МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

ИНСТРУКЦИЯ ДГТУ ОД

Система менеджмента качества

УТВЕРЖДАЮ

Ректор

_____ Б.Ч. Месхи

«18» ноября 2024 г.

Введена в действие приказом ректора

от 18.11.2024 № 235

ИНСТРУКЦИЯ

Инструкция по обеспечению безопасности при возникновении нештатных ситуаций в информационных системах в федеральном государственном бюджетном образовательном учреждении высшего образования «Донской государственный технический университет»

Ростов-на-Дону
2024

1 Общие положения

1.1 Инструкция по действиям персонала в нештатных ситуациях в ДГТУ (далее именуемое – Университет) предназначена для определения порядка действий работников при возникновении нештатных ситуаций.

1.2 Цель создания данной инструкции – повысить безопасность защиты ПДн за счет организации эффективного информационного взаимодействия работников Университета, Ответственного за обеспечение безопасности конфиденциальной информации и руководителей подразделений Университета и упорядочение процессов передачи информации.

1.3 Нештатная ситуация – это событие, процессы или явление, влияющие на безопасность работы компьютерной сети, ПЭВМ, содержащих ПДн работников и студентов, а также сохранность бумажных, электронных и других носителей, содержащих базы ПДн.

1.4 Нештатными (кризисными) ситуациями являются:

а) Разглашение информации ограниченного доступа, не составляющей государственной тайны (далее – защищаемая информация), работниками Университета, имеющими к ней право доступа, в том числе:

– разглашение информации лицам, не имеющим права доступа к защищаемой информации;

– передача информации по открытым линиям связи;

– обработка информации на незащищенных технических средствах обработки информации;

– опубликование информации в открытой печати и других средствах массовой информации;

– передача носителя информации лицу, не имеющему права доступа к ней;

– публикация информации на ресурсах общего пользования «Интернет»;

– утрата носителя с информацией.

б) Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

– несанкционированное изменение информации;

– несанкционированное копирование информации;

– несанкционированное удаление информации.

в) Несанкционированный доступ к защищаемой информации:

– подключение технических средств к средствам и системам объекта информатизации;

– использование закладочных устройств;

– маскировка под зарегистрированного пользователя;

– использование дефектов программного обеспечения объекта информатизации (ОИ);

– использование программных закладок;

– применение программных вирусов;

– хищение носителя защищаемой информации;

– нарушение функционирования технических средств (ТС) обработки информации;

– блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

г) Дефекты, сбои, отказы, аварии ТС и систем ОИ.

д) Дефекты, сбои и отказы программного обеспечения ОИ.

е) Сбои, отказы и аварии систем обеспечения ОИ.

ж) Природные явления, стихийные бедствия:

– термические, климатические факторы (пожары, наводнения и т. д.);

– механические факторы (землетрясения и т. д.);

– электромагнитные факторы (грозовые разряды и т. д.).

1.5 В случае наличия нештатной ситуации порядок действий при которой не регламентирован настоящей инструкцией, Ответственным за обеспечение безопасности конфиденциальной информации вырабатывается конкретный план действий с учетом текущей ситуации.

1.6 Резервируемые в Университете информационные ресурсы и способы их резервирования представлены в Инструкции по резервному копированию защищаемой информации в информационных системах персональных данных ДГТУ.

1.7 План обеспечения непрерывной работы и восстановления информации при нештатных ситуациях определены в Приложении 1 к настоящей Инструкции.

1.8 Для эффективной реализации мероприятий по реагированию в случае нештатных ситуаций должны проводиться регулярные тренировки по различным нештатным ситуациям. По результатам тренировки в случае необходимости проводится уточнение настоящей Инструкции.

1.9 Все руководители подразделений и работники Университета, имеющие доступ к работе с ПДн, знакомятся с положениями и приложениями Инструкции под подпись.

1.10 Ознакомление с требованиями Инструкции работников Университета осуществляет Ответственный за обеспечение безопасности конфиденциальной информации в Университете под подпись с выдачей электронных или бумажных копий Инструкции непосредственно для повседневного использования в работе.

2 Классификация нештатных ситуаций

Нештатные ситуации классифицируются в соответствии с оценками, представленными в таблице 2.1.

Таблица 2.1. Оценки нештатных ситуаций

Нештатная ситуация		**Оценка ситуации (раздел Инструкции)**	**Раздел Инструкции (пункт)**
Разглашение защищаемой информации работниками, имеющими к ней право доступа			(3.2)
Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации	Несанкционированное копирование конфиденциальной информации	Обнаружился случившийся факт	(3.2)
		Производится в текущий момент	(3.3)
	Несанкционированное изменение конфиденциальной информации	Обнаружился случившийся факт	(3.2)
		Производится в текущий момент	(3.2)
	Несанкционированное удаление конфиденциальной информации	Обнаружился случившийся факт	(3.2)
		Производится в текущий момент	(3.2)
Несанкционированный доступ к	Подключение технических средств к средствам и	Обнаружился случившийся факт	(3.2)

Нештатная ситуация		**Оценка ситуации (раздел Инструкции)**	**Раздел Инструкции (пункт)**
защищаемой информации	системам объекта информатизации (ОИ)	Производится в текущий момент	(3.4)
	Установка закладочных устройств	Обнаружение установленных	(3.2)
		Устанавливаются в настоящий момент	(3.5)
	Маскировка под зарегистрированного пользователя	Внешним злоумышленником в текущий момент	(3.6)
		Внутренним злоумышленником либо производилась в прошлом	(3.2)
	Использование дефектов программного обеспечения ОИ	Внешним злоумышленником в текущий момент	(3.7)
		Внутренним злоумышленником либо производилось в прошлом	(3.2)
	Использование программных закладок	Внешним злоумышленником в текущий момент	(3.8)
		Внутренним злоумышленником либо производилось в прошлом	(3.3)
	Обнаружение программных вирусов		(3.9)
	Хищение носителя защищаемой информации		(3.2)
	Нарушение функционирования ТС обработки информации злоумышленником	Производится в текущий момент	(3.10)
		Обнаружился случившийся факт	(3.11)

Нештатная ситуация		**Оценка ситуации (раздел Инструкции)**	**Раздел Инструкции (пункт)**
	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку	Производится в текущий момент внешним злоумышленником	(3.12)
		Производится в текущий момент внутренним злоумышленником	(3.13)
		Обнаружился случившийся факт	(3.14)
Ошибки пользователей системы при эксплуатации программных средств, ТС, средств и систем защиты информации		Ошибка повлекла утерю или повреждение защищаемой информации	(3.15)
		Ошибка привела к нарушению работоспособности ТС и ПО	(3.16)
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ			(3.17)
Сбои, отказы и аварии систем обеспечения ОИ			(3.18)
Природные явления, стихийные бедствия	Несущие угрозу жизни человека		(3.19)
	Не несущие угрозу жизни человека		(3.20)

3 Порядок действий при обнаружении нештатных ситуаций

3.1 Порядок действий сотрудников при возникновении нештатной ситуации.

а) Общий порядок действий при обнаружении нештатных ситуаций:

– немедленно доложить Ответственному за организацию обработки персональных данных и Ответственному за обеспечение безопасности конфиденциальной информации в ДГТУ;

– при необходимости немедленно позвонить в соответствующие службы помощи, список аварийных служб представлен в Приложении 3;

– немедленно оповестить других работников и принять все меры для самостоятельной оперативной защиты помещения;

– ответственный за организацию обработки персональных данных в ДГТУ немедленно сообщает руководителю Университета и при необходимости организует проведение служебного расследования;

– ректор и ответственный за организацию обработки персональных данных в ДГТУ анализируют ситуацию и принимают соответствующие меры;

– ректор создаёт комиссию для расследования нештатной ситуации.

б) Порядок действий при возникновении стихийного бедствия - пожара, наводнения, землетрясения и т.д.

Работнику, обнаружившему пожар или другое стихийное бедствие, необходимо:

– немедленно позвонить в соответствующие службы помощи, список аварийных и спасательных служб представлен в Приложении 3;

– немедленно доложить Ответственному за организацию обработки персональных данных и Ответственному за обеспечение безопасности конфиденциальной информации в ДГТУ.

Ответственный за организацию обработки персональных данных в ДГТУ немедленно сообщает руководителю Университета.

Ректор анализирует ситуацию и принимает соответствующие меры.

– немедленно оповестить других работников;

– все работники обязаны принять меры для самостоятельной оперативной защиты информации, вычислительной техники, содержащей ПДн, собрать и упаковать личные реквизиты защиты и действовать согласно п. 3.19.

в) Порядок действий при обнаружении факта взлома и проникновения в помещение, а также кражи находящихся там технических средств, содержащих информацию о ПДн субъектов.

Работнику, обнаружившему факт кражи, раскрытия или модификации данных вследствие физического взлома или проникновения в помещение:

– немедленно доложить Ответственному за организацию обработки персональных данных и Ответственному за обеспечение безопасности конфиденциальной информации в ДГТУ;

– сохранять помещение в первоначальном виде и воспрепятствовать проходу остальных работников и возможному уничтожению улик в помещении.

– Ответственный за обеспечение безопасности конфиденциальной информации в Университете немедленно составляет акт

– анализирует ситуацию и при необходимости вызывает сотрудников аварийных служб;

– совместно с Ответственным за организацию обработки персональных данных в ДГТУ принимает соответствующие меры, при необходимости организуя проведение служебного расследования;

– Ответственный за организацию обработки персональных данных в ДГТУ сообщает руководителю Университета о выявленной нештатной ситуации, принятых мерах, дальнейших действиях и результатах расследования (если оно проводилось);

– ректор принимает соответствующие меры и создаёт комиссию для расследования нештатной ситуации.

г) Действия в случае выявления любых нештатных ситуаций, связанных с нарушением целостности ПЭВМ и системы защитных знаков (СЗЗ):

– пользователь технического средства, опечатанного СЗЗ, осуществляет ежедневную визуальную проверку наличия и целостности СЗЗ и в случае нарушения целостности немедленно докладывает своему непосредственному руководителю.

– в случае выявления любых нештатных ситуаций, связанных с нарушением целостности СЗЗ, пользователь уведомляет об этом Ответственного за обеспечение безопасности конфиденциальной информации;

– Ответственный за обеспечение безопасности конфиденциальной информации в Университете составляет акт и немедленно информирует Ответственного за организацию обработки персональных данных в ДГТУ, который:

– анализирует ситуацию;

– принимает соответствующие меры, при необходимости организуя проведение служебного расследования;

– сообщает руководителю Университета о выявленной нештатной ситуации, принятых мерах, дальнейших действиях и результатах расследования (если оно проводилось);

– Ректор принимает соответствующие меры и создаёт комиссию для расследования нештатной ситуации.

4 Нештатные ситуации, которые повлекли утечку или повреждение защищаемой информации либо созданы внутренним злоумышленником

При обнаружении нештатных ситуаций, которые повлекли утечку, повреждение или уничтожение защищаемой информации, либо созданы внутренним злоумышленником, создается комиссия по расследованию оценки всех причин возникновения внештатных ситуаций и действий всех работников, состав данной комиссии утверждается Руководителем Университета.

При нештатных ситуациях, связанных с:

– Разглашением конфиденциальной информации;

– Обнаружением несанкционированной, скопированной или измененной конфиденциальной информации;

– Обнаружением подключения технических средств к средствам и системам объекта информатизации;

– Обнаружением факта уничтожения информации;

– Обнаружением закладочных устройств;

– Маскировкой под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки в прошлом (как внутренним, так и внешним злоумышленником);

– Использованием дефектов программного обеспечения ОИ внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);

– Использованием программных закладок внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);

– Хищением носителя защищаемой информации.

Первоочередные действия:

– Ответственным за обеспечение безопасности конфиденциальной информации предпринимаются действия по сбору и обеспечению сохранности улик незаметно для злоумышленника.

Комиссия дополнительно к общему порядку действий (в соответствии с разделом 3.1.) должна:

– если это возможно, определить куда произошла утечка конфиденциальной информации;

– определить возможные контрмеры, призванные уменьшить потери от утечки информации.

5 Несанкционированное копирование, изменение или удаление конфиденциальной информации в текущий момент времени со стороны лиц, имеющих право доступа к ней

В случае обнаружения злоумышленника, неправомерно копирующего, изменяющего защищаемую информацию, выполняются следующие действия:

Первоочередные действия:

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете прерывает несанкционированный процесс.

2. Ответственный за обеспечение безопасности конфиденциальной информации в Университете блокирует доступ к ИС Университета для злоумышленника.

3. Ответственный за обеспечение безопасности конфиденциальной информации в Университете перекрывает физический доступ нарушителю к средствам ИС.

4. Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности конфиденциальной информации предпринимаются действия по сбору и обеспечению сохранности улик.

Последующие действия:

Руководителем Университета создается комиссия для расследования инцидента. Руководителем Университета назначается ответственное лицо, которое будет составлять протокол о ходе всего расследования.

При выявлении нарушений Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности ПДн, обрабатываемых с использованием средств автоматизации, и Ответственным за обеспечение безопасности ПДн, обрабатываемых без

использования средств автоматизации, вносятся предложения по устранению выявленных нарушений.

6 Подключение технических средств к средствам и системам ОИ в текущий момент времени

В случае обнаружения злоумышленника, производящего подключение к техническим средствам и системам ОИ в текущий момент времени, выполняются следующие действия:

Первоочередные действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете прерывает процесс работы нарушителя.

2. В случае если нарушитель – пользователь ИС, Ответственный за обеспечение безопасности конфиденциальной информации в Университете блокирует доступ в ИС Университета для нарушителя.

Последующие действия

Руководителем Университета создается комиссия для расследования инцидента. Руководителем Университета назначается ответственное лицо, которое будет составлять протокол о ходе всего расследования.

При выявлении нарушений Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности ПДн, обрабатываемых с использованием средств автоматизации, и Ответственным за обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, вносятся предложения по устранению выявленных нарушений.

7 Установка закладочных устройств злоумышленником в текущий момент времени

В случае обнаружения злоумышленника, устанавливающего закладочные устройства, выполняются следующие действия:

Первоочередные действия

Ответственный за обеспечение безопасности конфиденциальной информации в Университете принимает меры к задержанию злоумышленника.

Последующие действия

Руководителем Университета создается комиссия для расследования инцидента. Руководителем Университета назначается ответственное лицо, которое будет составлять протокол о ходе всего расследования.

При выявлении нарушений Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности ПДн, обрабатываемых с использованием средств автоматизации, и Ответственным за обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, вносятся предложения по устранению выявленных нарушений.

8 Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени

В случае обнаружения внешнего злоумышленника, маскирующегося под зарегистрированного пользователя, выполняются следующие действия:

Первоочередные действия

Ответственный за обеспечение безопасности конфиденциальной информации в Университете блокирует доступ к ИС Университета для злоумышленника.

Последующие действия

Руководителем Университета создается комиссия для расследования инцидента. Руководителем Университета назначается ответственное лицо, которое будет составлять протокол о ходе всего расследования. При выявлении нарушений Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности ПДн, обрабатываемых с использованием средств автоматизации, и Ответственным за обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, вносятся предложения по устранению выявленных нарушений.

9 Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени

В случае обнаружения использования дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени выполняются следующие действия:

Первоочередные действия

Ответственный за обеспечение безопасности конфиденциальной информации в Университете блокирует доступ из внешних сетей к оборудованию, на котором используется уязвимое ПО.

Последующие действия

Руководителем Университета создается комиссия для расследования инцидента. Руководителем Университета назначается ответственное лицо, которое будет составлять протокол о ходе всего расследования. При выявлении нарушений Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности ПДн, обрабатываемых с использованием средств автоматизации, и Ответственным за обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, вносятся предложения по устранению выявленных нарушений.

10 Использование программных закладок внешним нарушителем в текущий момент времени

В случае обнаружения использования программных закладок внешним нарушителем в текущий момент времени выполняются следующие действия:

Первоочередные действия

Ответственный за обеспечение безопасности конфиденциальной информации в Университете блокирует доступ из внешних сетей к оборудованию, на котором установлена программная закладка.

Последующие действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете определяет возможный ущерб, нанесенный программной закладкой.

2. Ответственный за обеспечение безопасности конфиденциальной информации в Университете проводит мероприятия по обнаружению внедренных программных закладок и их нейтрализации, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.

3. Составляет акт об инциденте.

11 Обнаружение программных вирусов

В случае обнаружения программных вирусов выполняются действия, предусмотренные Инструкцией по антивирусной защите.

12 Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником

В случае обнаружения злоумышленника, нарушающего функционирование ТС обработки информации в текущий момент времени, выполняются следующие действия:

Первоочередные действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете принимает меры по немедленному удалению злоумышленника от средств вычислительной техники.

2. В случае если злоумышленник является пользователем системы, Ответственный за обеспечение безопасности конфиденциальной информации в Университете блокирует доступ к ИС Организации для злоумышленника.

Последующие действия

3. В случае наличия повреждений Ответственный за обеспечение безопасности конфиденциальной информации в Университете определяет ущерб, нанесенный ТС и информации.

4. Ответственный за обеспечение безопасности конфиденциальной информации в Университете производит восстановление работоспособности системы.

5. Руководителем Университета создается комиссия для расследования инцидента. Руководителем Университета назначается ответственное лицо, которое будет составлять протокол о ходе всего расследования. При выявлении нарушений Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности ПДн, обрабатываемых с использованием средств автоматизации, и Ответственным за обеспечение

безопасности ПДн, обрабатываемых без использования средств автоматизации, вносятся предложения по устранению выявленных нарушений.

13 Обнаружение нарушения функционирования ТС обработки информации, произведенного злоумышленником

В случае обнаружения нарушений в функционировании ТС обработки информации выполняются следующие действия:

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете определяет возможный круг лиц, причастных к нарушению функционирования ТС, определяет объем повреждений техническим и информационным ресурсам.

2. Ответственный за обеспечение безопасности конфиденциальной информации в Университете производит восстановление работоспособности системы.

3. Руководителем Университета создается комиссия для расследования инцидента. Руководителем Университета назначается ответственное лицо, которое будет составлять протокол о ходе всего расследования. При выявлении нарушений Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности ПДн, обрабатываемых с использованием средств автоматизации, и Ответственным за обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, вносятся предложения по устранению выявленных нарушений.

14 Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени

В случае обнаружения внешней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия:

Первоочередные действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете выявляет источник ложных заявок.

2. Ответственный за обеспечение безопасности конфиденциальной информации в Университете вырабатывает решение по блокированию потока ложных заявок и реализует выбранное решение.

Последующие действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете уведомляет провайдера, от которого идут ложные заявки, планирует и организует мероприятия по предотвращению повторения и нейтрализации последствий инцидента.

2. Ответственный за обеспечение безопасности конфиденциальной информации в Университете составляет акт об инциденте.

15 Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени

В случае обнаружения внутренней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия:

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете выявляет источник ложных заявок и блокирует доступ к ИС Университета для злоумышленника.

2. Руководителем Университета создается комиссия для расследования инцидента. Руководителем Университета назначается ответственное лицо, которое будет составлять протокол о ходе всего расследования. При выявлении нарушений Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности ПДн, обрабатываемых с использованием средств автоматизации, и Ответственным за обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, вносятся предложения по устранению выявленных нарушений.

16 Блокировка доступа к защищаемой информации, произошедшая в прошлом

При обнаружении факта блокировки доступа к защищаемой информации, произошедшей в прошлом, выполняются следующие действия:

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете выявляет источник ложных заявок.

2. В случае, если злоумышленник является внешним, Ответственный за обеспечение безопасности конфиденциальной информации в Университете уведомляет провайдера, от которого идут ложные заявки. Планирует и организует мероприятия по предотвращению повторения и нейтрализации последствий инцидента.

3. В случае, если злоумышленник является внешним, Ответственный за обеспечение безопасности конфиденциальной информации в Университете составляет акт об инциденте.

4. Руководителем Университета создается комиссия для расследования инцидента. Руководителем Университета назначается ответственное лицо, которое будет составлять протокол о ходе всего расследования. При выявлении нарушений Ответственным за организацию обработки персональных данных в ДГТУ совместно с Ответственным за обеспечение безопасности ПДн, обрабатываемых с использованием средств автоматизации, и Ответственным за обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, вносятся предложения по устранению выявленных нарушений.

17 Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации, выполняются следующие действия:

Первоочередные действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете проводит анализ и идентификацию причин инцидента.

2. В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в Приложении 1 данной Инструкции.

3. Ответственный за обеспечение безопасности конфиденциальной информации в Университете определяет ущерб, нанесенный нештатной ситуацией.

4. Ответственный за обеспечение безопасности конфиденциальной информации в Университете проводит мероприятия по восстановлению работоспособности системы и информации.

Последующие действия

1. Аттестационной комиссией, назначаемой ректором Университета проводится проверка знаний сотрудника, виновного в инциденте, и в случае необходимости его обучение.

2. Ответственный за обеспечение безопасности конфиденциальной информации в Университете составляет акт об инциденте, в случае необходимости выносит предложение руководителю Университета о применении дисциплинарной меры в отношении нарушителя.

18 Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО, выполняются следующие действия:

Первоочередные действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете проводит анализ и идентификацию причин инцидента.

2. В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.

Последующие действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете определяет ущерб, нанесенный нештатной ситуацией, восстанавливает работоспособность системы.

2. Ответственный за обеспечение безопасности конфиденциальной информации в Университете составляет акт об инциденте, в случае необходимости выносит предложение руководителю Университета о применении дисциплинарной меры в отношении нарушителя.

3. Проводится проверка знаний сотрудника виновного в инциденте и в случае необходимости его обучение.

19 Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ

В случае возникновения дефектов, сбоев, отказов, аварий ТС и систем ОИ выполняются следующие действия:

Первоочередные действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете выявляет возможные причины проявления дестабилизирующих факторов.

2. В случае наличия злоумышленных действий выполняется порядок действий соответствующего раздела Инструкции.

Последующие действия

1. Ответственный за обеспечение безопасности конфиденциальной информации в Университете восстанавливает работоспособность систем.

2. В случае потери данных Ответственным за обеспечение безопасности конфиденциальной информации по возможности проводится восстановление их из резервных копий.

3. Ответственным за обеспечение безопасности конфиденциальной информации производится составление акта.

20 Сбои, отказы и аварии систем обеспечения ОИ

В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем выполняется следующая последовательность действий:

1. В случае если наблюдается продолжительное отключение электропитания, Ответственным за обеспечение безопасности конфиденциальной информации производится отключение серверов до момента истечения резервов системы бесперебойного питания.
2. Проректором по общим вопросам Мозговым А.В. организуется работы по максимально быстрому восстановлению систем обеспечения.
3. В случае потери защищаемых данных Ответственным за обеспечение безопасности конфиденциальной информации по возможности проводится восстановление их из резервных копий.
4. Ответственным за обеспечение безопасности конфиденциальной информации производится составление акта.

21 Природные явления, стихийные бедствия, несущие угрозу жизни человека

В случае проявления стихийных бедствий и природных явлений, которые несут угрозу жизни человека, выполняются следующие действия:

1. Все работники (руководители подразделений в том числе) обязаны личные реквизиты защиты (например: металлические и/или электронные ключи, карты-идентификаторы, ключевые дискеты, печати и пр.) собрать и упаковать в водонепроницаемый пакет (необходимыми средствами непосредственный руководитель обеспечивает заранее) и лично обеспечивать сохранность этого пакета во время эвакуации.
2. По «Списку имущества и(или) документов в личном пользовании работника, подлежащего эвакуации в первую очередь» (списки разрабатываются работниками заранее и постоянно хранятся на рабочем месте) произвести сбор, упаковку, опись (в двух экз. – 1 экз. в тару) документов и технических средств в водонепроницаемый пакет (необходимыми средствами непосредственный руководитель обеспечивает заранее). Упакованное имущество работник передает под подпись (на своем экз. описи) лицам, обеспечивающим доставку имущества на эвакопункт, иначе - лично сопровождает груз во время его транспортировки.

3. Работник вкладывает в вышеназванный пакет картонную табличку с указанием текущей даты, своих персональных данных (ФИО, наименование организации, номер служебного телефона) и содержащую опись содержимого пакета, заверенную собственноручной подписью.

Руководители обязаны собрать в помещениях подразделения и лично упаковать (и далее лично хранить, как свои) реквизиты защиты и документы тех сотрудников, которых на момент эвакуации нет на рабочем месте (болезнь, командировка, учеба, отпуск и т.д.), списки первой очереди составляются Руководителями подразделений, в них включаются наиболее необходимые материальные ценности.

Руководители обязаны:

– При подготовке к эвакуации проверить обеспеченность (а при отсутствии – обеспечить) работников подразделения и/или Ответственного за обеспечение безопасности конфиденциальной информации упаковочным материалом, списками документов, дел и имущества, подлежащих эвакуации в первую очередь.

– Перед выездом в эвакопункт – проконтролировать исполнение задач эвакуации, приняв соответствующие доклады от работников о готовности к эвакуации, провести выборочную проверку готовности (комплектности) документов, дел, имущества подразделения и/или ИС к эвакуации.

22 Природные явления, стихийные бедствия, не несущие угрозу жизни человека

В случае проявления стихийных бедствий и природных явлений, которые не несут угрозу жизни и/или человека, выполняются следующие действия:

1. Работники Университета выключают свои персональные компьютеры.

2. Ответственный за обеспечение безопасности конфиденциальной информации в Университете выключает серверы и сетевое оборудование.

3. Ответственный за обеспечение безопасности конфиденциальной информации в Университете принимает меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества. В первую очередь эвакуируется имущество по «Списку имущества и(или) документов в личном пользовании работника, подлежащего эвакуации в первую очередь».

4. В случае локальных пожаров и частичных затоплений проректором по общим вопросам Мозговым А.В. организуются работы по ликвидации нештатной ситуации и ее последствий.

23 Производство расследований

Для расследования опасных ситуаций в случаях, предусмотренных настоящей Инструкцией, может создаваться комиссия. В состав комиссии должны входить:

– Председатель (Ректор);

– Ответственный за организацию обработки персональных данных в ДГТУ;

– Ответственный за обеспечение безопасности конфиденциальной информации в Университете;

– Юрисконсульт;

– Р отдела кадров;

– другие лица по решению председателя комиссии.

Деятельность комиссии должна по возможности происходить в режиме строгой конфиденциальности.

В общем случае комиссия проводит:

– анализ и идентификацию причин инцидента, определение виновных;

– определение ущерба, нанесенного нештатной ситуацией;

– планирование мер для предотвращения повторения, нейтрализации последствий (если это возможно);

– анализ и сохранение доказательств, следов инцидента, улик и свидетельств;

– определение меры ответственности виновного;

– определение вида (размера) наказания виновного;

– взаимодействие при необходимости с правоохранительными органами.

При сохранении улик:

– если есть возможность Ответственный за обеспечение безопасности конфиденциальной информации в Университете производит резервное копирование системной и защищаемой информации технических средств, вовлеченных в инцидент, включая журналы событий (контрольные записи).

По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются поясняющие материалы (копии экрана, распечатки журнала событий, и др.).

По результатам расследования Ответственным за обеспечение безопасности конфиденциальной информации организуются мероприятия по реализации предложенных комиссией мер для предотвращения либо уменьшения вероятности проявления подобных инцидентов в дальнейшем.

При проведении расследований, кроме того, необходимо ответить на следующие вопросы:

- можно ли было предусмотреть нештатную ситуацию?
- вызвана ли она слабостью средств защиты и регистрации?
- это первая кризисная ситуация такого рода?
- достаточно ли имеющегося резерва?
- есть ли необходимость пересмотра системы защиты?
- есть ли необходимость пересмотра настоящей инструкции?

24 Ответственные за контроль выполнения инструкции

Ответственными за постоянный контроль выполнения требований данной Инструкции являются:

– Ответственный за обеспечение безопасности конфиденциальной информации в Университете в части задач, возложенных на него настоящей инструкцией.

– Ответственный за организацию обработки персональных данных в ДГТУ в части общего контроля информационной безопасности.

– Проректор по общим вопросам в части задач, возложенных на него настоящей инструкцией.

25 Порядок замещения ответственных лиц

В случае отсутствия кого-либо из ответственных лиц при нештатной ситуации (отпуск, болезнь и т.п.) производится их замещение в соответствии с последовательностями, определенными ниже. Ответственное лицо замещает следующий идущий по списку работник.

Ответственные за информационную безопасность ИС:

1. Ректор.

2. Ответственный за обеспечение безопасности конфиденциальной информации в Университете.

3. Ответственный за организацию обработки персональных данных в ДГТУ.

Ответственные за материально-техническое обеспечение:

1. Ректор.
2. Проректор по общим вопросам.
3. Руководители подразделений.

26 Порядок пересмотра инструкции

Инструкция подлежит полному пересмотру при изменении приоритетов угроз безопасности ИС Университета.

Инструкция подлежит частичному пересмотру в следующих случаях:

– при изменении местоположения, состава и объема информационных ресурсов, подлежащих резервному копированию;

– при определении такой необходимости комиссией по результатам расследования нештатной ситуации;

– в целях повышения эффективности мероприятий, определенных в настоящей инструкции;

– при изменении состава, обязанностей и полномочий должностных лиц Университета, которые задействованы в мероприятиях настоящей Инструкции.

Полный пересмотр данного документа проводится Ответственным за обеспечение безопасности конфиденциальной информации, ответственным за организацию обработки персональных данных в ДГТУ с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИС Университета.

Частичный пересмотр данного документа проводится Ответственным за обеспечение безопасности конфиденциальной информации. Частичный пересмотр должен проводиться регулярно, не реже одного раза в год.

Приложение 1

План обеспечения непрерывной работы и восстановления информации

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Неправомерные действия со стороны лиц, допущенных к защищаемой информации					
Разглашение защищаемой информации работниками, имеющими к ней право доступа		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Обнаружение несанкционированно скопированной или измененной конфиденциальной информации		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц, имеющих право доступа к ней		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Несанкционированный доступ к информации					

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Обнаружение подключения технических средств к средствам и системам объекта информатизации		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Подключение технических средств к средствам и системам ОИ в текущий момент времени		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Обнаружение закладочных устройств		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Установка закладочных устройств злоумышленником в текущий момент времени		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	5 минут в рабочее время (1 час в нерабочее)	

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Использование программных закладок внешним нарушителем в текущий момент времени		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Использование программных закладок внутренним злоумышленником или обнаружение факта использования		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Обнаружение программных вирусов		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента		12 часов

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Хищение носителя защищаемой информации		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
	Нарушена работа группы пользователей	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента		2 дня

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
	Нарушена работа группы пользователей	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента		1 день
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку					

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	7 дней

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Обнаружение произошедшего факта блокировки доступа к защищаемой информации		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день
Ошибки пользователей системы					

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации		Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов в нерабочее)	1 день

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете в первый рабочий день после инцидента	20 минут	2 дня

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
	Нарушена работа группы пользователей	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	20 минут	1 день
Объективные факторы					

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ	Сбой ТС и систем ОИ	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после инцидента	1 час	2 дня

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
	Отказ ТС и систем ОИ, затронувший работу группы пользователей	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
	Отказ ТС и систем ОИ, затронувший работу одного пользователя	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете в первый рабочий день после инцидента	1 час	2 дня

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
	Авария ТС и систем ОИ	Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за обеспечение безопасности конфиденциальной информации в Университете как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час	1 день

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Сбои, отказы и аварии систем обеспечения ОИ	Сбой систем обеспечения ОИ	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента		

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
	Отказ систем обеспечения ОИ, затронувший работу группы пользователей	Ответственному за материально-техническое обеспечение и Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение и Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента		1 день

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
	Отказ систем обеспечения ОИ, затронувший работу одного пользователя	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента		2 дня

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
	Авария систем обеспечения ОИ	Ответственному за материально-техническое обеспечение, Ответственному за обеспечение безопасности конфиденциальной информации в Университете сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение, Ответственному за обеспечение безопасности конфиденциальной информации в Университете можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Природные явления, стихийные бедствия, несущие угрозу жизни человека		Руководителю, заместителям руководителя, которые оповещают всех своих работников сразу после получения информации	Руководителю, заместителям руководителя, которые оповещают всех своих работников сразу после получения информации		30 минут

Тип кризисной ситуации	**Критерии кризисной ситуации**	**Кому и в какие сроки докладывается**		**Срок реализации первоочередных действий**	**Максимальное время для выполнения всех мероприятий**
		В рабочее время	**В нерабочее время**		
Природные явления, стихийные бедствия, не несущие угрозу жизни человека		Руководителю, заместителям руководителя, Ответственному за обеспечение безопасности конфиденциальной информации в Университете	Руководителю, заместителям руководителя, Ответственному за обеспечение безопасности конфиденциальной информации в Университете		30 минут

Приложение 2.

ЖУРНАЛ УЧЕТА НЕШТАТНЫХ СИТУАЦИЙ

№ п/п	Дата, ИСПДн, ПЭВМ, описание ситуации, выполненные работы	Подпись исполнителя	Подпись Ответственного за обеспечение безопасности конфиденциальной информации в Университете

Приложение 3

СПИСОК АВАРИЙНЫХ СЛУЖБ

№ п/п	Наименование службы	Краткое описание нештатной ситуации	Номер телефона

Лист регистрации изменений

№ изменения	**Номера измененных листов**	**Основание для внесения изменений (№ и наименование измененного документа**	**Изменения внес**	
			Фамилия, инициалы	**Подпись, дата внесения изменений**

Лист ознакомления

Должность	Фамилия, инициалы	Дата	Подпись