??????????
??????????
??????????????

- ПРОЦЕДУРА ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ «SDU UNIVERSITY»

????????? ??????????
???????????? ??????????
«SDU UNIVERSITY»

СОДЕРЖАНИЕ

1 ЦЕЛЬ

2 ОБЛАСТЬ ПРИМЕНЕНИЯ

3 ОТВЕТСТВЕННЫЙ ЗА ПРИМЕНЕНИЕ ПРОЦЕДУРЫ

4 ОПРЕДЕЛЕНИЯ

5 СРЕДСТВА КОНТРОЛЯ

5.1 Ответственность за физическую безопасность

5.2 Доступ в Серверное помещение

5.3 Защита конфиденциальной информации в бумажном виде

5.4 Защита конфиденциальной информации в электронном виде

5.5 Стойки для серверного и сетевого оборудования

5.6 Физическое расположение Серверного помещения

5.7 Периодическая проверка физической безопасности

6 ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ И НОСИТЕЛЕЙ ИНФОРМАЦИИ

6.1 Отслеживание электронных носителей

6.2 Вынос ИТ-активов

6.3 Защита сетевых кабелей

6.4 Физическое расположение Серверного помещения

6.5 Оценка рисков для Серверного помещения

6.6 Перебои в подаче электроэнергии

6.7 Наблюдение за Серверным помещением

6.8 Управление экологическими рисками

6.9 Инвентаризация оборудования

6.10 Контроль за резервными носителями информации

6.11 Безопасность мобильных устройств

Приложение 1

1.????

Целью настоящей Процедуры Физической безопасности (далее – **Процедура**) в области защиты информации разработана с целью определения правил/процессов организации, средств контроля информационной безопасности в инфраструктуре информационных технологий SDU University (далее – **Университет**).

2.??????? ???????????

Настоящая Процедура в области физической безопасности охватывает следующие элементы:

- Серверное помещение, в которой размещены информационные системы или данные Университета
- Офисные помещения, занятые и находящиеся под контролем Университета;

- Информационные системы, принадлежащие и/или контролируемые Университета;
- Информационные системы, устанавливаемые в сетях Университета.

Если какая-либо часть настоящей Процедуры противоречит местным законодательным или нормативным требованиям, такие требования имеют преимущественную силу перед настоящей Процедурой. Все такие расхождения должны быть документированы.

Процедура носит обязательный характер и распространяется на всю информацию, хранящуюся в информационных системах Университета.

3.????????????? ?? ?????????? ?????????

Ответственным за надлежащее применение и соблюдение Процедуры является сотрудник, назначенный ответственным за физическую безопасность.

4. ???????????

Термины и определения, используемые в настоящей Процедуре толкуются в соответствии с терминами и определениями, использованными в Процедуре разработки, утверждения и обновления внутренних нормативных документов Университета.

Конфиденциальная информация – критичная информация, которая в случае разглашения неавторизованным лицами может нанести значительный ущерб

репутации Университета. Информация с таким уровнем классификации должна быть наиболее защищена от несанкционированного доступа или модификации;

Информационная система — система, предназначенная для хранения, поиска и обработки информации;

Сотрудник – штатный сотрудник Университета;

Серверное помещение – выделенное технологическое помещение со специально созданными и поддерживаемыми условиями для размещения и функционирования серверного и телекоммуникационного оборудования;

СКУД - Система контроля и управления доступом.

5.???????? ????????

5.1 Ответственность за физическую безопасность

Ответственность за физическую безопасность возлагается на заведующего Отдела информационно-технической поддержки (далее – **ОИТП**) согласно его должностной инструкции.

Согласно которой, работник несет ответственность за обеспечение документального оформления и реализацию всех процедур физической безопасности.

5.2 Доступ в Серверное помещение

Физический доступ в Серверное помещение должен контролироваться следующим образом:

- вход в Серверное помещение осуществляется при помощи специальной карты доступа СКУД. Программирование карт доступа сотрудников Университета, имеющих право доступа в Серверное помещение, осуществляется ИТ специалистом;

- запрещается держать дверь Серверного помещения открытой. В этих целях дверь в Серверное помещение оборудуется электронно-магнитным замком;

- предоставление доступа в Серверное помещение лиц осуществляющих хозяйственные (например, уборка или чистка), регламентные, ремонтные, сервисные работы осуществляется на основании представления ИТ специалиста и разрешения ректора Университета. Доступ данных лиц в Серверное помещение, осуществление каких-либо работ в Серверном помещении, производится при участии и при непосредственном контроле ИТ специалиста;

- записи о всех неуполномоченных посетителях, посещающих Серверное помещение, должны храниться не менее 12 месяцев в журнале регистрации доступа в Серверное помещение;

- при отсутствии дальнейшей необходимости, право доступа должно быть немедленно отменено;

- права доступа в Серверное помещение должны пересматриваться не реже одного раза в год для подтверждения их обоснованности.

5.3 Защита конфиденциальной информации в бумажном виде

Каждый сотрудник обеспечивается запираемым ящиком для хранения конфиденциальной информации в бумажном виде. Все ящики должны быть заперты.

Все сотрудники Университета несут ответственность за хранение конфиденциальной печатной информации в запираемых хранилищах (например, файловый шкаф, файловые комнаты, ящики и т.п.).

5.4 Защита конфиденциальной информации в электронном виде

Серверы, SAN (сети хранения данных) и другая ключевая ИТ-инфраструктура, на которых работают критически важные приложения / системы или размещена

конфиденциальная информация, должны находиться в защищенном месте, например, в Серверном помещении.

5.5 Стойки для серверного и сетевого оборудования

Стойки для серверного и сетевого оборудования в офисной среде должны быть заперты, а доступ к ним должен быть разрешен только специально уполномоченному персоналу.

5.6 Физическое расположение Серверного помещения

Серверное помещение должно быть физически отделено от офисных помещений полными стенами от пола до потолка и расположено вдали от наружных стен здания.

Необходимо провести оценку физического риска до принятия решения о переносе или строительстве Серверного помещения, включая местоположение объекта, потенциальные стихийные бедствия, наличие ключевых ресурсов и климат местоположения.

5.7 Периодическая проверка физической безопасности

Каждые 12 месяцев ИТ специалист обязан проводить периодическую проверку физической безопасности в Университете, в Серверном помещении для обеспечения надлежащего рабочего состояния контролей безопасности, таких как дверные замки, камеры и т.д.

• физический доступ к центру обработки данных или компьютерной комнате;

• защита от перехвата, прерывания или повреждения силовых и телекоммуникационных кабелей, которые несут данные или поддерживают информационные услуги;

• идентифицировать и документировать процессы и механизмы для обеспечения упорядоченного отключения вычислительных ресурсов в случае длительного сбоя питания в соответствии с требованиями бизнеса.

Данная проверка оформляется актом проверки физической безопасности, указанным в Приложении №1 настоящей Процедуры.

6.?????????? ???????????? ???????????? ? ????????? ??????????

6.1 Отслеживание электронных носителей

Для записи и отслеживания электронных носителей, таких как резервные ленты, USB-накопители и т.д., с момента первой записи до утилизации/замены, должен быть создан документированный процесс.

Каждый электронный носитель должен быть учтен, а его местонахождение постоянно обновляется. Это начинается с жестких дисков USB, внешних и внутренних жестких дисков, резервных лент и зарезервированных мест хранения на серверах в облаке.

Отслеживание действий с электронными носителями:

- Учет и отслеживание всех электронных носителей, например, резервных лент, USB-накопителей, внешних жестких дисков, внутренних жестких дисков и флэш-памяти путем инвентаризации активов.
- Утилизация электронных носителей происходит согласно процедуре обработки активов, используемой Университетом для отслеживания запросов на утилизацию, безопасного стирания, уничтожения носителей.
- Срок хранения записей о сроке службы резервных носителей и любые записи об уничтожении носителей составляет не менее 12 месяцев в виде электронной таблицы excel.
- Журнал отслеживания носителей ведется ответственным лицом. Журнал хранится в ДИТ.

6.2 Вынос ИТ-активов

ИТ-оборудование или программное обеспечение Университета, включая ноутбуки, планшеты и мобильные телефоны, запрещено выносить за пределы здания Университета без предварительного разрешения ректора Университета.

Разрешение регистрируется в журнале регистрации ИТ оборудования Университета, а журнал хранится не менее 12 месяцев в Управлении информационных технологий.

6.3 Защита сетевых кабелей

Все сетевые кабеля должны быть защищены от несанкционированного доступа, кабеля должны быть проложены в труднодоступных (закрытых) местах, таких как плинтуса, стены, потолки, кабель-каналы, и т.д.

Все силовые кабели должны быть отделены от кабелей сетевой связи для предотвращения помех.

Все кабели и оборудование должны быть четко промаркированы для минимизирования ошибок вследствие неправильного обращения.

6.4 ?????????? ???????????? ?????????? ?????????

Серверное помещение должно быть физически отделено от офисных помещений полными стенами от пола до потолка и расположено вдали от наружных стен здания. Серверное помещение не должно иметь окна в общественные помещения.

Ответственное лицо за информационную безопасность проводит оценку физического риска до принятия решения о переносе или строительстве Серверного помещения.

Серверное помещение не должно располагаться непосредственно под резервуарами с водой или водопроводными трубами и должны быть расположены выше уровня земли, если существует риск затопления.

6.5 Оценка рисков для Серверного помещения

Ответственное лицо за информационную безопасность обеспечивает проведение оценки рисков для физической безопасности Серверного помещения не реже одного раза в год.

Такая оценка риска может включать в том числе:

- проверку физического доступа в Серверное помещение;
- защиту от перехвата или повреждения кабелей питания, сетевых и телекоммуникационных кабелей, используемых для передачи данных или обслуживания информационных систем;

По результатам оценки риска Ответственное лицо за информационную безопасность формирует отчет, в котором указываются рекомендации. Данный отчет доводится до сведения руководства Университета. Ответственное лицо за информационную безопасность обеспечивает и контролирует реализацию одобренных мер по снижению риска физической безопасности.

6.6 Перебои в подаче электроэнергии

В случае длительного перебоя в подаче электроэнергии в здании Университета выполняются следующие действия:

- ИТ-специалист должен определить характер чрезвычайной ситуации (пожар, затопление, перегрев, сбой питания и т.д.) и оценить потенциальную угрозу для жизни. В случае опасности немедленно покинуть помещение.
- Если отсутствует прямая угроза, ИТ-специалист обязан остановить сервисы, виртуальные машины и базы данных, а затем выполнить корректное завершение работы серверов через удалённый интерфейс
- ИТ-специалист должен убедиться в наличии актуальных резервных копий и корректной работе механизмов репликации данных, если это возможно в

условиях ЧС.

- При необходимости специалист отключает маршрутизаторы, коммутаторы и иное активное сетевое оборудование для предотвращения дальнейших повреждений.
- ИТ-специалист должен обеспечить закрытие серверного помещения и при необходимости временно отключить систему доступа.
- По завершении аварийных действий специалист составляет отчёт, в котором фиксирует причину происшествия, время реагирования, принятые меры и список остановленного оборудования.
- После устранения последствий ЧС ИТ-специалист выполняет диагностику оборудования, поэтапный запуск систем и проверку целостности данных и журналов.

После подачи электроэнергии в здание Университета ИТ специалист проводит включение серверного оборудования.

ИТ специалист проверяет работоспособность всех систем.

6.7 Наблюдение за Серверным помещением

ИТ специалист должен контролировать физический доступ к Серверному помещению. Такой мониторинг может включать, в том числе:

- камеры / системы видеонаблюдения;
- двери, оборудованные системой СКУД;
- услуги охранников;
- просмотр отчета посещения СКУД;

Серверное помещение должно контролироваться 24 часа в сутки, 365 дней в году. При использовании камер / систем видеонаблюдения, записи с такого

оборудования должны храниться не менее 90 дней.

6.8 Управление экологическими рисками

ИТ специалист должен гарантировать, что инфраструктура и оборудование в Серверном помещении защищено от экологических рисков путем использования соответствующих средств контроля:

- системы отопления;
- системы вентиляции;
- системы кондиционирования воздуха;
- системы пожаротушения или ручным переносным углекислотным огнетушителем;
- системы бесперебойной подачи питания;
- резервное питание и охлаждение;
- датчики температуры и влажности, которые регулярно сообщают о состоянии окружающей среды внутри серверного помещения или центра хранения и обработки данных;

6.9 Инвентаризация оборудования

Бухгалтерия должна обеспечить наличие документированной процедуры для проведения инвентаризации всего оборудования информационных систем Университета, размещенного в Серверном помещении. Информационные системы Университета должны иметь четкую маркировку или обозначения для возможности их точной идентификации в качестве оборудования Университета.

Такое оборудование в числе прочего включает:

- серверы и рабочие станции;

- маршрутизаторы, коммутаторы, сетевые мосты и другое оборудование связи;
- беспроводные точки доступа (WAP);
- сети хранения данных (SAN);

6.10 Контроль за резервными носителями информации

ИТ специалист должен гарантировать наличие документально оформленной процедуры по регистрации и отслеживанию резервных носителей информации, например, резервные магнитные ленты, от первой записи до утилизации / замены.

Данная процедура должна предусматривать хранение документации, в которой указан срок службы резервных носителей. Записи об уничтожении носителя информации должны хранится в течение не менее 12 месяцев или другого периода времени в соответствии с политикой хранения данных Университета, в зависимости от того, какой срок больше.

6.11 Безопасность мобильных устройств

Неиспользуемые мобильные устройства, такие как ноутбуки, должны размещаться в защищенной зоне хранения, например, в запираемом шкафу или хранилище, либо запираться тросами с замком во избежание кражи.

Акт

проверки физической безопасности здания Университета

г.Алматы «___» _____
20_г.

Настоящий акт составлен по результатам проверки физической безопасности здания Университета, расположенного по адресу:

В результате проведенных действий
установлено:_____
_____

_____

_____
_____
_____

_____

Замечания, заявления, сделанные при осмотре:
_____

Проверку произвел:

_____ _____ _____

Должность, подразделение Подпись ФИО

Ознакомлен:

_____ _____ _____

Должность, подразделение Подпись ФИО