Приложение

КГЭУ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

УТВЕРЖДЕН
приказом КГЭУ
от 07.08.2025 № 326

ПОРЯДОК

ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ФГБОУ ВО «КГЭУ»

ПРЕДИСЛОВИЕ

РАЗРАБОТАН директором Департамента информационных технологий ФГБОУ ВО «КГЭУ» Беляевым Э.И.

ПРИНЯТ приказом ФГБОУ ВО «КГЭУ» от 07.08.2025 № 326

ВВЕДЕН в действие с 07.08.2025

Периодичность ПЕРЕСМОТРА Порядка по необходимости

Порядок соответствует требованиям ИСО 9001:2015 и СТО СМК УД-16 «Управление документацией»

СОДЕРЖАНИЕ

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий Порядок регламентирует организацию мероприятий по обеспечению информационной безопасности корпоративной информационной системы Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский государственный энергетический университет» (далее – КГЭУ), обеспечивает основу для соблюдения защищенности информации, понимание работниками КГЭУ юридических и этических обязанностей в отношении защиты информации и возможностей собирать, использовать, хранить и распространять информацию соответствующим образом.

2. НОРМАТИВНЫЕ ССЫЛКИ

Порядок разработан в соответствии с:

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»;

Иными нормативными правовыми актами Российской Федерации в регулируемой сфере;

Иными локальными нормативными актами КГЭУ.

3. ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем Порядке используются следующие термины и сокращения:

Аппаратные ресурсы – совокупность технических средств (серверы, рабочие станции, сетевое оборудование и пр.), обеспечивающих обработку, хранение и передачу информации в корпоративной информационной системе КГЭУ.

Инцидент информационной безопасности – событие или совокупность событий, которые привели или могут привести к нарушению конфиденциальности, целостности, доступности информационных ресурсов КГЭУ.

Информационная безопасность – состояние защищённости информационных ресурсов КГЭУ от внутреннего и внешнего несанкционированного доступа, нарушений целостности, конфиденциальности и доступности, обеспечивающее устойчивое функционирование корпоративной информационной системы КГЭУ.

Информационные ресурсы – совокупность данных, документов, цифровых материалов, программных продуктов и информационных систем, созданных, приобретённых или используемых работниками КГЭУ при выполнении должностных обязанностей.

Компонент корпоративной информационной системы – это функционально обособленный программно-аппаратный модуль, входящий в состав

корпоративной информационной системы КГЭУ, предназначенный для цифровизации, сопровождения и поддержки деятельности КГЭУ.

Корпоративная информационная система – это совокупность программно-аппаратных модулей.

Несанкционированный доступ — доступ к информационным ресурсам, системам, данным или техническим средствам КГЭУ, осуществлённый с нарушением установленного порядка или без предоставленных на то прав, в том числе с использованием поддельных учетных данных, уязвимостей программного обеспечения или обхода технических средств защиты.

Программные ресурсы – программное обеспечение (включая операционные системы, прикладные программы, платформы управления обучением и др.), используемое для реализации информационных процессов и предоставления сервисов пользователям.

Тестовый контур – это отдельная, изолированная цифровая среда, в которой можно проводить тестирование программного обеспечения и информационных систем, не влияя на работу корпоративной информационной системы КГЭУ.

КИС – корпоративная информационная система;

ПО – программное обеспечение.

4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. Настоящий Порядок распространяется на все аппаратные, программные и информационные ресурсы входящие в КИС КГЭУ.

4.2. Целью настоящего Порядка является обеспечение состояния защищенности КИС КГЭУ, выражающейся в обеспечении целостности, доступности и конфиденциальности данных, а также их полноты и актуальности.

4.3. Деятельность по защите информации должна проводиться с учетом внешних и внутренних угроз, т.е. в условиях наличия реальных или потенциально возможных событий, действий, процессов или явлений, которые могут нанести ущерб КИС КГЭУ.

4.4. Контроль за обеспечением информационной безопасности КИС КГЭУ осуществляется работниками Департамента информационных технологий КГЭУ (далее – Департамент ИТ).

5. ТРЕБОВАНИЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИС КГЭУ

5.1. Работникам КГЭУ необходимо применять организационные, технические, правовые и иные меры защиты информации, направленные на предотвращение несанкционированного доступа, искажения, утраты и разглашения информации, а также обеспечение стабильной работы КИС КГЭУ при выполнении своих должностных обязанностей.

5.2. Организационные меры обеспечения информационной безопасности КИС КГЭУ включают следующие требования:

5.2.1. Назначение ответственных работников КГЭУ за обеспечение информационной безопасности КИС в каждом структурном подразделении КГЭУ.

5.2.2. Регламентация уровней доступа к КИС КГЭУ.

5.2.3. Ознакомление работников КГЭУ с локальными нормативными актами КГЭУ в области информационной безопасности при приёме на работу.

5.2.4. Регулярное проведение инструктажей и повышения осведомленности в области информационной безопасности работников КГЭУ.

5.2.5. Поддержание соответствующего взаимодействия с заинтересованными профессиональными сообществами и ассоциациями или форумами, проводимыми специалистами по информационной безопасности.

5.3. Технические меры обеспечения информационной безопасности КИС КГЭУ включают следующие требования:

5.3.1. Использование антивирусной и межсетевой защиты, систем мониторинга и анализа событий в КИС КГЭУ для обеспечения информационной безопасности.

5.3.2. Регулярное резервное копирование данных, которые используются при выполнении должностных обязанностей работниками КГЭУ.

5.3.3. Применение технических средств контроля доступа к КИС КГЭУ и аутентификации;

5.3.4. Ограничение физического доступа к серверным и критическим компонентам КИС КГЭУ.

5.4. Иные меры обеспечения информационной безопасности КИС КГЭУ включают следующие требования:

5.4.1. Ведение учёта и инвентаризации информационных и иных ресурсов КИС КГЭУ, которые используются при выполнении должностных обязанностей работниками КГЭУ.

5.4.2. Своевременное обновление ПО и устранение уязвимостей.

5.4.3. Управление доступом осуществляется в соответствии с Порядком доступа работников к информационно – телекоммуникационной сети Интернет и к информационным ресурсам ФГБОУ ВО «КГЭУ».

5.4.4. Проверка и комплексное тестирование ПО и других компонентов КИС КГЭУ осуществляется в тестовом контуре.

5.4.5. Установление и согласование соответствующих требований в области информационной безопасности с каждым поставщиком, который может получить доступ к информационным и иным ресурсам КИС КГЭУ, обрабатывать, хранить, передавать информацию или предоставлять соответствующие компоненты КИС КГЭУ.

6. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ

6.1. Работники КГЭУ имеют право:

6.1.1. Получать необходимую информацию и консультации от работников Департамента ИТ о мерах защиты информации при работе в КИС КГЭУ;

6.1.2. Инициировать мероприятия по защите информации при выявлении потенциальных угроз или инцидентов информационной безопасности.

6.2. Работники КГЭУ обязаны:

6.2.1. Использовать информационные ресурсы КГЭУ только при выполнении своих должностных обязанностей;

6.2.2. Не допускать разглашения имен пользователей, паролей, ключей электронной подписи и другой служебной информации;

6.2.3. В случае инцидентов информационной безопасности незамедлительно сообщать об этом директору Департамента ИТ.

6.3. Работники Департамента ИТ обязаны:

6.3.1. Обеспечивать устойчивое функционирование и информационную безопасность КИС КГЭУ, в том числе администрирование прав доступа, антивирусную защиту, ведение журналов инцидентов;

6.3.2. Своевременно обновлять ПО и закрывать уязвимости, выявленные в ходе эксплуатации КИС КГЭУ;

6.3.3. Проводить регулярный контроль соблюдения требований информационной безопасности.

6.4. Работники КГЭУ несут персональную ответственность за действия, повлекшие нарушение информационной безопасности КИС КГЭУ.

6.5. Нарушение требований, установленных настоящим Порядком, может повлечь дисциплинарную, административную или иную ответственность в соответствии с законодательством Российской Федерации и локальными нормативными актами КГЭУ.

7. РЕГИСТРАЦИЯ И ХРАНЕНИЕ ПОРЯДКА

7.1. Настоящий Порядок регистрируется в Оргдепартаменте.

7.2. Оригинальный экземпляр настоящего Порядка хранится в Оргдепартаменте до его замены в установленном порядке.

7.3. Заверенная копия Порядка хранится в составе документов Департамента ИТ и выставляется в разделе структурного подразделения на официальном сайте.

Разработал:
Директор Департамента ИТ Э.И. Беляев

ЛИСТ ОЗНАКОМЛЕНИЯ

С настоящим Порядком ознакомлен и принял к исполнению:

1 _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

2. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

3. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

4. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

5. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

6. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

7 _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

8. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

9. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

10. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

11. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

12. _____
(*Должность*)

_____ _____
(*Подпись*) (*И.О.Фамилия*)

_____
(*Дата*)

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номера листов (страниц)			Всего листов в документе	Ф.И.О. и подпись лица, внесшего изменение	Дата
	замененных	новых	изъятых			