Министерство просвещения Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Глазовский государственный инженерно-педагогический университет имени В.Г. Короленко»

УТВЕРЖДАЮ
Ректор
_____ Я. А. Чиговская-Назарова
приказ от «18» НОЯБРЯ 2024г. № 136

Документ подписан
усиленной квалифицированной
электронной подписью

Сертификат: 0258bf5d001ab2109d4d10696c09935145
Владелец: **Чиговская-Назарова Янина Александровна**
Действителен: с 31.10.2024 по 31.01.2026

Регламент

оценки показателя состояния технической защиты информации и обеспечения безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Глазовский государственный инженерно-педагогический университет имени В.Г. Короленко»

Глазов 2024

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий Регламент оценки показателя состояния технической защиты информации и обеспечения безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Глазовский инженерно-педагогический университет имени В.Г. Короленко» (далее - Университет) разработана в соответствии с подпунктами 4 и 6.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

2. Настоящий Регламент определяет показатель, характеризующий текущее состояние технической защиты информации, не составляющей государственную тайну (далее — защита информации), и (или) обеспечения безопасности Университета, его нормированное значение, а также порядок его расчета.

3. Настоящий Регламент применяется для оценки текущего состояния защиты информации в ФГБОУ ВО «ГИПУ», и степени его соответствия минимально необходимому уровню защиты информации от типовых актуальных угроз безопасности информации.

В качестве минимально необходимого уровня защиты информации задан состав мер, реализация которых предусмотрена нормативными правовыми актами Российской Федерации, и который минимально достаточен для блокирования (нейтрализации) типовых актуальных угроз безопасности информации.

4. Несоответствие значения показателя, характеризующего текущее состояние защиты информации, установленному в соответствии с настоящим Регламентом нормированному значению указывает на наличие в Университете возможности реализации актуальных угроз безопасности информации или предпосылок для их реализации.

5. Настоящий Регламент применяется в ФГБОУ ВО «ГИПУ» для оценки текущего состояния защиты информации и разработки на основе такой оценки мер по повышению уровня защищенности, а также оценки эффективности деятельности должностного лица, на которого возложены полномочия по обеспечению информационной безопасности Университета, осуществляющего функции по обеспечению информационной безопасности.

6. Регламент не применяется для оценки деятельности в области обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

II. ПОКАЗАТЕЛЬ ЗАЩИЩЕННОСТИ И ЕГО НОРМИРОВАННОЕ ЗНАЧЕНИЕ

1. В качестве показателя, характеризующего текущее состояние защиты информации в ФГБОУ ВО «ГИПУ», используется показатель текущего состояния защищенности $К_{ЗИ}$ (далее — показатель защищенности $К_{ЗИ}$, показатель $К_{ЗИ}$).

Показатель $К_{ЗИ}$ характеризует степень достижения Университета минимально необходимого уровня защиты информации от типовых актуальных угроз безопасности информации во временном интервале оценивания и заданных условиях эксплуатации информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, иных объектов информатизации.

2. Информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, иные объекты информатизации и содержащаяся в них информация (далее — информационные системы) Университета имеют минимально необходимый уровень защищенности от типовых актуальных угроз безопасности информации, если значение показателя $К_{ЗИ}$ соответствует нормированному значению:

$$К_{ЗИ} = 1$$

3. Полученное в соответствии с настоящим Регламентом значение показателя защищенности $К_{ЗИ}$ является критерием принятия в ФГБОУ ВО «ГИПУ» управленческих решений в части необходимости реализации первоочередных мер по защите информации от актуальных угроз безопасности информации и их приоритетности.

III. ПОРЯДОК ОЦЕНКИ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ

1.Оценка показателя защищенности $К_{ЗИ}$ включает:

а) сбор и анализ исходных данных, необходимых для оценки показателя $К_{ЗИ}$;

б) оценку значений частных показателей безопасности j

в) расчет значения показателя $К_{ЗИ}$ и его сравнение с нормированным значением.

2. Оценка показателя $К_{ЗИ}$ проводится не реже одного раза в шесть месяцев.

3. Оценка показателя защищенности $К_{ЗИ}$ проводится в отношении всех информационных систем, подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации. Включение в область оценки иных информационных систем ФГБОУ ВО «ГИПУ» осуществляется по решению ректора (должностного лица) Университета.

Информационные системы Университета функционируют на базе информационно-телек

4. В ФГБОУ ВО «ГИПУ» оценка показателя $К_{ЗИ}$ организуется проректором по образовательной деятельности Университета и проводится центром информатизации и дистанционного обучения (далее- ЦИиДО), осуществляющими функции по обеспечению информационной безопасности.

Указанная оценка может проводиться на основе результатов внутреннего контроля или внешней оценки соответствия (аудита безопасности), мониторинга информационной безопасности, оценки защищенности и (или) аттестации информационных систем, иных мероприятий по изучению и контролю уровня защищенности информации.

5. О полученном по результатам расчета значении показателя $К_{ЗИ}$, не соответствующем нормированному значению, информируется ректор Университета для принятия решения о необходимости совершенствования (улучшения) принимаемых в органе (организации) мер по защите информации.

6. Результаты оценки показателя защищенности $К_{ЗИ}$ предоставляются Университетом в ФСТЭК России по ее запросу в целях оценки текущего состояния защиты информации и обеспечения безопасности объектов в соответствии с подпунктом 6.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 1085. ФСТЭК России могут быть запрошены отдельные исходные данные, используемые для оценки показателя защищенности $К_{ЗИ}$, подтверждающие получение представленных результатов оценки. ФСТЭК России принимаются меры по обеспечению конфиденциальности информации, представляемой Университетом.

7. ФСТЭК России проводится анализ поступивших результатов оценки показателя $К_{ЗИ}$ и (или) исходных данных, используемых для его оценки, осуществляется верификация результатов его расчета и делается вывод о текущем состоянии защиты информации в ФГБОУ ВО «ГИПУ».

Значение показателя $К_{ЗИ}$ Университета может быть уточнено ФСТЭК России в соответствии с выводами о достаточности принимаемых мер по защите информации, сделанными по результатам государственного контроля, проведенного в пределах ее полномочий, и (или) на основе результатов анализа документов, иных материалов, предоставленных по запросу ФСТЭК России Университетом. О значении показателя защищенности $К_{ЗИ}$, определенном ФСТЭК России, в случае его несоответствия нормированному значению информируется ФГБОУ ВО «ГИПУ».

8. В случае если значение показателя защищенности $К_{ЗИ}$ не соответствует нормированному значению, в Университете на основе полученных значений частных

показателей kj_i определяются меры по защите информации, которые не реализованы или реализация которых не обеспечивает защиту от типовых актуальных угроз безопасности информации, и приоритетность их реализации, а также планируются мероприятия по реализации (совершенствованию) мер в соответствии с установленными целями по обеспечению защиты информации.

9. Внеочередная оценка показателя защищенности $К_{ЗИ}$ проводится ФГБОУ ВО «ГИПУ» в случаях:

а) возникновения инцидента информационной безопасности, повлекшего наступление негативных последствий (возникновение значимого инцидента);

б) развития (изменения) архитектуры информационных систем;

в) запроса ректора Университета о текущем значении показателя защищенности $К_{ЗИ}$;

г) запроса ФСТЭК России.

IV СБОР И АНАЛИЗ ИСХОДНЫХ ДАННЫХ, НЕОБХОДИМЫХ ДЛЯ ОЦЕНКИ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ

1. Исходными данными, необходимыми для оценки показателя защищенности $К_{ЗИ}$ могут являться:

а) акты, протоколы, иные документы, составленные по результатам государственного контроля в области защиты информации;

б) отчеты, протоколы, иные документы, составленные по результатам внутреннего контроля уровня защищенности информации;

в) отчеты, составленные по результатам внешней оценки соответствия в области защиты информации;

г) внутренние организационно-распорядительные документы, регламентирующие организацию защиты информации в Университете;

д) эксплуатационная документация на средства защиты информации, содержащая сведения об их настройках и конфигурации;

е) результаты проведения инвентаризации информационных систем;

ж) результаты опроса (интервьюирования) работников ФГБОУ ВО «ГИПУ» о выполнении ими функций (задач) с использованием информационных систем и (или) по обеспечению информационной безопасности;

з) результаты анализа функционирования (применения) отдельных программных, программно-аппаратных средств информационных систем Университета.

и) результаты работы инструментальных средств оценки (анализа) защищенности информационных систем и (или) мониторинга информационной безопасности.

2. Для сбора и анализа исходных данных назначаются специалисты из ЦИиДО, осуществляющие функции по обеспечению информационной безопасности Университета.

Рекомендуется назначать специалистов, обладающих следующими компетенциями:

а) знание целей, задач, основ организации защиты информации;

б) знание состава и содержания организационно-распорядительных документов по вопросам защиты информации;

в) знание процессов организации защиты информации и умение их внедрять;

г) знание основных методов и способов защиты информации и умение их практически реализовывать.

3. Специалисты ЦИиДО Университета не должны проводить оценку материалов, характеризующих (демонстрирующих, подтверждающих) результаты реализации ими собственных функций и (или) задач.

4. Порядок назначения специалистов ЦИиДО Университета определяется во внутренних регламентах с учетом положений настоящего Регламента.

5. Специалисты ЦИиДо Университета:

а) запрашивают в структурных подразделениях (филиалах, представительствах) ФГБОУ ВО «ГИПУ» требуемые для анализа документы и материалы;

б) проводят опросы (интервьюирование) работников Университета о выполнении ими функций с использованием информационных систем и(или) по обеспечению информационной безопасности;

в)осуществляют анализ функционирования отдельных программных, программно-аппаратных средств в информационных системах, в том числе средств защиты информации, средств инвентаризации информационных систем, инструментальных средств оценки защищенности и (или) мониторинга информационной безопасности.

Подразделения и специалисты ФГБОУ ВО «ГИПУ», привлекаемые для сбора исходных данных, оказывают содействие и принимают исчерпывающие меры для предоставления документов и материалов, требуемых для анализа.

В случае непредставления структурным подразделением и привлекаемыми специалистами Университета запрошенных для проведения оценки документов и

материалов соответствующим частным показателям безопасности kj_i присваивается значение 0.

6. Результаты проведения опроса (интервьюирования) работников ФГБОУ ВО «ГИПУ» о составе и порядке реализации ими функций (задач) в информационных системах и (или) обеспечении информационной безопасности подлежат документированию в виде и в форме, определяемыми Университетом.

7. Собранные исходные данные подлежат анализу специалистами по сбору и анализу исходных данных с целью формирования выводов о реализации в Университете мероприятий (процессов) по защите информации о достаточности принимаемых мер по защите информации. По результатам анализа исходных данных специалисты формируют выводы о реализации мер, соответствующих частным показателям безопасности kj_i.

8. Полученные результаты анализа исходных данных, а также результаты расчета значений показателя защищенности $К_{ЗИ}$ подлежат документированию и направляются в ФСТЭК России в случае поступления запроса.

V. ОПРЕДЕЛЕНИЕ ЗНАЧЕНИЙ ЧАСТНЫХ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ

1. Для оценки показателя защищенности $К_{ЗИ}$ определяются значения частных показателей безопасности j где j — номер группы частных показателей безопасности,

i— номер частного показателя в соответствующей группе показателей безопасности.

Частные показатели безопасности kj_i характеризуют реализацию в Университете отдельных мер по защите информации от актуальных угроз безопасности информации, а также их соответствие целям обеспечения безопасности в Университете.

2. Определение значений частных показателей безопасности kj_i осуществляется специалистами, проводившими сбор и анализ исходных данных.

3. Перечень используемых частных показателей безопасности kj_i, их наименования и максимальные значения приведены в таблице 1.

4. Частные показатели безопасности kj_i определяются для всех информационных систем, подлежащих защите в соответствии с нормативными правовыми актами Российской Федерации, находящихся в распоряжении Университета.

5. Определение значений частных показателей безопасности kji предусматривает присвоение им значений на основе результатов анализа материалов, подтверждающих

актуальных угроз безопасности информации.

6. Если по результатам проведенного анализа материалов сделаны выводы, что меры по защите информации в Университете реализованы, соответствующему частному показателю присваивается значение, установленное для него в таблице 1.

Если по результатам проведенного анализа материалов сделаны выводы, что соответствующая мера не реализована или реализована неэффективно (не в полном объеме), соответствующему частному показателю присваивается значение 0.

Таблица 1

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование показателя безопасности	Значение частного	Значение весового коэффициент группы показателей (Rj)
1.	Организация и управление	11. На должностное лицо возложены[1] полномочия за обеспечение информационной безопасности Университета и определены его обязанности	0,30	0,10
		2. Определены функции ЦИиДО ФГБОУ ВО «ГИПУ»	0,40	
		3. К подрядным организациям, имеющим доступ к информационным системам с привилегированными правами, в договорах установлены требования о реализации мер по защите от угроз через информационную инфраструктуру подрядчика[2]	0,30	
2.	Защита пользователей	1. Отсутствуют учетные записи с паролем, сложность которого не соответствует установленным требованиям к парольной политике. В случае отсутствия технической возможности обеспечения требуемой сложности паролей реализованы компенсирующие меры	0,30	0,25
		2. Реализована многофакторная аутентификация привилегированных пользователей (при аутентификации не менее 50% администраторов, разработчиков или иных привилегированных пользователей используется второй фактор)[3]	0,30	

1 Возложение полномочий и (или) определение структурного подразделения (работников) в органе (организации) подтверждается изданием соответствующего локального правового акта.

2 В случае если подрядные организации не привлекаются, частному показателю безопасности ki_3 присваивается значение из таблицы 1.

3 В случае отсутствия технической возможности реализации в информационной системе или в технических средствах двухфакторной аутентификации соответствующему показателю безопасности присваивается значение из таблицы 1.

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование показателя безопасности	Значение частного показателя (kji)	Значение весового коэффициент группы показателей (Rj)
		3. Отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными ими по умолчанию	0,20	
		4. Отсутствуют активные учетные записи работников органа (организации) и работников, привлекаемых на договорной основе, с которыми прекращены трудовые или иные отношения	0,20	
3.	Защита информационных систем	1. На сетевом периметре информационных систем установлены межсетевые экраны уровня L3/L4 (доступ к 100% интерфейсов, доступных из сети Интернет[6], контролируется межсетевыми экранами уровня L3/L4)	0,20	0,35
		2. На устройствах и интерфейсах, доступных из сети Интернет, отсутствуют уязвимости критического уровня опасности с датой публикации обновлений (компенсирующих мер по устранению) в банке данных угроз ФСТЭК России, на официальных сайтах разработчиков, иных открытых источниках более 30 дней или в отношении таких уязвимостей реализованы компенсирующие меры	0,20	
		3. На пользовательских устройствах и серверах отсутствуют уязвимости критического уровня с датой публикации обновления (компенсирующих мер по устранению) более 90 дней (не менее 90% устройств и серверов) или в отношении таких уязвимостей реализованы компенсирующие меры	0,10	
		4. Обеспечен документальный или автоматизированный учет пользовательских устройств, серверов и сетевых устройств (не менее 80% устройств и серверов учтено в документах (ведомостях,	0,10	

6) В случае отсутствия в информационных системах устройств, интерфейсов, взаимодействующих с сетью Интернет, соответствующим показателям безопасности присваиваются значения из таблицы 1.

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование показателя безопасности	Значение частного показателя (kji)	Значение весового коэффициент группы показателей (Rj)
		паспортах, эксплуатационной документации) или в автоматизированных системах (CMDB))		
		5. Обеспечена проверка вложений в электронных письмах электронной почты на наличие вредоносного программного обеспечения (проверяются вложения не менее чем на 80% пользовательских устройств)	0,15	
		6. Обеспечено централизованное управление средствами антивирусной защиты[4] [5] [6](не менее чем 80% пользовательских устройств[9] контролируются средствами антивирусной защиты с централизованным управлением). При этом обеспечены контроль и установка обновлений баз данных признаков вредоносного программного обеспечения не реже чем 1 раз в месяц	0,15	
		7. Реализована очистка входящего из сети Интернет сетевого трафика от аномалий на уровне[7] L3/L4 (заключен договор с провайдером)	0,10	
4.	Мониторинг Информационной безопасности и	1. Реализован централизованный сбор событий безопасности и оповещение о неудачных попытках входа для привилегированных учетных записей	0,40	0,30

4 В случае если в информационных системах органа (организации) не используется электронная почта, частному показателю безопасности k_{35} присваиваются значение из таблицы 1.

5 Если в органе (организации) используются автономные рабочие места, на них должны быть установлены автономные средства антивирусной защиты (тип «Г»). В этом случае частному показателю безопасности k_{36} присваивается значение из таблицы 1.

6 Если информационные системы содержат пользовательские устройства, в которых конструктивно отсутствуют интерфейсы для возможного внедрения вредоносного программного обеспечения, частному показателю безопасности k_{36} присваивается значение из таблицы 1.

7 Если в информационных системах отсутствуют веб-сайт или иные сервисы, подверженные DDos-атакам, частному показателю безопасности k_{37} присваивается значение из таблицы 1.

Номер группы показателей (j)	Наименование групп показателей	Номер (i) и наименование показателя безопасности	Значение частного показателя (kji)	Значение весового коэффициент группы показателей (Rj)
	реагирование	2. Реализован централизованный сбор и анализ событий безопасности на всех устройствах, взаимодействующих с сетью Интернет	0,35	
		3. Утвержден документ, определяющий порядок реагирования на компьютерные инциденты	0,25	

VI. РАСЧЕТ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ И ЕГО СРАВНЕНИЕ С НОРМИРОВАННЫМ ЗНАЧЕНИЕМ

1.Расчет показателя защищенности $К_{зи}$ осуществляется по следующей формуле:

K^(kn+ki2+ki3)Ri+(k2i+k22+...+k2i)R2+(k3i+k32+...+k3i)R3+(k4i+k42+...+k4i)R4,

где Rj — весовой коэффициент j — й группы частных показателей безопасности, определяемый в соответствии с таблицей 1.

2.Если при очередном расчете показателя защищенности $К_{зи}$ фиксируется повторное (в течении 12 месяцев) невыполнение мер, предусмотренных частным показателем безопасности j и данному показателю безопасности повторно присвоено значение 0, то весовому коэффициенту этой группы показателей Rj присваивается значение 0 (обнуляется вся группа показателей).

3.Рассчитанный в соответствии с пунктом 33 показатель защищенности $К_{зи}$ сравнивается с нормированным значением. На основе результатов сравнения формируются выводы (таблица 2) о текущем состоянии защиты информации в Университете.

Таблица 2

Значение Кзи	Текущее состояние защиты информации (обеспечения безопасности объектов КИИ)
Кзи=1	Обеспечивается минимальный уровень защиты от типовых актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как минимальный базовый («зеленый»)
0,75<Кзи<1	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеются предпосылки реализации актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как низкий («оранжевый»)
Кзи<0,75	Минимальный уровень защиты от актуальных угроз безопасности информации не обеспечивается, имеется реальная возможность реализации актуальных угроз безопасности информации. Уровень состояния защищенности характеризуется как критический («красный»)

4.В случае если по результатам расчета получено значение показателя защищенности Кзи, характеризующее текущее состояние защищенности в Университете как низкое («оранжевый») или критическое («красный»), разрабатывается план реализации мероприятий по достижению следующего уровня защиты от актуальных угроз. Срок реализации мероприятий, определенных в плане, не должен превышать срок до проведения следующей плановой оценки показателя Кзи.