МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ И НАУКИ
КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КАБАРДИНО-БАЛКАРСКИЙ ТОРГОВО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

Рассмотрен
Педагогическим советом
Протокол №1 от«31»августа 2023г.

УТВЕРЖДЕН
Приказом ГБПОУ «КБТТК»
№ 10-02/208-1 о/д
от «31» АВГУСТА 2023г

Принят
Советом учреждения
Протокол № 1 от «31» августа 2023 г.

Положение
об электронной информационно-образовательной среде ГБПОУ «Кабардино-Балкарский торгово-технологический колледж»

г.о. Нальчик, 2023 г

1. Область применения

Настоящее Положение регламентирует порядок функционирования и доступа к электронной информационно-образовательной среде при реализации основных профессиональных образовательных программ среднего профессионального образования в Государственном бюджетном профессиональном образовательное учреждение «Кабардино-Балкарский торгово-технологический колледж» (далее-ГБПОУ «КБТТК")

2. Нормативные ссылки

Настоящее Положение разработано в соответствии со следующими нормативными документами:

Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27.07.2006 №152 -ФЗ «О персональных данных»;

Приказ Федеральной службы по надзору в сфере образования и науки от 12.01.2022 № 24 "О внесении изменений в Требования к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети "Интернет" и формату представления информации, утвержденные приказом Федеральной службы по надзору в сфере образования и науки от 14 августа 2020 г. № 831" (Зарегистрирован 20.05.2022 № 68527)

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ от 20 октября 2021 года N 1802 Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" и обновления информации об образовательной организации, а также о признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации (с изменениями на 6 июня 2023 года)

ПРИКАЗ МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ от 14 декабря 2017 года N 1218 О внесении изменений в Порядок проведения самообследования образовательной организации, утвержденный приказом Министерства образования и науки Российской Федерации от 14 июня 2013 г. N 462

ПРИКАЗ МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ от 24 августа 2022 года N 762 Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования (с изменениями на 20 декабря 2022 года);

Уставом ГБПОУ «КБТТК»

Термины и определения

В настоящем Положении применяются термины и определения:

Электронная информационно-образовательная среда - совокупность средств информационно-коммуникационных технологий, квалификации работников, ее использующих и поддерживающих, обеспечивающая:

- доступ к учебным планам, рабочим программам дисциплин, практик, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах;

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;

- индивидуальный учет результатов освоения обучающимися основных профессиональных образовательных программ;

- проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

- формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса;

- взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет».

Электронный информационный ресурс - источник информации, пользование которым возможно только при помощи компьютера или подключенного к нему периферийного устройства.

Электронный образовательный ресурс - учебный материал (контент), представленный в виде гипертекстовой структуры с мультимедиа приложениями, обеспеченной системой навигации по курсу и управления различными его компонентами. Контент - информационно-значимое наполнение курса: текст, графика, мультимедиа. Контент организуется в виде Web-страниц средствами гипертекстовой разметки. Существенными параметрами контента являются его объем, актуальность и релевантность.

Под электронным обучением понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников (Закон об Образования ст. 16).

Под дистанционными образовательными технологиями понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников (Закон об Образования ст. 16).

Функционирование электронной информационно-образовательной среды включает в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся (Закон об Образования ст. 16).

Портфолио - комплект документов, представляющий совокупность индивидуальных достижений обучающегося в различных сферах деятельности (учебная, научно- исследовательская, общественная, культурно-творческая, спортивная).

3. Обозначении и сокращения

В настоящем Положении применяются следующие сокращения:

Краткое наименование ГБПОУ «КБТТК» – Государственное бюджетное профессиональное образовательное учреждение «Кабардино-Балкарский торгово-технологический колледж»;

ЕАИСУ- единая автоматизированная информационная система управления;

ЛК – личный кабинет;

СДО- система дистанционного обучения;

УИ - управление информатизации;

ЭБ- электронная библиотека;

ЭБС- электронная библиотечная система;

ЭИОС- электронная информационно-образовательная среда;

ЭИР- электронный информационный ресурс;

ЭОР- электронный образовательный ресурс.

4. Ответственность и полномочия

4.1. Настоящее Положение утверждается директором ГБПОУ «КБТТК»

4.2. Ответственность за реализацию данного Положения несут- административно-управленческий персонал, педагогические работники.

5. Общие положения

5.1. Настоящее Положение устанавливает:

- Назначение ЭИОС ГБПОУ «КБТТК»;
- составные части;
- требования к техническому, технологическому и телекоммуникационному обеспечению функционирования;
- требования к аутентификации пользователей;
- порядок и формы доступа к ЭОИС ГБПОУ «КБТТК», правила использования ЭИОС под персональными учетными данными (логином и паролем) и ответственность за использование и поддержку ЭОИС;
- способы и порядок поддержки обучающихся и работников ГБПОУ «КБТТК» при использовании ЭИОС;
- порядок и формы доступа;
- порядок фиксации хода образовательного процесса, фиксацию и индивидуальный учет результатов освоения обучающимися ОПОП в ЭИОС;
- порядок и формы доступа к электронным информационным ресурсам, в официальную группу ВКонтакте;
- порядок и формы доступа к личному кабинету обучающегося;
- порядок и форма доступа к электронной библиотечной системе;
- порядок и форма доступа к электронному портфолио обучающегося.

5.2. Настоящее Положение является обязательным для всех обучающихся и работников ГБПОУ «КБТТК», являющихся пользователями ЭОИС и имеющих персональные учетные данные.

6. Назначение ЭИОС

ЭИОС ГБПОУ «КБТТК» обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин, практик, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах;
- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;
- проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;
- формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса;
- взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет».

7. Составные части ЭИОС

7.1. Электронные образовательные ресурсы:

- ЕАИСУ ГБПОУ «КБТТК»
- Официальный сайт ГБПОУ «КБТТК»
- Официальная группа ВКонтакте для обучающихся и работников ГБПОУ «КБТТК»
- Корпоративная почта
- Личный кабинет обучающегося, обеспечивающий фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной

образовательной программы и обеспечивающий взаимодействие между участниками образовательного процесса пользователям электронной информационно-образовательной среды доступ к средствам тестирования, интерактивным дидактическим инструментам обучения

-электронная библиотека ГБПОУ «КБТТК», обеспечивающая доступ (в том числе авторизованный к полнотекстовым документам) к внутренним и внешним ЭИР.

7.2 Электронные образовательные ресурсы:

– база электронных учебно-методических комплексов дисциплин;

– внешние электронные образовательные ресурсы, права пользования которыми приобретаются по подписке или доступны на основе открытых лицензий.

8. Требования к техническому, технологическому и телекоммуникационному обеспечению функционирования ЭИОС ГБПОУ «КБТТК»

8.1. Технические характеристики серверного оборудования удовлетворяют текущим требованиям для одновременной работы всех пользователей, включая всех обучающихся и работников, использующих ЭИОС.

8.2. Все серверное оборудование имеют средства резервирования и восстановления данных.

8.3. Обеспечивается восстановление информации в ретроспективе не менее двух недель.

8.4. Все компьютеры должны быть объединены в высокоскоростную корпоративную вычислительную сеть.

8.5. Для всех обучающихся и работников обеспечен из корпоративной вычислительной сети высокоскоростной (не менее 100 Мбит/с) выход в информационно-телекоммуникационную сеть «Интернет».

8.6. Обеспечивается модульное подключение сервисов в состав ЭИОС.

8.7. Обеспечивается доступ к альтернативным форматам представления содержания электронных курсов (видео-аудио материалы, виртуальные практикумы и лаборатории).

9. Требования к аутентификации пользователей в ЭИОС ГБПОУ «КБТТК»

9.1. Для аутентификации обучающихся и работников в ЭИОС ГБПОУ «КБТТК» используется аутентификация по парольному принципу.

9.2. Обучающиеся, преподаватели и сотрудники, получившие учетные данные для авторизованного доступа в ЭИОС, обязаны хранить их в тайне, не разглашать, не передавать их иным лицам.

10. Порядок и формы доступа к ЭОИС ГБПОУ «КБТТК», правила использования ЭИОС под персональными учетными данными (логином и паролем) и ответственность за использование и поддержку ЭОИС

10.1. Право доступа к ЭИОС имеют все обучающиеся, преподаватели и сотрудники ГБПОУ «КБТТК».

10.2. В случае увольнения работника или отчисления обучающегося, имеющего доступ к ЭИОС, учетная запись пользователя блокируется.

10.3. Основанием для получения обучающимся учетных данных для авторизованного доступа в ЭИОС является приказ о зачислении в ГБПОУ «КБТТК».

11. Способы и порядок поддержки обучающихся и работников ГБПОУ «КБТТК» при использовании ЭИОС

11.1. Каждый обучающийся и работник имеет право получения учебно-методической, технической поддержки при работе с ЭИОС ГБПОУ «КБТТК».

11.2. Учебно-методическую поддержку, разъяснения и консультации по вопросам

использования ЭИР и ЭОР, информационных и телекоммуникационных технологий, входящих в состав ЭИОС, оказывает зав. библиотекой и администратор по ведению ЭИОС

11.3. Учебно-методическая поддержка может быть получена по телефону, путем отправки сообщения на адрес электронной почты, на форум или в системе дистанционного обучения.

12. Порядок и формы доступа к ЕАИСУ ПГУПС

12.1. ЕАИСУ ГБПОУ «КБТТК» обеспечивает фиксацию хода образовательного процесса, фиксацию и индивидуальный учет результатов освоения обучающимися основных профессиональных образовательных программ (результатов текущего контроля успеваемости и промежуточной аттестации обучающихся), обеспечивает формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса.

12.2. ЕАИСУ ГБПОУ «КБТТК» обеспечивает условия функционирования ЭОИС требованиям об информационной безопасности и защите данных посредством настройки параметров аутентификации пользователя и управления правами доступа пользователя к объектам ЕАИСУ ГБПОУ «КБТТК», а также защиты, резервирования и копирования баз данных.

12.3. Право доступа к ЕАИСУ ГБПОУ «КБТТК» имеют все работники из числа профессорско- преподавательского, научного, административно-управленческого и учебно- вспомогательного персонала.

12.4. Форма предоставления доступа - персональный компьютер с выходом в сеть Интернет.

12.5. Предоставление доступа к ЕАИСУ ГБПОУ «КБТТК» осуществляется администратором по ведению ЭИОС

12.6. Администратором по ведению ЭИОС создается учетная запись (логин и пароль) для доступа к рабочему месту работника.

12.7. Личные учетные данные (логины и пароли) направляются на адрес электронной почты соответствующего работника ГБПОУ «КБТТК». Доступ осуществляется с момента получения логина и пароля по электронной почте пользователем.

12.8. В случае увольнения работника, имеющего доступ к ЕАИСУ, зам директора УВР ГБПОУ «КБТТК» в течение одного рабочего дня обязан сообщить администратору по ведению ЭИОС об этом факте с целью блокирования и последующего удаления учетных данных уволенного работника.

13. Порядок фиксации хода образовательного процесса, фиксация и индивидуальный учет результатов освоения обучающимися основных профессиональных образовательных программ в ЭИОС

13.1. Индивидуальный учет результатов освоения обучающимся основных профессиональных образовательных программ осуществляется в ЕАИСУ ГБПОУ «КБТТК».

13.2. К индивидуальному учету результатов освоения обучающимися программ относятся:

- аттестационные ведомости (экзаменационные, зачетные);
- дневник производственной практики;
- отчеты по практике;
- и другие документы.

13.3. В начале экзаменационной сессии работники учебной части формируют ведомости в ЕАИСУ ГБПОУ «КБТТК». Работники учебной части распечатывают

комплекты ведомостей и выдают их преподавателям для проставления отметок и оценок. После заполнения ведомости преподаватель возвращает ее в учебную часть.

13.4. Ввод выставленных отметок и оценок в базу данных ЕАИСУ ГБПОУ «КБТТК» выполняется в установленные сроки уполномоченным сотрудником учебной части:

- аттестационные ведомости: в следующий за сдачей контрольного мероприятия день;
- зачетные ведомости и ведомости по курсовым проектам (работам): в следующий за сдачей контрольного мероприятия день;
- экзаменационные ведомости: в следующий за экзаменом рабочий день;
- индивидуальные ведомости: в следующий за сдачей контрольного мероприятия день.

13.5. Введенные ведомости остаются на хранении в учебной части.

14. Порядок и формы доступа к официальному сайту ГБПОУ «КБТТК»

14.1. Право доступа к официальному сайту ГБПОУ «КБТТК» (https://kbttk.ucoz.ru/) имеют все пользователи ЭОИС.

14.2. Официальный сайт ГБПОУ «КБТТК» позволяет выполнить требования федерального законодательства об обеспечении открытости образовательной организации и обеспечения доступа к учебным планам, рабочим программам дисциплин и практик.

15. Порядок и формы доступа к электронным информационным ресурсам, в официальную группу ВКонтакте

15.1. Право доступа к форуму и официальной группе ВКонтакте ГБПОУ «КБТТК» (https://vk.com/club211280908) имеют все пользователи ЭОИС.

15.2. Форма предоставления доступа -web-интерфейс.

15.3. Для получения доступа к официальной группе ВКонтакте пользователи проходят процедуру авторизации на сайте ВКонтакте.

15.4. Порядок прохождения авторизации размещен на сайте ВКонтакте. Доступ осуществляется с момента авторизации пользователя на сайте ВКонтакте.

16. Порядок и формы доступа к личному кабинету обучающегося

16.1. Право доступа к ЛК имеют обучающиеся и работники ГБПОУ «КБТТК».

16.2. Форма предоставления доступа - web-интерфейс. Предоставление доступа осуществляется УИ.

16.3. Работа обучающихся и работников в личный кабинет осуществляется по авторизованному доступу с использованием личных учетных данных (логин и пароль).

16.4. Присвоение обучающемуся ГБПОУ «КБТТК» учетных данных осуществляется учебной частью.

16.5. Подготовку необходимого набора регистрационных данных для выдачи обучающемуся осуществляет администратор по ведению ЭИОС.

16.6. Основанием для получения обучающимся учетных данных для авторизованного доступа в ЛК является приказ о зачислении в ГБПОУ «КБТТК».

16.7. Учетные данные для авторизованного доступа создаются на основе данных ЕАИСУ ПГУПС и предоставляются обучающимся посредством работников учебной части.

16.8. Учетные данные для доступа работников к ЛК присваивает администратор по ведению ЭИОС.

16.9. Учетные данные работников направляются администратор по ведению ЭИОС на адрес электронной почты работника.

17. Порядок и форма доступа к электронной библиотечной системе

17.1. Право доступа к ЭБС имеют все пользователи ЭИОС ГБПОУ «КБТТК».

17.2. Форма предоставления доступа -web-интерфейс.

17.3. Работа обучающихся и работников в ЭБС осуществляется в режиме авторизованного доступа с использованием личных учетных данных (логин и пароль).

17.4. Порядок подключения пользователей к ЭБС размещается на сайте ЭБС.

17.5. Для получения доступа к ЭБС пользователи ЭИОС (обучающиеся и работники) получают учетные данные от зав.библиотекой и администратором по ведению ЭИОС.

17.6. Для получения доступа к внешним ЭБС, доступ к которым предоставляется по подписке, пользователи ЭИОС проходят процедуру персональной регистрации на странице внешней ЭБС находясь на территории действия ЭИОС ГБПОУ «КБТТК» , либо подключаясь к ней удаленно. В отдельных случаях возможна предварительная регистрация пользователей посредством генерации и передачи обезличенных учетных данных во внешние ЭБС с последующим автоматизированным предоставлением учетных данных пользователям ЭИОС посредством электронной почты или личного кабинета в ЭБС.

17.7. Порядок прохождения персональной регистрации во внешних ЭБС размещается на сайте ЭБС. Доступ предоставляется с момента получения учетных данных пользователем и авторизации пользователя в ЭБС.

17.8. ЭБС обеспечивает доступ к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах.

18. Порядок и форма доступа к электронному портфолио обучающегося

18.1. Портфолио обучающегося формируется по мере получения достижений в различных видах деятельности.

18.2. Портфолио состоит из двух групп данных: данных, формируемых на основании сведений, имеющихся в ЕАИСУ ГБПОУ «КБТТК», и данных, предоставляемых обучающимися.

19. Ответственность за использование информационных ресурсов ЭИОС

Обучающиеся и работники обязаны использовать ресурсы ЭИОС ГБПОУ «КБТТК» с соблюдением авторских прав, не воспроизводить полностью или частично информацию под своим либо иным логином и паролем, не распространять, не переделывать или иным способом модифицировать информацию.

20. Ответственность за сохранность регистрационных данных в ЭИОС

20.1. Обучающиеся или работники, получившие учетные данные для авторизованного доступа в ЭИОС ГБПОУ «КБТТК», обязаны хранить их в тайне, не разглашать, не передавать их иным лицам.

20.2. Обучающиеся и работники несут ответственность за несанкционированное использование регистрационной информации других обучающихся или работников, в частности, за использование других логинов и паролей для входа в ЭИОС ГБПОУ «КБТТК» и осуществление различных операций от имени другого обучающегося и/или работника.

20.3. Обучающиеся и работники несут ответственность за умышленное использование программных средств (вирусов и/или самовоспроизводящегося кода), позволяющих осуществлять несанкционированное проникновение в ЭИОС ГБПОУ «КБТТК» с целью модификации информации, кражи, угадывания паролей, осуществление любого рода коммерческой деятельности и других несанкционированных действий.

20.4. Обучающиеся и работники несут ответственность за использование информационно-телекоммуникационной сети «Интернет» в противоправных

целях, для распространения материалов, оскорбляющих человеческое достоинство и общественную нравственность, пропагандирующих насилие, способствующих разжиганию расовой или национальной вражды, а также рассылку обманных, беспокоящих или угрожающих сообщений.

20.5. В случае невозможности авторизованного входа с первичным или измененным пользователем паролем, в социальную сеть ГБПОУ «КБТТК», в ЭБ ГБПОУ «КБТТК» от своего имени обучающийся или работник обязаны немедленно уведомить администратора по ведению ЭИОС

20.6. Обучающийся или работник обязаны немедленно уведомить администратора по ведению ЭИОС о любом случае несанкционированного доступа и/или о любом нарушении безопасности.

20.7. Колледж имеет право в случае несоблюдения требований Положения запретить использование определенных учетных данных и/или изъять их из обращения.

20.8. За нарушение Положения обучающийся и работник могут быть привлечены к дисциплинарной и гражданско-правовой ответственности в соответствии с действующим законодательством.

20.9. Базы данных ЭИОС ГБПОУ «КБТТК» являются интеллектуальной собственностью Колледжа. В случае нарушения авторских прав обучающиеся и работники несут административную, гражданско-правовую и уголовную ответственность в соответствии с действующим законодательством.

21. Согласование, хранение, рассылка и изменения

Согласование настоящего Положения осуществляется с педагогическим советом колледжа, а также с учетом мнения совета обучающихся.

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ И НАУКИ
КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КАБАРДИНО-БАЛКАРСКИЙ ТОРГОВО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

Утвержден приказом
№ 10-02/208 о/д
от 31.08.2023 г.

РЕГЛАМЕНТ

по выявлению, анализу и устранению критичных уязвимостей в информационных системах в государственном бюджетном профессиональном образовательном учреждении «Кабардино-Балкарский торгово- технологический колледж»

Нальчик, 2023 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах (далее – ИС) эксплуатируемых в государственном бюджетном профессиональном образовательном учреждении «Кабардино-Балкарский торгово-технологический колледж» (далее – Колледж) разработан в соответствии с Руководством по организации процесса управления уязвимостями в органе (организации) утвержденным ФСТЭК России от 17 мая 2023 г. и в соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств утвержденной ФСТЭК России от 28 октября 2022 г.

1.2. Настоящий Регламент подлежит применению операторами информационных систем при принятии ими мер по выявлению, анализа и устранению уязвимостей программных, программно-аппаратных средств информационных систем в соответствии с требованиями о защите информации, содержащейся в государственных ИС, а также иными нормативными правовыми актами и методическими документами ФСТЭК России.

1.3. Выявление, анализ и устранение уязвимостей в сертифицированных программных, программно-аппаратных средствах защиты информации обеспечивается в приоритетном порядке и осуществляется в соответствии с эксплуатационной документацией на них, а также с рекомендациями разработчика.

1.4. В Регламенте используются термины и определения, установленные национальными стандартами ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей», ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» и иными национальными стандартами в области защиты информации и обеспечения информационной безопасности.

Целями регламента являются:

– координация деятельности всех структурных подразделений Колледжа по выявлению, анализу и устранению критичных уязвимостей в ИС;

– создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования ГБПОУ «КБТТК»;

– организация взаимодействия между структурными подразделениями Колледжа по вопросам устранения уязвимостей.

2. ПОРЯДОК ВЫЯВЛЕНИЯ КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

2.1. В ИС должно осуществляться выявление следующих типов уязвимостей:

– недостатки и(или) ошибки программного обеспечения (далее ПО) ИС и ее системы защиты информации (далее – СЗИ).

– недостатки аппаратных средств ИС, в том числе аппаратных средств защиты информации.

– организационно-технические недостатки.

2.2. Непосредственными исполнителями мероприятий по выявлению, анализу и устранению уязвимостей ИС являются администратор безопасности и системные администраторы ИС.

На этапе мониторинга уязвимостей и оценки их применимости осуществляется выявление уязвимостей на основании данных, получаемых из внешних и внутренних источников и принятие решений по их последующей обработке.

Процесс управления уязвимостями организуется для всех ИС Колледжа и должен предусматривать постоянную и непрерывную актуализацию сведений об уязвимостях и объектах ИС. При изменении статуса уязвимостей (применимость к ИС, наличие исправлений, критичность) должны корректироваться способы их устранения.

Процесс управления уязвимостями связан с другими процессами и процедурами деятельности органа (организации):

– мониторинг информационной безопасности – процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей;

– оценка защищенности – анализ возможности использования обнаруженных уязвимостей для реализации компьютерных атак на ИС Колледжа;

– оценка угроз безопасности информации – выявление и оценка актуальности угроз, реализация (возникновение) которых возможна в ИС Колледжа;

– управление конфигурацией – контроль изменений, состава и настроек программного и программно-аппаратного обеспечения ИС;

– управление обновлениями – приобретение, анализ и развертывание обновлений программного обеспечения в Колледже;

– применение компенсирующих мер защиты информации – разработка и применение мер защиты информации, которые применяются в ИС взамен

отдельных мер защиты информации, подлежащих реализации в соответствии с требованиями по защите информации, в связи с невозможностью их применения.

Уровень критичности уязвимостей оценивается в целях принятия обоснованного решения администраторами безопасности о необходимости устранения уязвимостей, выявленных в программных, программно-аппаратных средствах по результатам анализа уязвимостей в ИС.

Исходными данными для определения критичности уязвимостей являются:

– база уязвимостей программного обеспечения, программно-аппаратных средств, содержащаяся в Банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), а также иные источники, содержащие сведения об известных уязвимостях;

– официальные информационные ресурсы разработчиков программного обеспечения, программно-аппаратных средств и исследователей в области информационной безопасности;

– сведения о составе и архитектуре информационных систем, полученные по результатам их инвентаризации и (или) приведенные в документации на информационные системы;

– результаты контроля защищенности информационных систем, проведенные оператором.

Указанные исходные данные могут уточняться или дополняться с учетом особенностей области деятельности, в которой функционируют ИС.

Оценка уровня критичности уязвимостей программных, программно-аппаратных средств проводится администраторами безопасности.

Оценка уровня критичности уязвимостей программных, программно-аппаратных средств применительно к конкретной ИС включает:

– определение программных, программно-аппаратных средств, подверженных уязвимостям;

– определение в информационной системе места установки программных, программно-аппаратных средств, подверженных уязвимостям (например, на периметре системы, во внутреннем сегменте системы, при реализации критических процессов (бизнес-процессов) и других сегментах ИС);

– расчет уровня критичности уязвимости программных, программно-аппаратных средств в ИС.

3. ПОРЯДОК АНАЛИЗА КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

На этапе анализа уязвимостей определяется уровень критичности уязвимостей применительно к ИС Колледжа и осуществляется выявление уязвимостей на основании данных из следующих источников:

а) внутренние источники:

– системы управления информационной инфраструктурой (далее – ИТ - инфраструктура);

– базы данных управления конфигурациями;

– документация на ИС;

– электронные базы знаний органов (организаций);

б) база данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации (далее – БДУ) ФСТЭК России;

в) внешние источники:

– базы данных, содержащие сведения об известных уязвимостях;

– официальные информационные ресурсы разработчиков программных и программно-аппаратных средств и исследователей в области информационной безопасности.

Источники данных могут уточняться или дополняться с учетом особенностей функционирования образовательной организации.

На этапе анализа уязвимостей и оценки их применимости выполняются операции, приведенные в таблице 3.1.

Таблица 3.1

№ п/п	Наименование операции	Описание операции
1	Анализ информации об уязвимости	Анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к информационным системам органа (организации). Агрегирование и корреляция собираемых данных об уязвимостях
2	Оценка применимости уязвимости	На основе информации об объектах информационных систем и их состоянии определяется применимость уязвимости к информационным системам органа (организации) с целью определения уязвимостей, не требующих дальнейшей обработки (не релевантных уязвимостей). Оценка применимости уязвимостей производится: на основе анализа данных об ИТ-инфраструктуре, полученных из баз данных управления конфигурациями в рамках процесса «Управление конфигурацией»; на основе анализа данных о возможных объектах воздействия, полученных в результате

		моделирования угроз в рамках процесса «Оценка угроз»; по результатам оценки защищенности
3	Принятие решений на получение дополнительной информации	Запрос дополнительной информации об уязвимости (сканирование объектов, оценка защищенности), если имеющихся данных недостаточно для принятия решений по управлению уязвимостями
4	Постановка задачи на сканирование объектов	Запрос на внеплановое сканирование объектов информационных систем в случае недостаточности либо неактуальности имеющихся данных, а также в случае получения информации об уязвимости после последнего сканирования
5	Сканирование объектов	Поиск уязвимостей и недостатков с помощью автоматизированных систем анализа защищенности. Выбор объектов и времени сканирования, уведомление заинтересованных подразделений (например, ситуационного центра, подразделения ИТ) о проведении сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
6	Оценка защищенности	Экспертная оценка возможности применения уязвимости к информационным системам. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в информационных системах органа (организации) с использованием средства эксплуатации уязвимости, в том числе, в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации)

На основе таблицы 3.1. в образовательной организации должно разрабатываться детальное описание операций, включающее наименование операций, описание операций, исполнителей, продолжительность, входные и выходные данные. Детальное описание операций включается в организационно-распорядительные документы по защите информации образовательной организации.

4 ПОРЯДОК УСТРАНЕНИЯ КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

4.1. На этапе определения методов и приоритетов устранения уязвимостей определяется приоритетность устранения уязвимостей и выбираются методы их устранения: обновление программного обеспечения и (или) применение компенсирующих мер защиты информации, также принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей.

На этапе определения методов и приоритетов устранения уязвимостей решаются задачи:

– определения приоритетности устранения уязвимостей;

– выбора методов устранения уязвимостей:

–обновление программного обеспечения и (или) применение компенсирующих мер защиты информации.

На этапе определения методов и приоритетов устранения уязвимостей выполняются операции, приведенные в таблице 4.1.

Таблица 4.1

№ п/п	Наименование операции	Описание операции
1	Определение приоритетности устранения уязвимостей	Определение приоритетности устранения уязвимостей в соответствии с результатами расчета критичности уязвимостей на этапе оценки уязвимостей (этап 4)
2	Определение методов устранения уязвимостей	Выбор метода устранения уязвимости: установка обновления или применение компенсирующих мер защиты информации
3	Принятие решения о срочной установке обновлений	При обнаружении критической уязвимости может быть принято решение о срочной установке обновления программного обеспечения объектов информационных систем, подверженных уязвимости
4	Создание заявки на срочную установку обновления	Заявка на срочную установку обновления направляется на согласование руководителю подразделения ИТ
5	Принятие решения о срочной реализации компенсирующих	При обнаружении критической уязвимости может быть принято решение о срочной реализации компенсирующих мер защиты информации в качестве временного решения до установки обновления

	мер защиты информации	
6	Создание заявки на установку обновления	Заявка создается в случае, если определено, что установка обновления для устранения данной уязвимости не запланирована
7	Создание заявки на реализацию компенсирующих мер защиты информации	Заявка на реализацию компенсирующих мер защиты информации формируется при отсутствии возможности установки обновления, а также в случае необходимости принятия мер до устранения уязвимости

На основе таблицы 4.1. в образовательной организации должно разрабатываться детальное описание операций, включающее наименование операций, описание операций, исполнителей, продолжительность, входные и выходные данные. Детальное описание операций включается в организационно-распорядительные документы по защите информации органа (организации).

4.2. На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) уязвимостей, выявленные на этапе мониторинга. При этом выполняются операции, представленные в таблице 4.2.

Таблица 4.2

№ п/п	Наименование операции	Описание операции
1	Согласование установки с руководством подразделения ИТ	Срочная установка обновлений программного обеспечения предварительно согласовывается с руководством подразделения ИТ
2	Тестирование обновления	Выявление потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации (далее – недекларированные возможности)
	Установка обновления в тестовом сегменте	Установка обновлений на выбранном тестовом сегменте информационной системы в целях определения влияния их установки на ее функционирование
	Принятие решения об установке обновления	В случае, если негативного влияния от установки обновления на выбранном сегменте системы не выявлено, принимается решение о его распространении в системе. В случае обнаружения негативного влияния от установки обновления

		на выбранном сегменте системы дальнейшее распространение обновления не осуществляется, при этом для нейтрализации уязвимости применяются компенсирующие меры защиты информации
	Установка обновления	Распространение обновления на объекты информационных систем
	Формирование плана установки обновлений	Уязвимости, для устранения которых не была определена необходимость срочной установки обновлений, устраняются в ходе плановой установки обновлений. Формирование плана обновлений осуществляется с учетом заявок на установку обновлений
	Разработка и реализация компенсирующих мер защиты информации	Разработка и применение мер защиты информации, которые применяются в информационных системах взамен отдельных мер защиты информации, подлежащих реализации в соответствии с требованиями по защите информации, в связи с невозможностью их установки, обнаружением негативного влияния от установки обновления, а также в случае необходимости принятия мер до устранения уязвимости. К компенсирующим мерам защиты информации могут относиться: организационные меры защиты информации, настройка средств защиты информации, анализ событий безопасности, внесение изменений в ИТ - инфраструктуру

Тестирование обновлений программных и программно-аппаратных средств осуществляется в соответствии с Регламентом по выявлению, анализу и устранению критичных уязвимостей в ИС эксплуатируемых в органе, организации, по решению организации в случае отсутствия соответствующих результатов тестирования в БДУ ФСТЭК России.

При наличии соответствующих сведений могут быть использованы компенсирующие меры защиты информации, представленные в бюллетенях безопасности разработчиков программных, программно-аппаратных средств, а также в описаниях уязвимостей, опубликованных в БДУ ФСТЭК России.

Рекомендуемые сроки устранения уязвимостей:

– критический уровень опасности до 24 часов;

– высокий уровень опасности – до 7 дней;

– средний уровень опасности – до 4 недель;

– низкий уровень опасности – до 4 месяцев.

В рамках выполнения подпроцесса разработки и реализации компенсирующих мер защиты информации выполняются операции, приведенные в таблице 4.3.

Таблица 4.3.

№ п/п	Наименование операции	Описание операции
1	Определение мер защиты информации и ответственных за их реализацию	Определение компенсирующих мер защиты информации, необходимых для нейтрализации уязвимости либо снижения возможных негативных последствий от ее эксплуатации. В ходе выполнения данной операции должны быть определены работники, участие которых необходимо для реализации выбранных компенсирующих мер защиты информации
2	Согласование привлечения работников	В случае необходимости привлечения работников других подразделений для реализации компенсирующих мер защиты информации руководитель подразделения защиты согласует их привлечение с руководителями соответствующих подразделений
3	Реализация организационных мер защиты информации	Реализация организационных мер защиты информации предусматривает: ограничение использования ИТ-инфраструктуры; организация режима охраны (в частности, ограничение доступа к техническим средствам); информирование и обучение персонала организации
4	Настройка средств защиты информации	Оценка возможности реализации компенсирующих мер с использованием средств защиты информации, выбор средств защиты информации (при необходимости). Выполнение работ по настройке средств защиты информации
5	Организация анализа событий безопасности	Организация постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления и блокирования попыток эксплуатации уязвимости
6	Внесение изменений в ИТ-инфраструктуру	Внесение изменений в ИТ-инфраструктуру включает действия по внесению изменений в конфигурации программных и программно-аппаратных средств (в том числе, удаление (выведение из эксплуатации))

На основе таблиц 4.2 и 4.3. в образовательной организации должно разрабатываться детальное описание операций, включающее наименование операций, описание операций, исполнителей, продолжительность, входные и выходные данные.

Детальное описание операций включается в организационно-распорядительные документы по защите информации организации.

В случае невозможности получения, установки и тестирования обновлений программных, программно-аппаратных средств принимаются компенсирующие меры защиты информации.

Выбор компенсирующих мер по защите информации осуществляется оператором с учетом архитектуры и особенностей функционирования ИС, а

также способов эксплуатации уязвимостей программных, программно-аппаратных средств.

Компенсирующими организационными и техническими мерами, направленными на предотвращение возможности эксплуатации уязвимостей, могут являться:

– изменение конфигурации уязвимых компонентов ИС, в том числе в части предоставления доступа к их функциям, исполнение которых может способствовать эксплуатации выявленных уязвимостей;

– ограничение по использованию уязвимых программных, программно-аппаратных средств или их перевод в режим функционирования, ограничивающий исполнение функций, обращение к которым связано с использованием выявленных уязвимостей (например, отключение уязвимых служб и сетевых протоколов);

– резервирование компонентов ИС, включая резервирование серверов, телекоммуникационного оборудования и каналов связи;

– использование сигнатур, решающих правил средств защиты информации, обеспечивающих выявление в ИС признаков эксплуатации уязвимостей;

– мониторинг информационной безопасности и выявление событий безопасности информации в ИС, связанных с возможностью эксплуатации уязвимостей.

V. ПОРЯДОК ПРИНЯТИЯ И УТВЕРЖДЕНИЯ РЕГЛАМЕНТА

5.1 Регламент, прошедший правовую и литературную экспертизу, а также процедуру согласования, подлежит принятию и утверждению директором Колледжа в соответствии с Уставом Колледжа.

5.2 Регламенты могут приниматься директором, общим собранием трудового коллектива, педагогическим советом, экспертно-методическим советом, органом государственно-общественного управления (Управляющим советом), либо иным органом, наделенным полномочиями по принятию локальных актов в соответствии с уставом Колледжа - по предметам их ведения и компетенции.

5.3. При принятии Регламента, затрагивающих права обучающихся, учитывается мнение студенческого совета, родительского совета, представительных органов обучающихся.

5.4 Не подлежат применению Регламенты, ухудшающие положение работников по сравнению с трудовым законодательством, коллективным договором, соглашениями, а также локальные акты, принятые с нарушением порядка учета мнения представительного органа работников.

5.5 Прошедший процедуру принятия Регламент утверждается директором Колледжа. Процедура утверждения оформляется либо подписью, либо приказом директора Колледжа.

5.6 Регламент вступает в силу с момента, указанного в нем, либо, в случае отсутствия такого указания, по истечении 7 календарных дней с даты принятия данного локального акта. Датой принятия локального акта, требующего утверждения директором Колледжа, является дата такого утверждения.

5.7 Утвержденные Регламенты размещаются на официальном сайте колледжа.