ЮЗГУ	**МИНОБРНАУКИ РОССИИ** **Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет»**
	Система менеджмента качества

УТВЕРЖДАЮ

Ректор университета
(должность)

С.Г. Емельянов
(подпись)

«21» июля 2023 г.

ПОЛОЖЕНИЕ

о постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры, принадлежащих ФГБОУ ВО «Юго-Западный государственный университет»

П 96.210–2023

(Издание 1)

Введено в действие **Приказом от** «10» августа 2023 г. № 1092

Дата введения «10» августа 2023 г.

Срок действия до «10» августа 2028 г.

Введено впервые

:

Содержание

1 Область применения

1.1 Настоящее положение о постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры (далее - Комиссия) определяет основные функции, направления, задачи, порядок и обеспечение деятельности комиссии по категорированию объектов критической информационной инфраструктуры Российской Федерации, принадлежащих ФГБОУ ВО «Юго-Западный государственный университет» (далее – Университет).

1.2 Комиссия создается для принятия решения об отнесении информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, принадлежащих на праве собственности, аренды или на ином законном основании университету к объектам критической информационной инфраструктуры, включению объектов критической информационной структуры в Перечень объектов критической информационной инфраструктуры Университета, с последующим установлением одной из категорий значимости объектов критической информационной инфраструктуры, либо решения об отсутствии оснований для их отнесения к объектам критической информационной инфраструктуры в соответствии с требованиями Федерального закона от 25.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и Постановления Правительства Российской Федерации № 127 от 08.02.2018 г. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

1.3 Комиссия является постоянно действующим консультативно-совещательным органом Университета.

1.4 Комиссия руководствуется в своей деятельности правовыми актами Российской Федерации и настоящим положением.

2 Нормативные ссылки

Отношения в области обеспечения безопасности критической информационной инфраструктуры регулируются в соответствии с Конституцией Российской Федерации, общепризнанными принципами и нормами международного права, федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами:

№ п/п	Наименование документа	Кем или каким правовым актом утвержден документ
Федеральные законы		
1.	«О безопасности критической информационной инфраструктуры Российской Федерации»	Федеральный закон № 187-ФЗ от 26 июля 2017 г.
2.	«О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»	Федеральный закон № 193-ФЗ от 26 июля 2017 г.
3.	«О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»	Федеральный закон № 194-ФЗ от 26 июля 2017 г.

4.	«О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»	Федеральный закон № 141-ФЗ от 26 мая 2021 г.
Указы Президента Российской Федерации		
5.	«Доктрина информационной безопасности Российской Федерации»	Указ Президента Российской Федерации от 5 декабря 2016 г. № 646
6.	«О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»	Указ Президента Российской Федерации от 22 декабря 2017 г. № 620
7.	«О дополнительных мерах по обеспечению безопасности информационной инфраструктуры Российской Федерации»	Указ Президента Российской Федерации от 5 октября 2020 г. № 612
8.	«О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»	Указ Президента Российской Федерации от 30 марта 2022 г. № 166
9.	«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»	Указ Президента Российской Федерации от 1 мая 2022 г. № 250
10.	«Об утверждении Основ государственной политики в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации»	Указ Президента Российской Федерации от 8 июля 2022 г. № 438ДСП
Постановления Правительства Российской Федерации		
11.	«Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса»	Постановление Правительства Российской Федерации от 16 мая 2016 г. № 399
12.	«О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации»	Постановление Правительства Российской Федерации от 20 декабря 2022 г. № 2360
13.	«О внесении изменения в Правила организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса»	Постановление Правительства Российской Федерации от 11 июля 2018 г. № 808
14.	«Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»	Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127
15.	«О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127»	Постановление Правительства Российской Федерации № 452 от 13 апреля 2019 г.
16.	«О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации»	Постановление Правительства Российской Федерации № 2431 от 24 декабря 2021 г.
17.	«Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»	Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162
18.	«Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры»	Постановление Правительства Российской Федерации от 8 июня 2019 г. № 743

19.	«О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»	Постановление Правительства Российской Федерации от 6 июля 2015 г.№ 676
20.	«Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»	Постановление Правительства Российской Федерации от 15 июля 2022 г. № 1272
21.	«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»	Распоряжение Правительства Российской Федерации от 22 июня 2022 г. № 1661
22.	«О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации»	Постановление Правительства от 19 августа 2022 г. № 1463
23.	«Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц»(за исключением организаций с муниципальным участием),на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, Правил согласования закупок иностранного программного обеспечения,в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупкив соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих имзначимых объектах критической информационной инфраструктуры Российской Федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах,и Правил перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, заказчиками, осуществляющими закупкив соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации.	Постановление Правительства от 22 августа 2022 г. № 1478
Приказы ФСТЭК России		
24.	«Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»	Приказ ФСТЭК России от 21 декабря 2017 г. № 235
25.	«О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235»	Приказ ФСТЭК России от 27 марта 2019 г. № 64

26.	«Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»	Приказ ФСТЭК России от 22 декабря 2017 г. № 236
27.	«О внесении изменений в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236»	Приказ ФСТЭК России от 21 марта 2019 г. № 59
28.	«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»	Приказ ФСТЭК России от 25 декабря 2017 г. № 239
29.	«О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239»	Приказ ФСТЭК России от 9 августа 2018 г. № 138
30.	«О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239»	Приказ ФСТЭК России от 26 марта 2019 г. № 60
31.	«О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239»	Приказ ФСТЭК России от 20 февраля 2020 г. № 35
32.	«Об утверждении Порядка согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования»	Приказ ФСТЭК России от 28 мая 2020 г. № 75
33.	«Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»	Приказ ФСТЭК России от 29 апреля 2021 г. № 77
34.	«Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»	Приказ ФСТЭК России от 14 марта 2014 г. № 31
35.	«О внесении изменений в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. № 227»	Приказ ФСТЭК России от 10 февраля 2022 г. № 26
36.	Требования к обеспечению защиты информации, содержащихся в информационных системах управления производством, используемых предприятиями оборонно-промышленного комплекса.	Приказ ФСТЭК России от 28 февраля 2017 г. № 31ДСП
37.	«Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»	Приказ ФСТЭК России от 6 декабря 2017 г. № 227

38.	«О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31»	Приказ ФСТЭК России от 9 августа 2018 г. № 138
39.	Информационное сообщение о методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации от 4 мая 2018 г. № 240/22/2339	На сайте ФСТЭК России
40.	Информационное сообщение по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий от 17 апреля 2020 г. № 240/84/611	На сайте ФСТЭК России
Приказы ФСБ России		
41.	«Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты»	Приказ ФСБ России от 24 июля 2018 г. № 368
42.	«Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»	Приказ ФСБ России от 24 июля 2018 г. № 367
43.	«О Национальном координационном центре по компьютерным инцидентам»	Приказ ФСБ России от 24 июля 2018 г. № 366
44.	«Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»	Приказ ФСБ России от 6 мая 2019 г. № 196
45.	«Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»	Приказ ФСБ России от 19 июня 2019 г. № 281
46.	«Об утверждении порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»	Приказ ФСБ России от 19 июня 2019 г. № 282

Приказы Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации		
47.	«Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»	Приказ Минкомсвязи России от 17 марта 2020 г. № 114

3 Термины, определения, обозначения и сокращения

автоматизированная система управления - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

автоматизированное рабочее место – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

безопасность критической информационной инфраструктуры - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

значимый объект критической информационной инфраструктуры - объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

информационные ресурсы Российской Федерации- информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации;

информационная система - система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

компьютерный инцидент - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

АРМ – автоматизированное рабочее место;
АСУ - автоматизированная система управления;
ИБ - информационная безопасность;
ИТС - информационно-телекоммуникационная сеть;
КИИ - критическая информационная инфраструктура.

4 Положения

4.1 Организационная структура

4.1.1 Комиссия создается решением руководителя субъекта критической информационной инфраструктуры – ректора Университета.

4.1.2 Состав Комиссии утверждается приказом ректора Университета по представлению председателя Комиссии.

4.1.3 Руководство Комиссии осуществляет лицо, уполномоченное ректором Университета.

4.1.4 Председатель Комиссии может иметь одного заместителя.

4.1.5 Председатель Комиссии, его заместитель, а также состав Комиссии формируется в соответствии с требованиями статьи 11 постановления Правительства Российской Федерации от 08.02.2018 № 127 Об утверждении «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» и утверждается приказом ректора Университета.

4.1.6 К участию в работе Комиссии дополнительно решением председателя могут приглашаться (по согласованию) руководители и специалисты органов исполнительной власти Курской области, предприятий, организаций и учреждений, имеющих непосредственное отношение к рассматриваемым вопросам, иные специалисты, привлекаемые в качестве экспертов.

4.1.7 Периодичность созыва Комиссии определяется ее председателем.

4.2 Цели и задачи

4.2.1 **Целью деятельности Комиссии** является обеспечение безопасности объектов критической информационной инфраструктуры Университета далее –КИИ).

4.2.2 **Задачи**:

- своевременное выявление объектов КИИ,
- подготовка предложений для включения в перечень объектов КИИ;
- выявление возможных действий нарушителей в отношении объектов КИИ и иных источников угроз безопасности информации;
- анализ угроз безопасности информации и уязвимостей, компьютерных инцидентов на объектах КИИ;
- оценка критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;
- категорирование объектов КИИ.
- организация координации работы структурных подразделений университета по комплексной защите информации на объектах КИИ;
- мониторинг эффективности работы структурных подразделений университета по комплексной защите информации на объектах КИИ.

4.3 Функции

4.3.1 На Комиссию возлагаются следующие функции:

- определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности Университета;
- выявление наличия критических процессов у субъекта КИИ в рамках выполнения функций (полномочий) или осуществления видов деятельности Университета;
- выявление объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также подготовку предложений для включения в перечень объектов критической информационной инфраструктуры;
- формирование перечня объектов КИИ, подлежащих категорированию в университете (оформляется по форме предусмотренной приложением А);
- рассмотрение возможных действий нарушителей в отношении объектов КИИ, а также иных источников угроз безопасности информации;
- анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;
- оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ (оформляется по форме предусмотренной приложением Б);
- установление каждому из объектов КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им категорий значимости;

- подготовка и предоставление в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведений о собственных объектах критической информационной инфраструктуры в соответствии с требованиями постановления Правительства Российской Федерации от 08.02.2018 № 127.

4.4 Полномочия, порядок и обеспечение деятельности, ответственность

4.4.1 Заседания Комиссии проводятся по мере необходимости по решению председателя Комиссии.

4.4.2 Заседание Комиссии считается правомочным при присутствии на нем не менее 2/3 от общего числа членов Комиссии. Присутствие на заседании Комиссии иных лиц, кроме членов Комиссии, допускается с разрешения председателя Комиссии.

4.4.3 **Председатель Комиссии:**

- назначает дату, время и место проведения заседаний Комиссии;
- утверждает повестку заседания Комиссии;
- руководит заседанием Комиссии;
- распределяет обязанности между членами Комиссии;
- подписывает акты и иные документы, подготовленные Комиссией;
- пользуется правами члена Комиссии наравне с другими членами Комиссии;
- осуществляет организационное и материально-техническое обеспечение деятельности Комиссии.

В период временного отсутствия председателя Комиссии (командировка, отпуск, болезнь и пр.) его полномочия осуществляет один из заместителей председателя Комиссии, назначенный приказом ректора Университета на основании служебной записки председателя комиссии.

4.4.4 **Секретарь Комиссии:**

- координирует деятельность членов Комиссии;
- готовит проекты повесток заседаний Комиссии и представляет на утверждение председателю Комиссии;
- своевременно информирует членов Комиссии о дате, времени, месте и повестке заседаний Комиссии;
- в случае необходимости совместно с членами Комиссии готовит информацию, документы, иные материалы к заседаниям Комиссии;
- в течение 5 рабочих дней с даты проведения заседания Комиссии и в соответствии с ее решением готовит акт (протокол) и представляет его на подпись председателю Комиссии, заместителю председателя Комиссии, иным членам Комиссии;
- организует и ведет делопроизводство Комиссии.

В случае отсутствия секретаря Комиссии (командировка, отпуск, болезнь и пр.) его полномочия осуществляет один из членов Комиссии, назначенный председателем Комиссии.

4.4.5 **Члены Комиссии** имеют право:

- участвовать в работе Комиссии;
- участвовать в обсуждении вопросов, включенных в повестку заседания Комиссии, вносить по ним предложения;
- запрашивать и получать от структурных подразделений университета документы и информацию, необходимые для выполнения функций Комиссии;
- знакомиться с информацией, документами и материалами по вопросам, вынесенным на обсуждение Комиссии, на стадии их подготовки, вносить свои предложения;

- в случае несогласия с принятым решением изложить свое особое мнение в письменном виде, которое прилагается к соответствующему заключению Комиссии.
- вносить предложения по улучшению работы Комиссии, повышению эффективности ее функционирования;

4.4.6 Решения Комиссии принимаются простым большинством голосов членов Комиссии как присутствующих на заседании, так и отсутствующих, выразивших свое мнение в письменном виде и представивших его на заседание Комиссии.

4.4.7 Каждый член Комиссии имеет один голос. При равенстве голосов принятым считается решение, за которое проголосовал председательствующий на заседании Комиссии.

4.4.8 Решение Комиссии по проведению инвентаризации информационных ресурсов, выявления информационных систем, потенциально относящихся к объектам КИИ и подготовка предложений для включения в перечень объектов КИИ оформляются протоколом. Протокол подписывается председателем, заместителем председателя, секретарем и другими членами и утверждается ректором Университета.

4.4.9 Решение Комиссии по категорированию объектов КИИ оформляется актом, который должен содержать сведения об объекте КИИ, результаты анализа угроз безопасности информации объекта КИИ, реализованные меры по обеспечению безопасности объекта КИИ, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры. Акт подписывается председателем, заместителем председателя, секретарем и другими членами и утверждается ректором Университета.

4.4.10 Протоколы заседаний Комиссии, заключения и акты должны храниться в Университете до вывода из эксплуатации соответствующих объектов критической информационной инфраструктуры или до изменения решений, принятых в указанных документах из-за изменений в работе Университета или самих объектов критической информационной инфраструктуры.

4.5 Взаимодействие с другими структурными подразделениями университета и сторонними организациями

4.5.1 Комиссия, в лице председателя или уполномоченных им лиц, взаимодействует со сторонними организациями и структурными подразделениями Университета, по вопросам реализации ее функций в пределах полномочий, определенных настоящим положением.

4.5.2 Комиссия взаимодействует со структурными подразделениями Университета, эксплуатирующими и (или) создающими новые объекты критической информационной инфраструктуры, а также со структурными подразделениями, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов критической информационной инфраструктуры, структурным подразделением по защите государственной тайны субъекта критической информационной инфраструктуры (в случае, если объект критической информационной инфраструктуры обрабатывает информацию, составляющую государственную тайну) и структурным подразделением по гражданской обороне и защите от чрезвычайных ситуаций, а также со сторонними организациями, предприятиями, учреждениями, уполномоченными по ведению работ в

области обеспечения безопасности критической информационной инфраструктуры Российской Федерации:

4.5.3 Комиссия взаимодействует с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации:

- по объектам КИИ сфер финансового рынка, ракетно-космической, горнодобывающей, металлургической и химической промышленности, с 8 управлением ФСТЭК России: 105066, г. Москва, Старая Басманная ул., д.17;
- по объектам КИИ сфер здравоохранения, науки, энергетики, топливно-энергетического комплекса, оборонной промышленности и связи, с управлением ФСТЭК России по Центральному федеральному округу: 117342, г. Москва, Севастопольский просп., д.56/40, стр.1. электронная почта cfo_1otd@fstec.ru, контактный телефон +7 (495) 334-78-17.

4.6 Ответственность

4.6.1 Комиссия, в лице председателя несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации за нарушение требований Федерального законодательства в области обеспечения безопасности значимых объектов критической информационной инфраструктуры и принятых в соответствии с ним иных нормативных правовых актов.

4.6.2 Вид и степень ответственности за нарушения требований Федерального законодательства в области обеспечения безопасности значимых объектов критической информационной инфраструктуры определяется вышестоящим руководством Университета.

Приложение А

(обязательное)

Форма

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

СОГЛАСОВАНО

Должность руководителя государственного органа или российского юридического лица, выполняющего функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере в части подведомственных им субъектов критической информационной инфраструктуры или уполномоченного им лица

Подпись руководителя или уполномоченного им лица

Фамилия, имя, отчество (при наличии) руководителя или уполномоченного им лица

« » _____ 202 ___ г.

Дата согласования перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

УТВЕРЖДАЮ

Должность руководителя субъекта критической информационной инфраструктуры Российской Федерации (далее – субъект) или уполномоченного им лица

Подпись руководителя субъекта или уполномоченного им лица

Фамилия, имя, отчество (при наличии) руководителя субъекта или уполномоченного им лица

« » _____ 202 ___ г.

Дата утверждения перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

Перечень
объектов критической информационной инфраструктуры (наименование субъекта), подлежащих категорированию

№ п/п	Наименование объекта КИИ	Тип объекта	Сфера (область) деятельности, в которой функционирует объект	Планируемый срок категорирования объекта КИИ	Должность, фамилия, имя, отчество представителя, его телефон, адрес электронной почты
1					
…					

(Наименование должности руководителя субъекта критической информационной инфраструктуры или уполномоченного им лица)

(подпись)

(инициалы, фамилия)

М.П.

«___» _____ 20___ г.

Приложение Б

(обязательное)

Форма

Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

1. Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	
1.4.	Назначение объекта	
1.5.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	

2. Сведения о субъекте критической информационной инфраструктуры

2.1.	Наименование субъекта	
2.2.	Адрес местонахождения субъекта	
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	
2.6.	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	
3.2.	Наименование оператора связи и (или) провайдера хостинга	
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводный), протоколов взаимодействия	

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1.	Наименование лица, эксплуатирующего объект	
4.2.	Адрес местонахождения лица, эксплуатирующего объект	
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	
4.4.	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры

5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	
	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (прикладные программы, входящие в состав дистрибутивов операционных систем, не указываются)	
5.4.	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	

6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	

7. Возможные последствия в случае возникновения компьютерных инцидентов

7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости

8.1.	Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий	
8.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	
8.3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	

9. Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры

9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	

(Наименование должности руководителя субъекта критической информационной инфраструктуры или уполномоченного им лица)	(подпись)	(инициалы, фамилия)

М.П.

«___» _____ 20___ г.

Приложение В

(обязательное)

Форма

Сведения о результатах реализации (наименование субъекта КИИ) положений Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и изданных в его исполнение нормативных правовых актов

<table>
<tr><td colspan="13">Сведения о результатах реализации (наименование субъекта КИИ) положений Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и изданных в его исполнение нормативных правовых актов</td></tr>
<tr><td colspan="13">(сфера: оборонная, ракетно-космическая промышленность)</td></tr>
<tr><td rowspan="3">№ п/п</td><td rowspan="3">Наименование субъетка КИИ</td><td colspan="3">Проведение работ по определению наличия в организации объектов КИИ①</td><td rowspan="3">Формирование и направление в ФСТЭК России перечня объектов КИИ, подлежащих категорированию (исходящий номер и дата)③</td><td colspan="5">Категорирование объектов КИИ④</td><td colspan="2" rowspan="2">Получение из центрального аппарата ФСТЭК России, Управления ФСТЭК России по Центральному федеральному округу уведомления (исходящий номер и дата)⑥</td></tr>
<tr><td rowspan="2">Наименование, номер и дата правового акта по созданию постоянно действующей комиссии②</td><td rowspan="2">Дата окончания выполнения работ (чч.мм.гг)</td><td rowspan="2">Наличие объектов КИИ (количество или отсутствуют)</td><td colspan="4">Количество объектов КИИ по категориям значимости</td><td rowspan="2">Направление в центральный аппарат ФСТЭК России, управление ФСТЭК России по Центральному федеральному округу результатов категорирования объектов КИИ (исходящий номер и дата)⑤</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>без категории</td><td>о включении объектов КИИ в Реестр значимых объектов КИИ РФ</td><td>о направлении сведений в ГосСОПКА</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td></tr>
<tr><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

(Наименование должности руководителя субъекта критической информационной инфраструктуры или уполномоченного им лица) _____ (подпись) _____ (инициалы, фамилия)

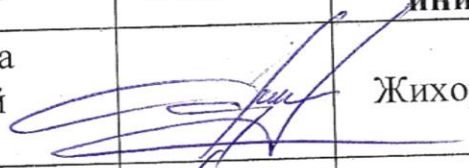
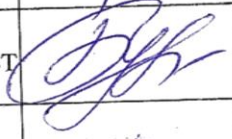
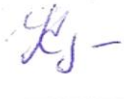
М.П.

«___» _____ 20___ г.

Лист согласования

Основание для разработки: Приказ от 18.07.2023 № 990а

(наименование, дата и номер документа)

	Должность	Подпись	Фамилия, инициалы	Дата
Разработан:	Начальник отдела информационной безопасности		Жихорцев А.А.	19.07.2023г.
Проверен:	Проректор по цифровой трансформации		Пыхтин А.И.	21.07.2023г.
Согласован:	Ведущий юрисконсульт		Будовская Е.В.	20.07.2023г.
	Начальник отдела менеджмента качества		Дмитракова Т.В.	20.07.2023г.

Лист ознакомления

С положением о постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры, принадлежащих ФГБОУ ВО «Юго-Западный государственный университет» ознакомлен:

Фамилия, инициалы	Дата ознакомления	Подпись

Лист регистрации изменений

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	заменен-ных	аннулиро-ванных	новых			