Приложение 14
к Положению об
информационной безопасности

Правила
организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов

1. Общие положения

1. Размещение серверов и коммуникационного оборудования НАО «Евразийский Государственный Университет имени Л.Н. Гумилева» (далее - Университет) производится в специализированном серверном помещении, расположенном по адресу: г. Нур-Султан, ул. Сатпаева 2, (далее – Серверная).

2. Серверное помещение располагается в отдельном, непроходном помещении без оконных проемов.

3. Для поверхности стен, потолков и пола применяются материалы, не выделяющие и не накапливающие пыль. Для напольного покрытия применяются материалы с антистатическими свойствами. Серверное помещение защищается от проникновения загрязняющих веществ.

4. Стены, двери, потолок, пол и перегородки серверного помещения обеспечивают герметичность помещения.

5. Двери серверного помещения составляют 1,2 метра в ширину и 2,2 метра в высоту, открываются наружу. Конструкция рамы двери не предусматривает порога и центральной стойки.

6. Серверное помещение оборудовано фальшполом для размещения кабельных систем и инженерных коммуникаций.

7. Монтаж коммуникационных каналов для прокладки силовых и слаботочных кабельных сетей здания выполняется в отдельных или разделенных перегородками кабельных лотках, коробах или трубах, разнесенных между собой. Слаботочные и силовые шкафы устанавливаются раздельно и закрываются на замок.

8. Прокладка кабелей через перекрытия, стены, перегородки осуществляется в отрезках несгораемых труб с герметизацией негорючими материалами.

9. Серверное помещение надежно защищается от внешнего электромагнитного излучения.

10. Система обеспечения микроклимата включает систему кондиционирования, систему вентиляции и систему мониторинга микроклимата. Системы обеспечения микроклимата серверного помещения не объединяются с другими системами микроклимата, установленными в здании.

11. Температура в серверном помещении поддерживается в диапазоне от 20 С до 25 С при относительной влажности от 45% до 55 %.

12. Мощность системы кондиционирования воздуха должна превышать суммарное тепловыделение всего оборудования и систем. Система кондиционирования воздуха обеспечивается резервированием. Электропитание кондиционеров серверного помещения осуществляется от системы гарантированного электропитания или системы бесперебойного электропитания.

13. Система вентиляции обеспечивает приток свежего воздуха с фильтрацией и подогревом поступающего воздуха в зимний период. В серверном помещении давление создается избыточным для предотвращения поступления загрязненного воздуха из соседних помещений. На воздуховодах приточной и вытяжной вентиляций устанавливаются защитные клапаны, управляемые системой пожаротушения.

14. Системы кондиционирования и вентиляции отключаются автоматически по сигналу пожарной сигнализации.

15. Система мониторинга микроклимата контролирует климатические параметры в серверных шкафах и телекоммуникационных стойках:

1) температура воздуха;
2) влажность воздуха;
3) запыленность воздуха;
4) скорость потока воздуха;
5) задымленность воздуха;
6) открытие (закрытие) дверей шкафов.

16. Система охранной сигнализации серверного помещения выполняется отдельно от систем безопасности здания. Сигналы оповещения выводятся в помещение круглосуточной охраны в виде отдельного пульта. Контролю и охране подлежат все входы и выходы серверного помещения, а также внутренний объем серверного помещения. Система охранной сигнализации имеет собственный источник резервированного питания.

17. Расположение камер системы видеонаблюдения выбирается с учетом обеспечения контроля всех входов и выходов в серверное помещение, пространства и проходов возле оборудования. Угол обзора и разрешение камер должны обеспечить распознавание лиц. Изображение с камер выводятся на отдельный пульт в помещение круглосуточной охраны

18. Система пожарной сигнализации серверного помещения выполняется отдельно от пожарной сигнализации здания. В серверном помещении устанавливаются два типа датчиков: температурные и дымовые.

19. Датчиками контролируются общее пространство серверного помещения и объемы, образованные фальшполом. Сигналы оповещения системы пожарной сигнализации выводятся на пульт в помещение круглосуточной охраны.

20. Система пожаротушения серверного помещения оборудуется автоматической установкой газового пожаротушения, независимой от системы пожаротушения здания. В качестве огнегасителя в автоматической установке газового пожаротушения используется специальный нетоксичный газ. Порошковые и жидкостные огнегасители не используются. Установка газового пожаротушения размещается непосредственно в серверном помещении или вблизи него в специально оборудованном для этого шкафу. Запуск системы пожаротушения производится от датчиков раннего обнаружения пожара, реагирующих на появление дыма, а также от ручных датчиков, расположенных у выхода из помещения. Время задержки выпуска огнегасителя составляет не более 30с. Оповещение о срабатывании системы пожаротушения выводится на табло, размещаемые внутри и снаружи помещения. Система пожаротушения выдает команды на закрытие защитных клапанов системы вентиляции и отключение питания оборудования.

Серверное помещение, оборудованное системой пожаротушения, оснащается вытяжной вентиляцией для удаления огнегасящего газа.

21. Система гарантированного электропитания предусматривает наличие двух вводов электропитания от разных источников внешнего электропитания на напряжение ~400/230В, частотой 50 Гц и автономного генератора. Все источники электроэнергии подаются на автомат ввода резерва, осуществляющий автоматическое переключение на резервный ввод электропитания при прекращении, перерыве подачи электропитания на основном вводе. Параметры линий электропитания и сечение жил определяются исходя из планируемой суммарной потребляемой мощности оборудования и подсистем серверного помещения. Линии электропитания выполняются по пятипроводной схеме.

22. Система гарантированного электропитания предусматривает электроснабжение оборудования и систем серверного помещения через источники бесперебойного питания. Мощность и конфигурация источников бесперебойного питания рассчитываются с учетом всего запитываемого оборудования и запаса для перспективного развития. Время автономной работы от источников бесперебойного питания рассчитывается с учетом потребностей, а также с учетом необходимого времени для перехода на резервные линии и времени запуска генератора в рабочий режим.

23. Система заземления серверного помещения выполняется отдельно от защитного заземления здания. Все металлические части и конструкции серверного помещения заземляются с общей шиной заземления. Каждый шкаф (стойка) с оборудованием заземляется отдельным проводником, соединяемые с общей шиной заземления. Открытые токопроводящие части оборудования обработки информации должны быть соединены с главным заземляющим зажимом электроустановки.

24. Заземляющие проводники, соединяющие устройства защиты от перенапряжения с главной заземляющей шиной, должны быть самыми короткими и прямыми (без углов).

25. При построении и эксплуатации системы заземления необходимо руководствоваться:

1) Правилами устройства электроустановок, утвержденными приказом уполномоченного органа в сфере энергетики;

2) стандартом Республики Казахстан СТ РК МЭК 60364-5-548-96 «Электроустановки зданий. Часть 5. Выбор и монтаж электрооборудования». Раздел 548 «Заземление устройства и системы уравнивания электрических потенциалов в электроустановках, содержащих оборудование обработки информации»;

3) стандартом Республики Казахстан СТ РК МЭК 60364-7-707-84 «Электроустановки зданий. Часть 7. Требования к специальным электроустановкам». Раздел 707 «Заземление оборудования обработки информации»;

4) стандартом Республики Казахстан СТ РК ГОСТ 12.1.030-81 «ССБТ. Электробезопасность. Защитное заземление, зануление»;

5) стандартом Республики Казахстан СТ РК ГОСТ 464-79 «Заземление для стационарных установок проводной связи, радиорелейных станций,

радиотрансляционных узлов проводного вещания и антенн систем коллективного приема телевидения. Нормы сопротивления».

2. Назначение документа

26. Настоящие Правила определяют организацию физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов всех автоматизированных информационных систем, принадлежащих Университету.

3. Нормативные ссылки

27. В части правового обеспечения и оснований для разработки данного документа, использовались следующие документы:

1) Концепция информационной безопасности Республики Казахстан до 2016 года, Указ Президента Республики Казахстан от 14 ноября 2011 года № 174;

2) Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V (с изменениями и дополнениями по состоянию на 28.12.2017 г.);

3) Закон Республики Казахстан «О техническом регулировании» от 9 ноября 2004 года;

4) СТ РК 34.005-2002 «Основные термины и определения в области информационных технологий»;

5) СТ РК 34.006-2002 «Основные термины и их определения в области баз данных»;

6) СТ РК 34.007-2002 «Основные термины и их определения в области телекоммуникационных сетей»;

7) ГОСТ ИСО/МЭК 2700-2006 «Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности».

8) СТ РК ИСО/МЭК 27002-2015 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью».

4. Требования к организации физической защиты серверного помещения и контроля доступа

28. Доступ в помещение Серверной предоставлен только авторизованному персоналу.

29. Доступ в Серверную контролируется охранной сигнализацией.

30. Список авторизованного персонала, имеющего доступ в Серверную, ежегодно составляется руководителем отдела коммуникаций, согласовывается с руководителем службы охраны Университета.

31. После завершения работ сотрудник возвращает ключ от Серверной в отдел коммуникаций и делается отметка в соответствующем журнале.

32. Посещения Серверной фиксируются в Журнале учета посещений по форме:

Журнал регистрации посещений серверного помещения

Дата посещения	Время посещения		Наименование проводимых работ	ФИО	Должность	Роспись	Разрешение на посещение (по списку
	Вход	Выход					

							доступа, по заявке)

33. В случае возникновения необходимости доступа в серверное помещение лицам, не входящих в список допуска, оформляется заявка с обоснованием физического доступа. Данная заявка подписывается руководителем отдела коммуникаций, согласовывается с директором департамента информатизации. При наличии разрешительного документа лица, которым разрешен физический доступ в серверное помещение, должны сопровождаться дежурным администратором серверов, находящемся в списке авторизованного доступа.

34. Система контроля и управления доступом обеспечивает только санкционированный вход в серверное помещение и санкционированный выход из него. Преграждающие устройства и конструкция входной двери предотвращают возможность передачи идентификаторов доступа в обратном направлении через тамбур входной двери.

35. Электроснабжение системы контроля и управления доступом (сигнализации) осуществляется от свободной группы щита дежурного освещения. Система контроля и управления доступом обеспечивается резервным электропитанием.

5. Требования по выполнению работ в серверном помещении

36. В случае проведения в Серверные необходимые работы по сопровождению серверного, телекоммуникационного или вспомогательного оборудования, в том числе привлекаемыми сторонними организациями, необходимо обеспечить выполнение мероприятий:

1) о существовании зоны информационной безопасности и проводимых в ней работах должны быть осведомлены только лица, которым это необходимо в силу производственной необходимости;

2) из соображений безопасности и предотвращения возможности злонамеренных действий в охраняемых зонах необходимо избегать случаев работы без надлежащего контроля со стороны уполномоченного персонала Университета;

3) пустующие зоны безопасности должны быть физически закрыты, и их состояние необходимо периодически проверять;

4) использование фото, видео, аудио или другого записывающего оборудования, цифровых камер в мобильных устройствах должно быть разрешено только при получении специального разрешения.

6. Требования по безопасному размещению серверного оборудования

37. Оборудование Университета необходимо размещать таким образом, чтобы свести до минимума излишний доступ в места его расположения;

38. Средства обработки и хранения информации Университета следует размещать так, чтобы, уменьшить риск несанкционированного наблюдения за их функционированием;

39. В Серверной запрещаются: прием пищи, напитков и курение вблизи средств обработки информации Университета;

40. Мониторинг состояния окружающей среды в целях выявления условий (температура, влажность), которые могли бы неблагоприятно повлиять на функционирование средств обработки информации Университета, должен проводиться постоянно сотрудниками отдела коммуникаций.

41. При размещении оборудования Университета дополнительно учитывается:

1) обеспечивается исполнение правил устройства электроустановок утвержденным уполномоченным органом в области коммунального хозяйства;

2) обеспечивается исполнение правил технической эксплуатации электроустановок потребителей, утвержденных уполномоченным органом в области коммунального хозяйства;

3) обеспечивается исполнение требований производителя оборудования к установке (монтажу), нагрузке на перекрытия и фальшпол, с учетом веса оборудования и коммуникаций;

4) обеспечивается наличие свободных служебных проходов для обслуживания оборудования;

5) учитывается организация воздушных потоков системы обеспечения микроклимата;

6) учитывается организация системы фальшполов.

7. Требования по организации вспомогательных услуг для Университета

42. Все вспомогательные услуги, такие как электричество, водоснабжение, канализация, отопление, вентиляция и кондиционирование, должны соответствовать системам, для которых они предназначены. Все инженерные системы и их оборудования должны регулярно осматриваться и соответствующим образом тестироваться для обеспечения их надлежащего функционирования и сокращения риска вследствие их неисправности или сбоя. Также необходимо обеспечить подходящее энергоснабжение, соответствующее техническим характеристикам от производителя оборудования.

43. Чтобы обеспечить безопасное выключение и/или непрерывное функционирование устройств, поддерживающих критические бизнес-процессы, рекомендуется подключать оборудование через UPS. В планах обеспечения непрерывности следует предусматривать действия, которые должны быть предприняты при отказе UPS. Резервный генератор следует применять, если необходимо обеспечить функционирование оборудования в случае длительного отказа подачи электроэнергии от общего источника. Для бесперебойной работы генератора в течение длительного срока необходимо обеспечить соответствующую поставку топлива. Оборудование UPS и генераторы следует регулярно проверять на наличие адекватной мощности, а также тестировать в соответствии с рекомендациями производителя.

44. Аварийные выключатели электропитания необходимо располагать около запасных выходов помещений, где расположено оборудование, чтобы

ускорить отключение электропитания в случае критических ситуаций. Следует обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети.

45. Система водоснабжения должна быть стабильной и приемлемой для:

1) обеспечения кондиционирования воздуха;

2) увлажнения воздуха (при необходимости);

3) оборудования систем пожаротушения.

46. Неисправности в системе водоснабжения могут повредить оборудование или создать помехи для эффективной работы систем пожаротушения. При необходимости устанавливается автоматическая система обнаружения неисправностей в системе водоснабжения.

8. Требования по безопасному использованию кабельной сети

47. Необходимо обеспечить следующие мероприятия:

1) силовые и телекоммуникационные линии, связывающие средства обработки информации, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой;

2) сетевой кабель должен быть защищен от неавторизованных подключений или повреждения, например, посредством использования специального кожуха или выбора маршрутов прокладки кабеля в обход общедоступных участков;

3) силовые кабели должны быть отделены от коммуникационных, чтобы исключить помехи;

4) четко определенная маркировка кабелей и оборудования должна быть использована для минимизации обработки ошибки, такие как неправильно выбранные сетевые кабели;

5) документы со списком обновлений, должны быть использованы для уменьшения вероятности ошибок;

6) использование дублирующих маршрутов прокладки кабеля или альтернативных способов передачи;

7) использование электромагнитного экранирования для защиты кабелей;

8) инициирование технических зачисток и физических осмотров для несанкционированных устройств, присоединенных к кабелям;

9) ограничение доступа к соединительным панелям и кабельным линиям.

9. Требования по безопасному техническому обслуживанию серверного оборудования Университета

48. Необходимо обеспечить следующие мероприятия:

1) оборудование Университета следует обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком;

2) необходимо, чтобы техническое обслуживание и ремонт оборудования Университета проводились только авторизованным персоналом;

3) следует хранить записи обо всех предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного технического обслуживания;

4) необходимо принимать соответствующие меры безопасности при отправке оборудования Университета для технического обслуживания за пределы организации в отношении удаленных, стертых и перезаписанных данных;

5) необходимо соблюдать все требования, устанавливаемые использующимися правилами страхования.

49. При техническом сопровождении оборудования, установленного в серверном помещении, документируются в специальном журнале по нижеприведенной форме:

1) обслуживание оборудования;

2) устранение проблем, возникающих при работе аппаратно-программного обеспечения;

3) факты сбоев и отказов, а также результаты восстановительных работ;

4) послегарантийное обслуживание критически важного оборудования по истечении гарантийного срока обслуживания.

Журнал регистрации технического обслуживания оборудования

Дата	Время работ		Наименование проводимых работ	ФИО	Должность	Роспись	Основание проведения работ
	Начало	Окончание					

50. Обслуживание критически важного оборудования выполняется сертифицированным техническим персоналом.

51. В непосредственной близости от серверного помещения создается склад запасных частей для критически важного оборудования, содержащий запас комплектующих и оборудования для выполнения оперативной замены при проведении ремонтно-восстановительных работ.

52. Вмешательство в работу находящегося в эксплуатации оборудования возможно только с разрешения руководителя отдела коммуникаций либо лица, его замещающего.

10. Требования к безопасной утилизации или повторному использованию оборудования Университета

53. Все компоненты оборудования Университета, содержащего носители данных, следует проверять на предмет удаления всех важных данных и лицензионного программного обеспечения.

54. Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать безопасным образом, а не использовать стандартные функции удаления.

55. В отношении носителей данных, содержащих важную информацию, может потребоваться оценка рисков с целью определения целесообразности их разрушения, восстановления или выбраковки.

56. Служебная информация может быть скомпрометирована вследствие небрежной утилизации или повторного использования оборудования.

11. Требования к выносу/вносу оборудования Университета

57. Оборудование Университета, информация или программное обеспечение не должны вывозиться за пределы подразделения организации без соответствующего разрешения.

58. Запрещается вывоз оборудования Университета подрядчиками или пользователями сторонних организаций

59. Оборудование следует регистрировать при выносе и при вносе, а также делать отметку, когда оно возвращено.

60. Порядок вноса/выноса оборудования следующий:

1) для вноса (выноса), ввоза (вывоза) материальных ценностей из здания Университета выдается материальный пропуск на бумажном носителе руководителем финансово-хозяйственного отдела на основании заявки руководителей подразделений и их заместителей.

2) материальный пропуск выписывается только на то количество груза (места, веса и др.), которое может быть вынесено (вывезено) одновременно и действителен на дату, указанную в нем.

3) в случае выноса (вывоза) большого количества разноименных товарно-материальных ценностей, к заявке прилагается документы, в котором указан перечень выносимых (вывозимых) товарно-материальных ценностей (например, акт приема-передачи, счет-фактура и др.) Ответственный работник финансово-хозяйственного отдела указывает в материальном пропуске ссылку на соответствующий документ, его наименование, номер и дату. При этом документ, в котором указан перечень выносимых (вывозимых) товарно-материальных ценностей, предъявляется постовому подразделения охраны вместе с материальным пропуском.

4) лицо, на которое выписан материальный пропуск, при выносе (вывозе) материальных ценностей из здания Университета сдает пропуск постовому подразделения охраны.

5) постовой подразделения охраны при проверке материального пропуска устанавливает принадлежность его предъявителя по документам, удостоверяющим личность, наличие подписи руководителя финансово-хозяйственного отдела, а также соответствие выносимых (вывозимых) товарно-материальных ценностей, указанных в пропуске, после чего делает отметку в пропуске о времени выноса (вывоза), заверяет ее подписью и производит соответствующие записи в журнале учета разовых и материальных пропусков.