соответствие защитных мер современным угрозам и актуализации требований по защите информации. Внеплановая корректировка Политики проводится в обязательном порядке в следующих случаях:

при изменении ЛПА актов и (или) документов Университета, касающихся ИБ;

при возникновении в процессе деятельности по защите информации ситуаций и(или) инцидентов, которые создают угрозу безопасного функционирования ИС, но необходимость реагирования на них не предусмотрена Политикой ИБ.

94. Положения настоящей Политики ИБ могут дополняться и уточняться другими внутренними нормативными документам БГУИЯ.