Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

ПРИКАЗ

г. Самара

№ 238-ОВ «10» апреля 2018 г.

Об утверждении положения о разрешительной системе доступа, порядка учета машинных носителей, правил внутреннего контроля, перечня мероприятий по контролю обеспечения безопасности информации, перечня программного обеспечения и компонентов, соглашения о неразглашении информации

Во исполнение приказа Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Приказываю:

1. Утвердить Положение о разрешительной системе допуска к ресурсам к абонентскому пункту автоматизированной системы «Единая федеральная межведомственная система учёта Контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» (далее – АП АС ГС «Контингент»).

2. Утвердить Порядок учета, хранения и уничтожения машинных носителей информации (Далее - МНИ) в информационных системах персональных данных (Далее – ИСПДн).

3. Утвердить Правила внутреннего контроля соответствия обработки защищаемой информации, в том числе персональных данных (Далее – ПДн), требованиям безопасности информации в ИСПДн.

4. Утвердить Перечень мероприятий по контролю обеспечения безопасности информации, в том числе ПДн в ИСПДн.

5. Утвердить Перечень программного обеспечения и (или) его компонентов, разрешенного к использованию на АП АС ГС «Контингент».

6. Утвердить Соглашение о неразглашении информации содержащей ПДн.

7. Лебедевой О.Н., начальнику управления кадров, довести приказ до сотрудников университета в части касающейся.

8. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. ректора Г.Р. Хасаев

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом и.о. ректора
ФГБОУ ВО «СГЭУ»
№ 238-ОД от «10» декабря 2018 г.

Положение
о разрешительной системе допуска к ресурсам АП АС ГС «Контингент»

Сокращения

В настоящем документе использованы следующие сокращения:

Администратор АП АС ГС «Контингент» – ответственный за функционирование АП АС ГС «Контингент».

Администратор безопасности АП АС ГС «Контингент» – ответственный за защиту информации в АП АС ГС «Контингент».

АП АС ГС «Контингент» – абонентский пункт автоматизированной системы «Единая федеральная межведомственная система учёта Контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам».

АРМ – автоматизированное рабочее место (рабочая станция).

ЗИ – защита информации.

ИСПДн – информационная система персональных данных.

Ответственный за ЗИ – ответственный за обеспечение безопасности персональных данных на АП АС ГС «Контингент».

ПДн – персональные данные.

ПО – программное обеспечение.

РФ – Российская Федерация.

СЗИ – средство защиты информации.

ТС – технические средства.

Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет».

ФЗ – Федеральный закон.

ФСТЭК – Федеральная служба по техническому и экспортному контролю.

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 г. N 152-ФЗ, приказом ФСТЭК России от 18 февраля 2013 г. № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", Постановлением Правительства Российской Федерации № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и руководящими документами по вопросам обеспечения защиты информации.

1.2. Разрешительная система допуска к ресурсам АП АС ГС «Контингент» представляет собой совокупность процедур оформления права субъектов на доступ к информационным ресурсам АП АС ГС «Контингент» и ответственных лиц, осуществляющих реализацию этих процедур.

1.3. Подлежащие защите информационные ресурсы АП АС ГС «Контингент» включаются в «Перечень информации ограниченного доступа, обрабатываемой на АП АС ГС «Контингент».

1.4. Объектами доступа являются:

– информационные ресурсы и технические средства АП АС ГС «Контингент»;

– технологическая информация системы защиты информации АП АС ГС «Контингент».

1.5. Субъектами доступа являются:

– уполномоченные сотрудники Университета;

– лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (обслуживание, установка, настройка ПО).

1.6. Субъекты доступа несут персональную ответственность за соблюдение ими установленного в Университете порядка обеспечения защиты информационных ресурсов.

1.7. Ответственными лицами, осуществляющими реализацию процедур оформления прав субъектов на доступ к информационным ресурсам АП АС ГС «Контингент» являются:

– Администратор безопасности АП АС ГС «Контингент»;

– Администратор АП АС ГС «Контингент».

2. Допуск к информационным ресурсам сотрудников Университета

2.1. Лица, доступ которым к защищаемой информации, обрабатываемой в АП АС ГС «Контингент», необходим для выполнения служебных (трудовых) обязанностей, допускаются к ним на основании списков, утверждаемых ректором Университета.

2.2. Допуск сотрудников к защищаемой информации, осуществляется в объеме, необходимом для выполнения ими должностных обязанностей. Права доступа сотрудников к защищаемой информации и выполняемые роли определяются в Матрице доступа (Приложение 1).

2.3. Администратором безопасности АП АС ГС «Контингент» проверяется соответствие требуемых прав доступа с реально необходимыми для выполнения должностных (функциональных) обязанностей данного сотрудника.

2.4. После определения роли пользователя и в соответствии с обозначенными для него правами в Матрице доступа Администратор безопасности АП АС ГС «Контингент» в соответствии с документацией на СЗИ производит необходимые действия по созданию (изменению, удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ресурсам ИСПДн, включению его в соответствующие группы пользователей и другие необходимые действия. Для всех пользователей АП АС ГС «Контингент» устанавливается режим принудительного запроса смены пароля не реже одного раза в 120 дней, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 30 минут.

2.5. В случае производственной необходимости пользователю АП АС ГС «Контингент» могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в АП АС ГС «Контингент» одного и того же имени пользователя ("группового имени") запрещается.

2.6. При изменении должностных обязанностей сотрудника, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя подлежит изменению (корректировке), при этом старые полномочия аннулируются.

2.7. После внесения изменений в Матрицу доступа Администратор безопасности АП АС ГС «Контингент» производит настройку (при их наличии) специализированных средств защиты АРМ.

2.8. Все изменения в правах доступа выполняются администраторами не позднее трех суток с момента получения заявки на внесение изменений.

2.9. Блокирование учетных записей на время отпуска пользователей АП АС ГС «Контингент» осуществляется Администратором безопасности АП АС ГС «Контингент».

2.10. Работнику, зарегистрированному в качестве нового пользователя системы, Администратором безопасности АП АС ГС «Контингент» присваивается идентификатор (учетная запись) и начальное значение пароля. При этом необходимо учитывать, что повторное использование идентификатора пользователя исключается в течение одного года.

3. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций организации

3.1. К организациям, деятельность которых не связана с исполнением функций организации, могут относиться:

- правоохранительные органы;
- судебные органы;
- органы статистики;
- органы исполнительной и законодательной власти субъектов РФ;

– средства массовой информации и пр.

3.2. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций организации, регламентируется законодательством Российской Федерации, договорами и соглашениями об информационном обмене и другими нормативными актами.

3.3. Доступ к информационным ресурсам АП АС ГС «Контингент» сторонних организаций осуществляется на основании письменных запросов.

В письменном запросе указывается:

– основание (с приведением ссылки на нормативный акт), в соответствии с которым предоставляется информация;

– для каких целей необходима информация;

– конкретное наименование предоставляемой информации и ее объем;

– способ доступа (предоставления).

3.4. Основанием для доступа (предоставления) информации служит резолюция ректора Университета на соответствующем документе (запросе).

3.5. Для доступа к информационным ресурсам АП АС ГС «Контингент» сотруднику сторонней организации должна быть заведена временная учетная запись на ограниченный срок, достаточный для проведения необходимых работ (настройки, тестирования или иных работ).

4. Допуск к информационным ресурсам организации сторонних организаций, выполняющих работы в организации на договорной основе

4.1. К организациям, выполняющим работы на договорной основе, могут относиться:

– организации, выполняющие строительные работы и осуществляющие ремонт зданий, систем инженерно-технического обеспечения (отопления, освещения, водоснабжения, канализации, электропитания, кондиционирования и т.п.);

– организации, осуществляющие монтаж и настройку технических средств АС, сопровождение прикладного ПО;

– организации, оказывающие услуги в области ЗИ (проведение специальных проверок и исследований, монтаж и настройка средств защиты информации,

контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);

– организации, осуществляющие поставку товаров для обеспечения повседневной деятельности (мебели, канцтоваров, оргтехники, расходных материалов и т.п.);

– организации и частные лица, оказывающие юридические услуги, услуги по информационно-техническому обеспечению, осуществляющие преподавательскую деятельность и т.п.

4.2. Порядок допуска определяется в договоре на выполнение работ (оказание услуг).

4.3. Решением о допуске является подписанный в установленном порядке договор на выполнение работ или оказание услуг.

4.4. Для доступа к информационным ресурсам АП АС ГС «Контингент» сотруднику сторонней организации должна быть заведена временная учетная запись на ограниченный срок, достаточный для проведения необходимых работ (настройки, тестирования или иных работ).

4.5. Лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) также относятся к категории внутренних пользователей ИСПДн и им должны быть присвоены учетные записи в соответствии с правилами, определенными организационно-распорядительными документами по защите информации.

4.6. В договор на оказание услуг в обязательном порядке включается условие о неразглашении сведений, составляющих персональные данные, а также служебной информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений. Со всех работников сторонней организации, участвующих в выполнении работ, в этом случае берется подписка о неразглашении таких сведений.

5. Контроль функционирования разрешительной системы допуска к информационным ресурсам организации

5.1. Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

– планом основных мероприятий по защите информации на текущий год;

– функциональными обязанностями должностных лиц;

– приказами ректора Университета.

5.2. Контроль функционирования разрешительной системы допуска к информационным ресурсам АП АС ГС «Контингент» осуществляется ответственными лицами не реже одного раза в три месяца. Организация контроля возлагается на Администратора безопасности АП АС ГС «Контингент».

Приложение 1
к Положению о разрешительной системе допуска к ресурсам АП АС ГС «Контингент»

Матрица доступа к информационным ресурсам АП АС ГС «Контингент» (Форма)

N п/п	Фамилия, имя, отчество сотрудника (учетная запись)	Должность сотрудника	Уровень полномочий (роль)	Вид выполняемых функций	Наименование (тип) ресурса	Место хранения, размещения защищаемого ресурса	Права (тип) доступа к защищаемым ресурсам	Примечание
1	2	3	4	5	6	7	8	9
Администраторы								
1	Мишуров Дмитрий Александрович (admin)	Ведущий инженер отдела административной поддержки управления информационных систем и технологий	Администратор безопасности АП АС ГС «Контингент»	Администрирование и настройка средств защиты информации,	Windows 10 Pro	C:\Windows	Полный доступ	
					Microsoft Office стандартный 2003	C:\ProgramFiles\Microsoft Office	Полный доступ	
					Adobe Reader XI	C:\ProgramFiles\Adobe	Полный доступ	
					Mozilla Firefox 51.0	C:\ProgramFiles\Mozilla	Полный доступ	
					«Dr.Web Enterprise Security Suite 10»	C:\ProgramFiles\DrWeb	Полный доступ	
					ПО ViPNet Client 4.x (КС2)	C:\ProgramFiles\InfoteCS\	Полный доступ	
					Dallas Lock 8.0-K	C:\ProgramFiles\Dallas Lock	Полный доступ	
2	Черемисин Александр Александрович (CheremisinA.A)	Начальник отдела информационной безопасности	Ответственный за ЗИ	Администрирование и настройка средств защиты информации,	Windows 10 Pro	C:\Windows	Полный доступ	
					Microsoft Office стандартный 2003	C:\ProgramFiles\Microsoft Office	Полный доступ	
					Adobe Reader XI	C:\ProgramFiles	Полный	

N п/п	Фамилия, имя, отчество сотрудника (учетная запись)	Должность сотрудника	Уровень полномочий (роль)	Вид выполняемых функций	Наименование (тип) ресурса	Место хранения, размещения защищаемого ресурса	Права (тип) доступа к защищаемым ресурсам	Примечание
1	2	3	4	5	6	7	8	9
						\Adobe	доступ	
					Mozilla Firefox 51.0	C:\ProgramFiles \Mozilla	Полный доступ	
					«Dr.Web Enterprise Security Suite 10»	C:\ProgramFiles \DrWeb	Полный доступ	
					ПО ViPNet Client 4.x (КС2)	C:\ProgramFiles \InfoteCS\	Полный доступ	
					Dallas Lock 8.0-K	C:\ProgramFiles \Dallas Lock	Полный доступ	
3	Горбатов Сергей Васильевич (GorbatovS.V)	Начальник управления информационных систем и технологий	Администратор АП АС ГС «Контингент»	Администрирование и конфигурирование ПО и ТС АП АС ГС «Контингент»	Windows 10 Pro	C:\Windows	Полный доступ	
					Microsoft Office стандартный 2003	C:\ProgramFiles \Microsoft Office	Полный доступ	
					Adobe Reader XI	C:\ProgramFiles \Adobe	Полный доступ	
					Mozilla Firefox 51.0	C:\ProgramFiles \Mozilla	Полный доступ	
					«Dr.Web Enterprise Security Suite 10»	C:\ProgramFiles \DrWeb	Выполнение	
					ПО ViPNet Client 4.x (КС2)	C:\ProgramFiles \InfoteCS\	Выполнение	
					Dallas Lock 8.0-K	C:\ProgramFiles \Dallas Lock	Выполнение	
Пользователи								
4	Лебедева Ольга Николаевна	Начальник управления кадров	Пользователь	Внесение сведений в АС ГС	Windows 10 Pro	C:\Windows	Выполнение	
					Microsoft Office стандартный 2003	C:\ProgramFiles \Microsoft	Выполнение	

N п/п	Фамилия, имя, отчество сотрудника (учетная запись)	Должность сотрудника	Уровень полномочий (роль)	Вид выполняемых функций	Наименование (тип) ресурса	Место хранения, размещения защищаемого ресурса	Права (тип) доступа к защищаемым ресурсам	Примечание
1	2	3	4	5	6	7	8	9
	(LebedevaO.N)			«Контингент»		Office		
					Adobe Reader XI	C:\ProgramFiles \Adobe	Выполнение	
					Mozilla Firefox 51.0	C:\ProgramFiles \Mozilla	Выполнение	
					«Dr.Web Enterprise Security Suite 10»	C:\ProgramFiles \DrWeb	Выполнение	
					ПО ViPNet Client 4.x (КС2)	C:\ProgramFiles \InfoteCS\	Выполнение	
					Dallas Lock 8.0-K	C:\ProgramFiles \Dallas Lock	Выполнение	
5	Кондрова Наталья Ивановна (KondrovaN.I)	Начальник студенческого отдела управления кадров	Пользователь	Внесение сведений в АС ГС «Контингент»	Windows 10 Pro	C:\Windows	Выполнение	
					Microsoft Office стандартный 2003	C:\ProgramFiles \Microsoft Office	Выполнение	
					Adobe Reader XI	C:\ProgramFiles \Adobe	Выполнение	
					Mozilla Firefox 51.0	C:\ProgramFiles \Mozilla	Выполнение	
					«Dr.Web Enterprise Security Suite 10»	C:\ProgramFiles \DrWeb	Выполнение	
					ПО ViPNet Client 4.x (КС2)	C:\ProgramFiles \InfoteCS\	Выполнение	
					Dallas Lock 8.0-K	C:\ProgramFiles \Dallas Lock	Выполнение	
6	Хохлова Татьяна	Ведущий специалист по кадрам	Пользователь	Внесение сведений в АС ГС	Windows 10 Pro	C:\Windows	Выполнение	
					Microsoft Office стандартный 2003	C:\ProgramFiles \Microsoft	Выполнение	

N п/п	Фамилия, имя, отчество сотрудника (учетная запись)	Должность сотрудника	Уровень полномочий (роль)	Вид выполняемых функций	Наименование (тип) ресурса	Место хранения, размещения защищаемого ресурса	Права (тип) доступа к защищаемым ресурсам	Примечание
1	2	3	4	5	6	7	8	9
	Анатольевна (KhokhlovaT.A)	студенческого отдела управления кадров		«Контингент»		Office		
					Adobe Reader XI	C:\ProgramFiles \Adobe	Выполнение	
					Mozilla Firefox 51.0	C:\ProgramFiles \Mozilla	Выполнение	
					«Dr.Web Enterprise Security Suite 10»	C:\ProgramFiles \DrWeb	Выполнение	
					ПО ViPNet Client 4.x (КС2)	C:\ProgramFiles \InfoteCS\	Выполнение	
					Dallas Lock 8.0-K	C:\ProgramFiles \Dallas Lock	Выполнение	
7	Кузьмина Анастасия Валентиновна (KuzminaA.V)	специалист по учебно-методической работе отдела по организации учебного процесса учебно-методического управления	Пользователь	Внесение сведений в АС ГС «Контингент»	Windows 10 Pro	C:\Windows	Выполнение	
					Microsoft Office стандартный 2003	C:\ProgramFiles \Microsoft Office	Выполнение	
					Adobe Reader XI	C:\ProgramFiles \Adobe	Выполнение	
					Mozilla Firefox 51.0	C:\ProgramFiles \Mozilla	Выполнение	
					«Dr.Web Enterprise Security Suite 10»	C:\ProgramFiles \DrWeb	Выполнение	
					ПО ViPNet Client 4.x (КС2)	C:\ProgramFiles \InfoteCS\	Выполнение	
					Dallas Lock 8.0-K	C:\ProgramFiles \Dallas Lock	Выполнение	

Лист ознакомления
с Положением о разрешительной системе допуска к ресурсам
АП АС ГС «Контингент»
(утверждено приказом №238-ОВ от «10» апреля 2018 г.)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата
1.	Лебедева Ольга Николаевна	начальник УК	11.04.18г.
2.	Черепанов Александр Аркадьевич	Начальник ОИБ	12.04.18
3	Хохлова Екатерина Анатольевна	Вед. спец. гр. отд. кад.	12.04.18
4	Курьмина Анастасия Валентиновна	Специалист по УМР	12.04.18
5	Шишов Дмитрий Александр	Ведущий спец.	12.04.18
6	Ершов Сергей Васильев	Начальник Упр	12.04.18
7	Кондрова Наталья Ивановна	нач. сект. отдела	12.04.18

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом и.о. ректора
ФГБОУ ВО «СГЭУ»
№ 238-В от «10» апреля 2018 г.

Порядок
учета, хранения и уничтожения МНИ в ИСПДн.

Сокращения

В настоящем документе использованы следующие сокращения:

Администратор безопасности ИСПДн – ответственный за защиту информации в ИСПДн.

ИСПДн – информационная система персональных данных.

НСД – несанкционированный доступ (несанкционированные действия).

ОС – операционная система.

ПО – программное обеспечение.

СЗИ – средство защиты информации.

МНИ – машинные носители информации.

Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет».

1. Общие положения

1.1. Настоящий документ устанавливает организацию в Университете учета, хранения и уничтожения МНИ в ИСПДн.

2. Требования по обеспечению безопасности при использовании МНИ

2.1. При обращении с МНИ выполняются следующие основные правила:

– находящиеся на хранении и в обращении МНИ подлежат учёту;

– раздельному учету в журналах учета подлежат съемные носители (в том числе портативные) перезаписываемые МНИ (флэш-накопители, съемные жесткие диски);

– пользователи для работы в ИСПДн могут использовать только учтенные МНИ;

– МНИ, срок эксплуатации которых истек, уничтожаются в установленном порядке;

– все съемные носители информации хранятся в безопасном месте в соответствии с требованиями по их эксплуатации.

Ответственным за хранение, учет и выдачу съемных носителей информации является Администратор безопасности ИСПДн.

2.2. Порядок учета МНИ

Все находящиеся на хранении и в обращении МНИ учитываются в Журнале учета МНИ (форма Журнала в Приложении 1) и Журнале учета съемных МНИ (форма Журнала в Приложении 2).

Каждый МНИ должен иметь этикетку, на которой указывается его уникальный учетный номер. В качестве регистрационных номеров допускается использовать идентификационные (серийные) номера МНИ, присвоенные производителем этих МНИ, номера инвентарного учета, в т.ч. инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

Учет и выдачу МНИ осуществляет Администратор безопасности ИСПДн. Факт выдачи и получения МНИ конкретным сотрудником фиксируется в Журнале учета МНИ.

Учет встроенных в портативные или стационарные технические средства МНИ может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных МНИ, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

После окончания работ пользователь ИСПДн сдает съемный носитель Администратору безопасности ИСПДн, о чем делается соответствующая запись в

Журнале учета МНИ. При наличии личного сейфа у пользователя автоматизированной системы допускается хранение учтенных МНИ в личных сейфах, в противном случае, все МНИ должны храниться в сейфе у Администратора безопасности ИСПДн.

В случае передачи МНИ между пользователями должно обеспечиваться уничтожение (стирание) информации на МНИ при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

Уничтожение (стирание) информации на МНИ должно исключать возможность восстановления защищаемой информации при передаче МНИ между пользователями, в сторонние организации для ремонта или утилизации.

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных МНИ.

В ИСПДн должны применяться следующие меры по уничтожению (стиранию) информации на МНИ, исключающие возможность восстановления защищаемой информации:

– удаление файлов штатными средствами операционной системы и (или) форматирование МНИ штатными средствами ОС;

– перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

– Сотрудникам запрещается подключать к ИСПДн неучтенные МНИ и информационно-телекоммуникационные средства.

2.3. Порядок уничтожения МНИ

МНИ, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

Уничтожение МНИ осуществляется комиссией по уничтожению, назначенной ректором Университета. Форма приказа о назначении комиссии по уничтожению МНИ представлена в Приложении 3.

Уничтожение магнитных, оптических, магнитооптических и электронных носителей информации производится путем их физического разрушения. Перед уничтожением носителя информация с него стирается (уничтожается), если это позволяют физические принципы работы носителя.

Перед утилизацией оборудования, участвующего в обработке информации, Администратором безопасности ИСПДн осуществляется проверка всех его компонентов, включая носители информации (жесткие диски) на отсутствие информации и лицензированного программного обеспечения.

По результатам уничтожения комиссией составляется Акт уничтожения МНИ (Приложение 4), который хранится в помещении для хранения носителей информации, уничтоженные МНИ (утилизированное оборудование) снимаются с материального учета.

Приложение 1
к Порядку обращения, хранения и уничтожения МНИ в ИСПДн

Журнал учета МНИ в ИСПДн
(Форма)

Начат «____» _____ 20__ г.

Окончен «____» _____ 20__ г.

На _____листах

_____ _____/_____/
Должность ответственного за ведение и хранение журнала Подпись Расшифровка

№ п/п	Регистрационный номер	Дата учета	Тип/емкость носителя	Серийный номер	Отметка о постановке на учет (ФИО, подпись, дата)	Отметка о снятии с учета (ФИО, подпись, дата)	Местоположение носителя	Сведения об уничтожении носителя /стирании информации

Приложение 2
к Порядку учета, хранения и уничтожения МНИ в ИСПДн

Журнал учета съемных МНИ в ИСПДн

(Форма)

Начат «____» _____ 20__ г.

Окончен «____» _____ 20__ г.

На _____листах

В _____ _____
должность и Ф.И.О. ответственного за ведение и хранение журнала Подпись

№ п/п	Регистрационный номер	Дата учета	Тип/емкость носителя	Серийный номер	Кому выдан (ФИО, должность, наименование группы пользователей)	Отметка о выдаче (ФИО, подпись, дата)	Отметка о получении (ФИО, подпись, дата)	Местоположение носителя (№ кабинета)	Отметка об обратном приеме (ФИО, подпись, дата)	Сведения об уничтожении носителя /стирании информации (№ и дата акта)
1	2	3	4	5	6	7	8	9	10	11

Приложение 3
к Порядку обращения, хранения и уничтожения МНИ в ИСПДн

ПРИКАЗ

_____ «___»_____20__ г.

о назначении комиссии по уничтожению МНИ
(Форма)

Для уничтожения МНИ

ПРИКАЗЫВАЮ:

1. Назначить комиссию в составе:

Председатель комиссии:

_____
(Фамилия, инициалы) *(Занимаемая должность)*

Члены комиссии:

_____
(Фамилия, инициалы) *(Занимаемая должность)*

_____
(Фамилия, инициалы) *(Занимаемая должность)*

2. По результатам работ предоставить для утверждения акт об уничтожении машинных носителей ПДн;

3. Контроль за исполнением настоящего Приказа возложить на

_____
(Фамилия, инициалы) *(Занимаемая должность)*

И.о. ректора /Г.Р. Хасаев/

Приложение 4
к Порядку учета, хранения и уничтожения МНИ в ИСПДн

Акт
об уничтожении информации
(Форма)

Комиссия, наделенная полномочиями приказом ректора Университета от _____ № _____, в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор МНИ и установила, что информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя	Примечание

Всего носителей _____
(цифрами и прописью)

На указанных носителях информация уничтожена путем _____.

(стирания информации на устройстве средством гарантированного уничтожения в составе СЗИ от НСД Dallas Lock 8.0 и т.п.)

Перечисленные носители уничтожены путем _____
_____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель комиссии: _____ / /
Члены комиссии: _____ / /
_____ / /

Лист ознакомления
с Порядком учета, хранения и уничтожения МНИ в ИСПДн
(утверждена приказом № 238 ОВ от «10» апреля 2018 г.)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата
1	Лебедева Ольга Николаевна	Юрисконсульт УК	11.04.18
2	Чуракин Александр Александрович	Начальник ОИБ	12.04.18
3	Хохлова Анастасия Анатольевна	Вед. спец. студ. отд. кор.	12.04.18
4	Кухтина Анастасия Валентиновна	Специалист по УМР	12.04.18
5	Шишуров Дмитрий Александр.	Вед. инженер	12.04.18
6	Горбов Сергей Васильев	Нач. упр	12.04.18
7	Кондрова Наталья Ивановна	нач. сектор отдела	12.04.18

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом и.о. ректора
ФГБОУ ВО «СГЭУ»
№ 231-ОВ от «10» декабря 2018 г.

Правила
внутреннего контроля соответствия обработки защищаемой информации, в том числе ПДн, требованиям безопасности информации в ИСПДн

Сокращения

В настоящем документе использованы следующие сокращения:

Администратор ИСПДн – ответственный за функционирование ИСПДн.

Администратор безопасности ИСПДн – ответственный за защиту информации в ИСПДн.

ЗИ – защита информации.

ИСПДн – информационная система персональных данных.

Ответственный за ЗИ – ответственный за обеспечение безопасности персональных данных в ИСПДн.

ПДн – персональные данные.

Правила внутреннего контроля – Правила внутреннего контроля соответствия обработки защищаемой информации, в том числе ПДн, требованиям безопасности информации в ИСПДн.

СЗИ – средство защиты информации

Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет».

1. Общие положения

Настоящими Правилами внутреннего контроля определяются процедуры, направленные на выявление и предотвращение нарушений установленных требований по защите информации в ИСПДн.

Настоящие Правилами внутреннего контроля определяют порядок внутреннего контроля соответствия обработки защищаемой информации, в том числе ПДн, требованиям безопасности информации в ИСПДн и действуют постоянно.

2. Требования к организации внутреннего контроля

В целях осуществления внутреннего контроля обеспечения безопасности информации в ИСПДн организуется проведение периодических проверок условий обработки защищаемой информации.

2.1. Проверка включает в себя:

– контроль реализации правил разграничения доступа, полномочий пользователей в ИСПДн;

– контроль соблюдения пользователями ИСПДн правил организации парольной защиты;

– контроль соблюдения пользователями ИСПДн установленных правил антивирусной защиты;

– контроль соблюдения установленных в ИСПДн правил работы с машинными носителями информации;

– контроль соблюдения порядка доступа в помещения, где расположены элементы ИСПДн и ведется обработка защищаемой информации;

– контроль соблюдения порядка резервирования информации и хранения резервных копий;

– контроль соблюдения порядка работы со средствами защиты информации;

– контроль знания и соблюдения пользователями ИСПДн внутренних документов по ЗИ.

2.2. Проверки осуществляются Ответственным за ЗИ совместно с Администратором безопасности ИСПДн и Администратором ИСПДн (Далее – Комиссия).

2.3. Проверки проводятся на основании утвержденного ректором Университета «Перечня мероприятий по контролю за обеспечением безопасности информации, в том числе ПДн в ИСПДн».

2.4. При проведении проверки обеспечения безопасности информации в ИСПДн установленным требованиям должны быть полностью объективно и всесторонне установлены:

– порядок и условия применения организационных и технических мер по защите информации, исполнение которых обеспечивает установленный уровень защищенности ПДн в ИСПДн;

– соответствие состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, представленному в техническом паспорте ИСПДн;

– порядок и условия применения СЗИ;

– порядок и условия допуска лиц в помещения, где размещены средства ИСПДн;

– порядок организации и правильности учета МНИ;

– соблюдение установленных правил доступа субъектов доступа к объектам доступа;

– соблюдение установленного порядка использования мобильных технических средств;

– наличие (отсутствие) фактов несанкционированного доступа к информации и принятие необходимых мер;

– соблюдение установленных правил организации парольной и антивирусной защиты;

– знание персоналом базы нормативно-методических документов по защите информации.

2.5. При проведении внутренней проверки комиссия имеет право:

– запрашивать у сотрудников Университета, допущенных к работе в ИСПДн, информацию, необходимую для реализации полномочий;

– принимать меры по приостановлению или прекращению обработки защищаемой информации, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить ректору Университета предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности информации;

– вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в области защиты информации.

2.6. Мероприятия, проведенные в ходе внутреннего контроля, должны быть занесены в Журнал учета мероприятий по контролю за обеспечением защиты информации в ИСПДн (Приложение 1).

2.7. В отношении информации, ставшей известной комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

2.8. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений составляется протокол (Приложение 2), который должен быть представлен ректору Университета для ознакомления.

Приложение 1
к Правилам внутреннего контроля

Журнал учета мероприятий по контролю за обеспечением защиты информации в ИСПДн
(форма)

Начат «____» _____ 20__ г.

Окончен «____» _____ 20__ г.

На _____листах

_____ _____
должность и Ф.И.О. ответственного за ведение и хранение журнала Подпись

№ п/п	Мероприятие	Дата	Исполнитель	Результат

Приложение 2
к Правилам внутреннего контроля

П Р О Т О К О Л
результатов проведения внутренней проверки обеспечения безопасности информации в ИСПДн

Настоящий Протокол составлен в том, что «___» _____ 201_ года комиссией в составе: ответственного за защиту информации/администратора ИСПДн /администратора безопасности ИСПДн была проведена плановая внутренняя проверка обеспечения безопасности информации в ИСПДн.

Проверка осуществлялась в соответствии с требованиями _____

название внутреннего локального акта

В ходе проверки проверено:

_____

_____

Выявленные нарушения:

_____

_____

Меры по устранению нарушений:

_____

_____

Срок устранения нарушений: _____.

Проверку провели:

Ответственный за ЗИ подпись, ФИО

Администратор ИСПДн подпись, ФИО

Администратор безопасности ИСПДн подпись, ФИО

С результатами проверки ознакомлен:

Должность подпись, ФИО

«___» _____ 20__ года

Лист ознакомления
с Правилами внутреннего контроля
(утверждены приказом №938 ОВ от «10» апреля 2018 г.)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата
1	Лебедева Елена Николаевна	Начальник УК	ЛЕВ 11.04.18
2	Черешнев Александр Александрович	Начальник ОИБ	12.04.18
3	Хохлова Наталья Анатольевна	Вед. спец. студ. от. к.	12.04.18
4	Курьянова Анастасия Валентиновна	Специалист по УМР	12.04.18
5.	Шишов Дмитрий Александр.	Вед. инженер-[illegible]	12.04.18
6	Горбунов Сергей Васильевич	Нач. упр	12.04.2018
7	Кондрова Наталья Ивановна	нач. сект. отдела	12.04.18

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом и.о. ректора
ФГБОУ ВО «СГЭУ»
№2308 от «10» апреля 2018 г.

Перечень
мероприятий по контролю обеспечения безопасности информации, в том числе ПДн в ИСПДн

Сокращения

В настоящем документе использованы следующие сокращения:

Администратор АП АС ГС «Контингент» – ответственный за функционирование АП АС ГС «Контингент».

Администратор безопасности АП АС ГС «Контингент» – ответственный за защиту информации в АП АС ГС «Контингент».

АП АС ГС «Контингент» – абонентский пункт автоматизированной системы «Единая федеральная межведомственная система учёта Контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам».

ИСПДн – информационная система персональных данных.

МНИ – машинный носитель информации.

Ответственный за ЗИ – ответственный за обеспечение безопасности персональных данных в АП АС ГС «Контингент».

ПДн – персональные данные.

ПО – программное обеспечение.

СВТ – средство вычислительной техники.

СЗИ – средства защиты информации.

ТС – технические средства.

Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет».

Перечень мероприятий по контролю обеспечения безопасности информации, в том числе ПДн в ИСПДн на АП АС ГС «Контингент» Университета

Мероприятие	Периодичность	Исполнитель
Проверка соответствия состава и структуры программно-технических средств АП АС ГС «Контингент» документированному составу и структуре средств, представленному в техническом паспорте АП АС ГС «Контингент»	1 раз в 6 месяцев	*Администратор безопасности АП АС ГС «Контингент», Ответственный за ЗИ*
Проверка выполнения требований по условиям расположения СВТ в помещениях, в которых размещены элементы АП АС ГС «Контингент»	1 раз в 6 месяцев	*Администратор безопасности АП АС ГС «Контингент», Ответственный за ЗИ*
Проверка целостности опечатывания системных блоков и других ТС, участвующих в обработке информации	1 раз в 6 месяцев	*Администратор безопасности АП АС ГС «Контингент»*
Проверка организации допуска лиц в помещения, где размещены средства АП АС ГС «Контингент», в том числе перечня лиц, имеющих право доступа в помещения АП АС ГС «Контингент»	1 раз в 3 месяца	*Администратор безопасности АП АС ГС «Контингент», Ответственный за ЗИ*
Проверка актуальности перечня лиц, допущенных к работе в АП АС ГС «Контингент»	1 раз в 3 месяца	*Ответственный за ЗИ, Администратор безопасности АП АС ГС «Контингент»*
Проверка соответствия реального уровня полномочий по доступу к информации различных пользователей, установленному в матрице доступа	1 раз в 3 месяца	*Администратор безопасности АП АС ГС «Контингент»*
Проверка организации учета СЗИ, используемых в АП АС ГС «Контингент»	1 раз в 6 месяцев	*Ответственный за ЗИ*
Проверка наличия документов, подтверждающих возможность применения технических и программных СЗИ (сертификатов	1 раз в 6 месяцев	*Ответственный за ЗИ, Администратор безопасности АП АС ГС «Контингент»*

Мероприятие	Периодичность	Исполнитель
соответствия и других документов)		
Проверка неизменности настроенных параметров СЗИ, используемых в АП АС ГС «Контингент»	1 раз в месяц	*Администратор безопасности АП АС ГС «Контингент»*
Контроль состава ПО	1 раз в 3 месяца	*Администратор АП АС ГС «Контингент»*
Контроль правил заведения и удаления учетных записей пользователей	1 раз в 6 месяцев	*Ответственный за ЗИ, Администратор безопасности АП АС ГС «Контингент»*
Проверка соблюдения установленных правил организации парольной защиты	1 раз в 6 месяца	*Администратор АП АС ГС «Контингент», Администратор безопасности АП АС ГС «Контингент»*
Контроль соблюдения установленных правил организации антивирусной защиты	1 раз в 3 месяца	*Администратор АП АС ГС «Контингент», Администратор безопасности АП АС ГС «Контингент»*
Проверка работоспособности системы резервного копирования	1 раз в 6 месяцев	*Администратор АП АС ГС «Контингент»*
Проверка организации учета и условий хранения МНИ	1 раз в 6 месяцев	*Ответственный за ЗИ, Администратор безопасности АП АС ГС «Контингент»*
Проверка знаний персоналом базы нормативно-методических документов по защите информации	1 раз в 6 месяцев	*Ответственный за ЗИ*
Организация анализа и пересмотра имеющихся угроз безопасности информации АП АС ГС «Контингент», а также предсказание появления новых, еще неизвестных, угроз	Не реже 1 раз в год	*Ответственный за ЗИ, Администратор АП АС ГС «Контингент»*

Лист ознакомления
с Перечнем мероприятий по контролю обеспечения безопасности информации, в том числе ПДн в АП АС ГС «Контингент»
(утверждены приказом № 2380В от «10» апреля 2018 г.)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата
1	Лебедева Анна Николаевна	Начальник УК	11.04.18
2	Герасимов Александр Александрович	Начальник ОИБ	12.04.18
3	Жилова Екатерина Анатольевна	Вед. спец. студ. отд. кадров	12.04.18
4	Куликина Анастасия Валентиновна	Специалист по УМР	12.04.18
5.	Шишкарев Дмитрий Александр.	Вед. инженер	18.04.18
6	Горбунов Сергей Васильевич	Начальник управления	18.04.18
7	Кондрова Наталья Ивановна	нач. студ. отдела	18.04.18

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом и.о. ректора
ФГБОУ ВО «СГЭУ»
№ 2390В от «10» апреля 2018 г.

Перечень
программного обеспечения и (или) его компонентов, разрешенного к использованию на АП АС ГС «Контингент»

Сокращения

В настоящем документе использованы следующие сокращения:

АП АС ГС «Контингент» – абонентский пункт автоматизированной системы «Единая федеральная межведомственная система учёта Контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам».

НСД – несанкционированный доступ (несанкционированные действия).

ОС – операционная система.

ПДн – персональные данные.

ПО – программное обеспечение.

ПЭВМ – персональная электронная вычислительная машина.

СВТ – средство вычислительной техники.

СЗИ – средства защиты информации.

СКЗИ – средства криптографической защиты информации.

Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет».

ФСТЭК России – Федеральная служба по техническому и экспортному контролю России.

ФСБ России – Федеральная служба безопасности России.

Перечень программного обеспечения и (или) его компонентов, разрешенного к использованию на АП АС ГС «Контингент» Университета

№ п/п	Наименование и тип программного средства	Сведения о сертификате
ПЭВМ (г. Самара, ул. Советской Армии, 141, кабинет № 108А)		
1	Антивирус «Dr.Web Enterprise Security Suite 10»	Сертификат соответствия № 3509 Выдан 27.01.2016 г. Действителен до 27.01.2019 г
2	СКЗИ ПО ViPNet Client 4.x (КС2)	Сертификат соответствия ФСБ России СФ/124-2876 от 30.03.2016 г. Действителен до 31.12.2018 г. Сертификат соответствия ФСБ России СФ/515-2907 от 17.06.2016 г. Действителен до 29.04.2019 г.
3	Средство от НСД Dallas Lock 8.0-K	Сертификат соответствия ФСТЭК России № 2720 Выдан 25.09.2012 г. Действителен до 25.09.2015 г. Срок действия продлен до 25.09.2018 г.
4	ОС Windows 10 Pro	-
5	Microsoft Office стандартный 2003	-
6	Adobe Reader XI	-
7	Mozilla Firefox 51.0	-

Лист ознакомления
с Перечнем программного обеспечения и (или) его компонентов, разрешенного к использованию на АП АС ГС «Контингент»
(утверждены приказом № 238 ОВ от «10» апреля 2018 г.)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата
1	Лебедева Лина Николаевна	Начальник УК	11.04.18г.
2	Чернышов Александр Александрович	Начальник ОИБ	12.04.18г.
3	Хохлова Екатерина Анатольевна	Вед. спец. отд. ор. к.	12.04.18г.
4	Курышина Анастасия Валентиновна	Специалист по ГМР	12.04.18
5	Шишлов Дмитрий Владимирович	Вед. инженер	12.04.18
6	Гордеев Сергей Васильевич	Начальник отдела	12.04.18
7	Кедрова Наталья Ивановна	нач. отд. отдела	12.04.18

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом и.о. ректора
ФГБОУ ВО «СГЭУ»
№ 338-ОВ от «10» апреля 2018 г.

СОГЛАШЕНИЕ О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Я, _____,
(Ф.И.О.)

проживающий(ая) по адресу: _____
паспорт серия _____ №_____, выданный _____
_____
(кем и когда)

предупрежден(а) о том, что на период исполнения мною должностных обязанностей по Трудовому договору, заключенному между мною и Федеральным государственным бюджетным образовательным учреждением высшего образования «Самарский государственный экономический университет» (Далее – Университет) мне будет предоставлен доступ к персональным данным. Настоящим добровольно принимаю на себя обязательства:

– не передавать (в любом виде) и не разглашать третьим лицам и работникам Университета, не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением ректора Университета, информацию, содержащую персональные данные (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

– в случае попытки третьих лиц или работников Университета, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщать об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;

– не использовать информацию, содержащую персональные данные, с целью получения выгоды;

– выполнять требования закона и иных нормативных правовых актов Российской Федерации, а также внутренних документов Университета, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

– в течение 1 (Одного) года после прекращения моих прав на допуск к информации, содержащей персональные данные (переход на должность, не предусматривающую доступ к персональным данным или прекращения Трудового договора), не разглашать и не передавать третьим лицам и неуполномоченным на это работникам Университета известную мне информацию, содержащую персональные данные.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с действующим законодательством Российской Федерации.

_____ _____ _____
(дата) (подпись) (фамилия, инициалы)