МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное
образовательное учреждение высшего образования
«Казанский национальный исследовательский
технологический университет»
(ФГБОУ ВО «КНИТУ»)

ПРИКАЗ

30.11.2021 № 889-О

Об утверждении политики информационной безопасности

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» п р и к а з ы в а ю:

1. Утвердить политику информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (Приложение № 1).

2. Утвердить перечень документов политики информационной безопасности второго и третьего уровня (Приложение № 2).

3. Утвердить регламент реагирования на инциденты безопасности в ФГБОУ ВО «КНИТУ» (Приложение № 3).

4. Утвердить Положение об антивирусной защите в ФГБОУ ВО «КНИТУ» (Приложение № 4).

5. Утвердить Положение об использовании программного обеспечения в ФГБОУ ВО «КНИТУ» (Приложение № 5).

6. Утвердить Положение по использованию электронной почты в ФГБОУ ВО «КНИТУ» (Приложение № 6).

7. Утвердить Положение по использованию локальной сети и сети Интернет в ФГБОУ ВО «КНИТУ» (Приложение № 7).

8. Контроль за исполнением настоящего приказа возложить на проректора по РБ Муратова А.Х.

Врио ректора Ю.М. Казаков

Приложение № 1
к приказу ФГБОУ ВО «КНИТУ»
от __30.11.2021__ № ___889-о_____

Политика информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет»

Область применения

Политика информационной безопасности (далее – Политика) федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (далее – КНИТУ) представляет систему установленных в КНИТУ целей, принципов, основных направлений и задач по обеспечению информационной безопасности, включая противодействие угрозам информационной безопасности, защиту информации, циркулирующей в компьютерных и телекоммуникационных сетях, и входит составной частью в политику информационной безопасности КНИТУ.

Настоящий документ является решением руководства КНИТУ об осуществлении целенаправленной систематической деятельности по обеспечению информационной безопасности КНИТУ и является документом верхнего уровня Политики.

Документы Политики информационной безопасности среднего уровня, непосредственно детализирующие требования, задачи и правила, обозначенные в Политике, и отдельно описывающие основные сферы, в которых необходимо системное осуществление тех или иных организационных и/или технических мероприятий, а также детализированные документы политики информационной безопасности третьего уровня, перечислены в Приложении №2 к приказу.

Положения Политики распространяются на деятельность КНИТУ в области защиты конфиденциальной информации (в том числе персональных данных) и не затрагивают вопросы защиты информации, составляющей государственную тайну Российской Федерации, а также служебной информации ограниченного распространения с пометкой «Для служебного пользования».

Положения настоящей Политики обязательны для соблюдения всеми работниками КНИТУ, контрагентами, партнерами и организациями, допущенными к информации и информационной инфраструктуре КНИТУ на законных основаниях.

Нормативные ссылки

В Политике использованы нормативные ссылки на следующие документы:

2.1. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

2.2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

2.3. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

2.4. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Термины и определения

В Политике применены следующие термины с соответствующими определениями:

Информационная безопасность КНИТУ (далее – информационная безопасность): состояние защищенности компьютерных и телекоммуникационных сетей КНИТУ от внутренних и внешних информационных угроз, при котором обеспечивается реализация прав работников, достижение уставных целей, функционирование и устойчивое социально-экономическое развитие КНИТУ.

Информационная инфраструктура КНИТУ: совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и корпоративных компьютерных сетей связи КНИТУ.

Информационная система: совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [по ГОСТ Р 50922-2006].

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

Информационные технологии: процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Инцидент информационной безопасности: появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации

бизнес-операций и создания угрозы информационной безопасности [по ГОСТ Р ИСО/МЭК ТО 18044-2007].

Корпоративная компьютерная сеть: информационно-телекоммуникационная сеть, объединяющая локальные вычислительные сети КНИТУ и обеспечивающая обмен информацией между ними.

Обеспечение информационной безопасности: осуществление взаимоувязанных правовых, организационных, исследовательских, технических, информационно-аналитических, кадровых, экономических, физических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению угроз информации, циркулирующей в компьютерных и телекоммуникационных сетях и ликвидации последствий их проявления.

Риск информационной безопасности: возможность того, что имеющаяся угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации [по ГОСТ Р ИСО/МЭК 27005-2010].

Силы обеспечения информационной безопасности: руководство, подразделения и работники КНИТУ, уполномоченные на решение задач по информационной безопасности, а также организации и иные лица, выполняющие на основании гражданско-правовых договоров задачи по обеспечению информационной безопасности.

Система обеспечения информационной безопасности: совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

Средства обеспечения информационной безопасности: правовые, организационные, технические и иные средства, используемые силами обеспечения информационной безопасности.

Угроза информационной безопасности: совокупность действий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности или доступности информации [по ГОСТ Р 50922-2006].

Общие положения

КНИТУ является образовательной организацией высшего образования, осуществляющей в качестве основной цели её деятельности образовательную деятельность по программам высшего образования и научную деятельность, созданной для осуществления образовательных, научных, социальных и иных функций некоммерческого характера.

Основными видами деятельности КНИТУ являются:

1) образовательная деятельность по образовательным программам высшего образования и среднего профессионального образования, основным и дополнительным общеобразовательным программам, дополнительным профессиональным программам, а также основным программам профессионального обучения;

2) научная деятельность;

3) организация проведения общественно значимых мероприятий в сфере образования, науки и молодежной политики.

Информационные технологии приобрели всеобъемлющий характер и стали неотъемлемой частью всех направлений деятельности КНИТУ. Их эффективное развитие и применение является важнейшим фактором развития КНИТУ.

Информационная инфраструктура играет важную роль в реализации приоритетных направлений деятельности КНИТУ.

Руководство КНИТУ определяет, что компьютерная информация, информационная инфраструктура, применяемые информационные технологии являются важнейшими активами, которые нуждаются в обеспечении информационной безопасности.

Интересами КНИТУ в информационной сфере являются:

– обеспечение и защита прав и свобод работников КНИТУ в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение безопасности персональных данных;

– обеспечение устойчивого и непрерывного функционирования информационной инфраструктуры, в первую очередь корпоративной компьютерной сети;

– совершенствование деятельности учебных, научных административных, хозяйственных и эксплуатационных подразделений КНИТУ по выполнению норм и правил информационной безопасности, повышение профессионального уровня работников в области использования информационных технологий и обеспечения информационной безопасности;

– содействие формированию системы информационной безопасности Российской Федерации, участие в деятельности государственной системы обнаружения, предупреждения и ликвидации последствий информационных атак на информационные ресурсы Российской Федерации на правах рабочей группы противодействия атакам на информационные ресурсы КНИТУ.

Деятельность КНИТУ в области обеспечения информационной безопасности включает выполнение в практической деятельности требований:

– законодательства Российской Федерации в области безопасности информационных технологий и защиты информации, безопасности персональных данных;

– нормативных правовых актов федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, технической защиты информации, противодействия компьютерной разведке.

Реализация интересов в информационной сфере направлена на формирование информационной инфраструктуры, устойчивой к всевозможным видам воздействия, и создание безопасной среды оборота информации в целях обеспечения непрерывного функционирования учебного процесса, научной деятельности и решения административно-хозяйственных и финансовых задач.

Для реализации Политики в КНИТУ создано структурное подразделение информационной безопасности – центр компьютерной безопасности КНИТУ, а также назначаются уполномоченные лица (администраторы безопасности). На центр компьютерной безопасности возлагаются задачи по организации и координации работ в области информационной безопасности, определению и реализации мероприятий по защите информации, циркулирующей в компьютерных и телекоммуникационных сетях, противодействию компьютерным техническим разведкам, а также контролю за состоянием информационной безопасности в ходе образовательной, научной, административной и хозяйственной деятельности КНИТУ.

На управление информационных технологий, центр компьютерной безопасности, системных администраторов информационных систем (ИС) возлагаются задачи по внедрению, администрированию, технической эксплуатации и сопровождению на всех этапах жизненного цикла комплексов технических и аппаратно-программных средств, обеспечивающих защиту информации циркулирующей в компьютерных и телекоммуникационных сетях КНИТУ.

Процесс обеспечения информационной безопасности строится на основе разграничения полномочий и обязанностей структурных подразделений КНИТУ в данной сфере с учетом функциональных (должностных) обязанностей.

Политика информационной безопасности КНИТУ подлежит регулярному пересмотру начальником центра компьютерной безопасности и специалистами управления информационных технологий (не реже одного раза в три года), или раньше, если произошли значительные изменения, с

целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

Риски и угрозы информационной безопасности

Расширение областей и масштаба применения информационных технологий, применение большого количества технических средств и программного обеспечения (ПО) импортного производства сопровождается появлением новых уязвимостей информационных систем КНИТУ и связанных с этими уязвимостями рисками информационной безопасности.

Настоящая Политика учитывает наличие внешних и внутренних рисков и угроз информационной безопасности.

Внешние риски и угрозы обусловлены социально-экономическими и научно-техническими процессами и отношениями, развивающимися в мире и Российской Федерации вне сферы деятельности КНИТУ. Источниками внешних рисков информационной безопасности могут являться политическая и экономическая ситуация в стране и в мире, изменения федерального законодательства, обострение криминогенной обстановки («киберпреступность»), террористические акты, природные и техногенные явления.

Внутренние риски и угрозы обусловлены процессами и отношениями, складывающимися в КНИТУ, в их структурных подразделениях. Источниками внутренних рисков и угроз, прежде всего, служат:

– нарушения требований нормативных документов по информационной безопасности, принятых в КНИТУ;

– ошибки и уязвимости в работе ПО;

– отказы и сбои в работе средств вычислительной техники;

– возможное субъективное толкование требований нормативных документов и соответствующее их ошибочное правоприменение;

– низкая осведомленность работников в вопросах обеспечения информационной безопасности;

– деструктивные действия пользователей ИС, в том числе обладающих административными правами в ИС.

Для КНИТУ актуальны следующие группы рисков, влияющие на состояние информационной безопасности:

административно – правовые: связаны с изменением правового регулирования процессов обработки информации в компьютерных и телекоммуникационных сетях, необходимостью существенного изменения режимов обеспечения безопасности ИС;

экономические: связаны с изменением условий (рост цен, санкции) осуществления закупок оборудования и ПО (лицензий), услуг по техническому сопровождению и поддержке;

технологические: связаны с возникновением чрезвычайных ситуаций природного или техногенного характера, в том числе с возможными нарушениями правил эксплуатации и применения ИС;

информационные: связаны с развитием информационных технологий и созданием средств, способных преодолеть существующую защиту конфиденциальной информации и информационной инфраструктуры КНИТУ от несанкционированного доступа, уничтожения, блокирования, модифицирования и иных неправомерных действий информационного воздействия на информационную инфраструктуру, а также формирующих угрозу функционированию АС, в т.ч. с использованием технологий удаленного доступа;

кадровые: связаны с недобросовестным исполнением или неисполнением работниками своих должностных обязанностей, нарушением ими требований нормативных документов, с совершением противоправных действий, наносящих ущерб КНИТУ;

криминальные: связаны с преступными посягательствами на законные интересы КНИТУ в информационной сфере, хищением информации и средств вычислительной техники;

Основные угрозы информационной безопасности, характерные для КНИТУ:

Утечка и кража конфиденциальной информации (персональных данных), использование которой может облегчить организацию противоправных действий в отношении профессорско-преподавательского состава, работников и студентов.

Осуществление целевых, вирусных, компьютерных и прочих атак (спам, фишинг и др.) на информационную инфраструктуру КНИТУ хакерами.

Осуществление разведывательной деятельности иностранных государств (техническая компьютерная разведка).

Случайные (ошибочные) действия работников КНИТУ, а также представителей контрагентов, партнеров и иных организаций, допущенных к информации и информационной инфраструктуре КНИТУ на законных основаниях.

Действия злоумышленников и совершение работниками КНИТУ правонарушений в области информационной безопасности.

Недостаточный уровень конкуренции отечественного рынка информационных технологий, разработок ПО и аппаратных средств, и как следствие, высокая степень зависимости от иностранных производителей, в

ПО и аппаратных средствах в которых возможно проявление недекларируемых свойств.

Цели и основные направления обеспечения информационной безопасности

Основными целями КНИТУ в сфере обеспечения информационной безопасности являются:

Защита работников КНИТУ от возможного нанесения им материального, морального или иного ущерба посредством неправомерного использования касающейся их информации, в том числе персональных данных.

Защита и поддержка позитивного имиджа и деловой репутации КНИТУ в информационной сфере.

Поддержка инновационного и ускоренного развития информационной безопасности и информационных технологий в КНИТУ.

Минимизация вероятного ущерба от реализации угроз информационной безопасности.

Для достижения целей обеспечения информационной безопасности в КНИТУ осуществляется деятельность по следующим основным направлениям:

Обеспечение личной защищенности каждого работника в информационной сфере, в том числе за счет формирования культуры личной информационной безопасности.

Планирование деятельности по обеспечению информационной безопасности с учетом минимизации негативных воздействий на информацию, информационную инфраструктуру и применяемые в КНИТУ информационные технологии.

Развитие комплексной системы информационной безопасности в части взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Замещение импортного ПО и аппаратных средств на конкурентоспособное ПО и аппаратные средства отечественного производства.

Проектирование, строительство объектов информатизации изначально устойчивых к различным видам воздействия, с использованием современных и перспективных средств защиты информации и с учетом реализации политики импортозамещения.

Развитие кадрового потенциала КНИТУ в области обеспечения информационной безопасности и применения информационных технологий.

Применение, при необходимости, средств криптографической защиты информации с учетом требований и рекомендаций ФСБ России.

Уменьшение вероятности реализации угроз информационной безопасности на основе систематического аудита информационных систем, КНИТУ.

Прогнозирование, обнаружение и оценка информационных угроз с целью последовательного совершенствования методов, систем и средств защиты информации.

Основные принципы обеспечения информационной безопасности

В своей деятельности по обеспечению информационной безопасности КНИТУ руководствуется следующими принципами:

Законность – обеспечение информационной безопасности КНИТУ основывается на соблюдении требований Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, Устава КНИТУ, локальных нормативных актов КНИТУ, положений национальных и международных стандартов в области обеспечения информационной безопасности.

Централизация – единство организационного построения, управления системой обеспечения информационной безопасности. Вовлеченность руководства КНИТУ в процесс управления системой обеспечения информационной безопасности.

Экономическая целесообразность – сопоставимость затрат на обеспечение информационной безопасности и возможных потерь от реализации вероятных угроз информационной безопасности.

Достаточность сил и средств обеспечения информационной безопасности – способность системы обеспечения информационной безопасности выявить и предотвратить реализацию угроз безопасности, направленных на информационную инфраструктуру КНИТУ.

Профессионализм – привлечение к разработке и осуществлению мероприятий по обеспечению информационной безопасности профессионально подготовленных лиц и организаций, имеющих необходимые лицензии и квалификацию. Постоянная работа по повышению квалификации специалистов по информационной безопасности и осведомленности работников КНИТУ в вопросах обеспечения информационной безопасности, проведение профилактических мероприятий в структурных подразделениях КНИТУ.

Комплексность – системное осуществление взаимоувязанных правовых, организационных, исследовательских, технических,

информационно-аналитических, кадровых, физических (охранных) и иных мероприятий по обеспечению информационной безопасности.

Непрерывность – постоянное функционирование системы обеспечения информационной безопасности в целях обеспечения непрерывности научных и учебных процессов КНИТУ, учет требований информационной безопасности на всех этапах жизненного цикла ИС.

Своевременность – снижение времени реагирования на инциденты информационной безопасности, предотвращение деструктивных воздействий на компьютерные и телекоммуникационные сети путем внедрения современных и перспективных средств и систем защиты информации.

Минимизация полномочий – предоставление минимально необходимых полномочий и прав доступа к информации в соответствии с выполняемыми должностными обязанностями.

Персональная ответственность – работники КНИТУ должны обеспечивать информационной безопасность в рамках своей компетенции и несут персональную ответственность за нарушение требований информационной безопасности, режима безопасности персональных данных, правил электронного документооборота, эксплуатации ИС и обработки информации на средствах вычислительной техники. Ответственность за нарушение указанных требований включается в трудовые договоры и должностные инструкции работников, а также в договоры (соглашения) с контрагентами.

Задачи системы обеспечения информационной безопасности

Задачами КНИТУ в рамках деятельности, связанной с достижением целей обеспечения информационной безопасности, являются:

Обеспечение защиты информации (сведения, используемые в текущей деятельности, сведения, составляющие конфиденциальные сведения (персональные данные), защищаемые в соответствии с законодательством Российской Федерации), обладателем которой является КНИТУ, от несанкционированного доступа, уничтожения, блокирования, модифицирования и иных неправомерных действий в информационной и телекоммуникационных сетях.

Обеспечение информационной безопасности КНИТУ при взаимодействии с федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, средствами массовой информации, общественными организациями и контрагентами.

Проведение системного анализа угроз информационной безопасности и оценки рисков их реализации.

Осуществление правового и организационного регулирования деятельности по обеспечению информационной безопасности.

Развитие системы обеспечения информационной безопасности путём выбора экономически обоснованных технических, организационных решений и мероприятий.

Обеспечение оперативного выявления и реагирования на инциденты информационной безопасности, а также проведения мероприятий по ликвидации их последствий.

Реализация мероприятий по защите персональных данных в соответствии с требованиями федерального закона «О персональных данных» в объеме их защиты в информационных системах персональных данных.

Развитие инфраструктуры открытых ключей электронных подписей с целью создания возможности придать электронному документообороту юридическую значимость, с использованием технологий электронной подписи и шифрования в соответствии с требованиями федерального закона «Об электронной подписи».

Снижение зависимости от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет применения средств защиты информации российской разработки.

Создание учебно-методической базы для повышения уровня профессиональной подготовки работников подразделений информационной безопасности и качества выполнения ими своих функциональных обязанностей по обеспечению информационной безопасности.

Обучение и повышение осведомленности работников КНИТУ в вопросах информационной безопасности.

Контроль за состоянием информационной безопасности в КНИТУ.

Осуществление контроля за деятельностью пользователей, в том числе обладающих административными правами.

Оценка эффективности комплекса проводимых мер по обеспечению информационной безопасности.

Организационные основы обеспечения информационной безопасности

Правовую основу Политики составляют Конституция Российской Федерации, федеральные законы, Доктрина информационной безопасности Российской Федерации, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, нормативно-правовые документы по вопросам технической защиты информации ФСТЭК России и ФСБ России, положения Устава КНИТУ.

Настоящая Политика является основой для формирования и развития взаимодействия между подразделениями КНИТУ в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

КНИТУ, являясь участниками системы обеспечения информационной безопасности Российской Федерации, в соответствии с законодательством Российской Федерации участвует в решении задач по обеспечению информационной безопасности.

Каждый работник КНИТУ должен знать свою роль и обязанности по обеспечению информационной безопасности, обладать полномочиями по использованию информации, с учетом разграничения прав доступа к информационным активам КНИТУ.

Каждый работник КНИТУ должен знать и выполнять требования информационной безопасности, принятые КНИТУ. Ответственность за неисполнение указанных требований определяется в положениях о структурных подразделениях и должностных инструкциях работников КНИТУ.

Приложение № 2
к приказу ФГБОУ ВО «КНИТУ»
от _30.11.2021____ № __889-о____

I. Перечень документов политики информационной безопасности (второй уровень)

1. Положение о группе обеспечения функционирования и безопасности криптографических средств защиты информации (введено в действие приказом ректора от 26.08.2019 №588-о);
2. Инструкция по обеспечению функционирования и безопасности криптографических средств в информационных системах федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (введена в действие приказом ректора от 26.08.2019 №588-о);
3. Инструкция по обращению со средствами криптографической защиты информации в информационных системах федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (введена в действие приказом ректора от 26.08.2019 №588-о);
4. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи в ФБГОУ ВО «КНИТУ» (введено в действие приказом ректора от 21.08.2019 № 583-о);
5. Регламент реагирования на инциденты компьютерной безопасности в ФГБОУ ВО «КНИТУ» (Приложение №3);
6. Положение о рабочей группе по противодействию компьютерным атакам (введено в действие приказом ректора от 17.06.2020 № 308-о, уточнено приказом ректора от 18.03.2021 № 218-о);
7. Положение по организации парольной защиты в информационных системах федерального государственного бюджетного образовательного учреждения высшего образования «Казанского национального исследовательского университета» (введено в действие приказом ректора от 07.09.2020 №18-од);
8. Положение об антивирусной защите в ФГБОУ ВО «КНИТУ» (Приложение №4);
9. Положение об использовании программного обеспечения в ФГБОУ ВО «КНИТУ» (Приложение №5);
10. Положение по использованию электронной почты в ФГБОУ ВО «КНИТУ» (Приложение №6);
11. Положение по использованию локальной сети и сети Интернет в ФГБОУ ВО «КНИТУ» (Приложение №7).

II. Перечень документов детализированной политики компьютерной безопасности (третий уровень)

1. Инструкция пользователей средств криптографической защиты информации в информационных системах федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (введена в действие приказом ректора от 26.08.2019 №588-о);

2. Инструкция пользователя средствами электронной подписи (введена в действие приказом ректора от 21.08.2019 №583-о).

Приложение № 3
к приказу ФГБОУ ВО «КНИТУ»
от __30.11.2021___ № ____889-о____

РЕГЛАМЕНТ
реагирования на инциденты компьютерной безопасности в ФГБОУ ВО «КНИТУ»

1.Общие положения

1.1. Настоящий Регламент устанавливает порядок разбирательства и составления заключений по фактам несоблюдения условий хранения машинных носителей информации, несоблюдения правил использования средств защиты информации, которые могут привести (или привели) к нарушению конфиденциальности, целостности и доступности информации или другим нарушениям в компьютерных и телекоммуникационных сетях, приводящим к снижению уровня защищенности, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления, разбирательства и предотвращения иных инцидентов компьютерной безопасности в ФГБОУ ВО «КНИТУ» (далее – КНИТУ).

1.2. Регламент разработан в соответствии с 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", федеральным законом от 27.12.2002 № 184-ФЗ "О техническом регулировании", Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", национальным стандартом ГОСТ ИСО/МЭКТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

1.3. Настоящий Регламент разработан для реагирования на инциденты в компьютерных и телекоммуникационных сетях КНИТУ не обрабатывающих сведения, отнесенные к государственной тайне и/или к служебной информации ограниченного распространения (ДСП), и обязателен к соблюдению всеми работниками КНИТУ, участвующими в выявлении, разбирательстве и предотвращении инцидентов компьютерной безопасности (далее – КБ).

1.4. Разбирательство по всем инцидентам КБ проводится центром компьютерной безопасности (ЦКБ) с привлечением в необходимых случаях руководителей и сотрудников других подразделений.

1.5. Разбирательство инцидентов КБ, затрагивающих два или более подразделения КНИТУ, проводится ЦКБ с привлечением сотрудников и руководителей соответствующих подразделений.

Сокращения

АРМ – автоматизированное рабочее место;
ИТ – информационные технологии;
КБ – компьютерная безопасность;
ИР - Информационные ресурсы;
DDoS-атака (от англ. Distributed Denial of Service) – распределенная атака типа «отказ в обслуживании»;
DoS-атака (от англ. Denial of Service) – атака типа «отказ в обслуживании»;
ЦКБ - центр компьютернбой безопасности.

1.6. Реагирование на возникающие чрезвычайные ситуации (инциденты), связанные с нарушением компьютерной безопасности, является таким же важным направлением работы, как и построение системы защиты и предотвращения нарушений.

Инцидент компьютерной безопасности - какое-либо отклонение от нормального процесса использования информационных ресурсов и функционирования информационных систем, повлекшее ущерб для определенных информационных активов КНИТУ или непосредственно создающее угрозу нанесения такого ущерба.

Внутренний инцидент – инцидент, источником которого является нарушитель, связанный с КНИТУ непосредственным образом (трудовым договором или иным способом). Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- утечка персональных данных циркулирующих в компьютерных или телекоммуникационных сетях;
- неправомерный доступ к информации;
- несанкционированное удаление информации;
- компрометация информации;
- мошенничество с помощью ИТ;
- аномальная сетевая активность;
- аномальное поведение бизнес-приложений;
- использование активов КНИТУ в личных целях или в мошеннических операциях.

Внешний инцидент – инцидент, источником которого является нарушитель, не связанный с КНИТУ непосредственным образом. Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);
- перехват и подмена трафика;

- фишинг (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям);
- взлом, попытка взлома, сканирование портала КНИТУ;
- сканирование сети, попытка взлома сетевых узлов;
- вирусные атаки;
- неправомерный доступ к конфиденциальной информации.

2. Выявление инцидента компьютерной безопасности

2.1. Основными источниками информации об инцидентах КБ являются:
- факты, выявленные руководителем структурного подразделения КНИТУ, администратором безопасности – лицом, назначенным ответственным за информационную безопасность приказом ректора КНИТУ, а также другими сотрудниками организации.
- результаты работы средств мониторинга КБ, результаты проверок и аудита (внутреннего или внешнего);
- журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;
- обращения субъектов защищаемой информации с указанием инцидента КБ;
- запросы и предписания органов надзора за соблюдением прав субъектов защищаемой информации;
- другие источники информации.

2.2. Основными видами инцидентов КБ в КНИТУ могут являться:
- разглашение конфиденциальной или внутренней информации, либо угроза такого разглашения;
- несанкционированный доступ - доступ лиц, которые не имеют легального доступа к ресурсам КНИТУ;
- превышение полномочий - несанкционированный доступ к каким-либо ресурсам сотрудников КНИТУ;
- компрометация учетных записей или паролей;
- вирусная атака или вирусное заражение;
- нарушение или сбои в работе системы резервного копирования;
- нарушение правил использования защищаемой информации и персональных данных.

2.3. Администратор безопасности может выявить признаки наличия инцидента КБ путем анализа текущей ситуации на предмет ее соответствия требованиям защиты информации. Выявление несоответствий дают основания предполагать факт возникновения инцидента КБ. Любые сведения

о происшествие или инциденте КБ должны быть незамедлительно переданы выявившим их сотрудником администратору безопасности или в ЦКБ.

3. Анализ исходной информации и принятие решения о проведения разбирательства

3.1. Администратор безопасности после получения информации о предполагаемом инциденте КБ незамедлительно проводит первоначальный анализ полученных данных и докладывает начальнику ЦКБ. В процессе анализа администратор безопасности проводит проверку наличия в выявленном факте нарушений.

3.2. По усмотрению начальника ЦКБ единичный инцидент КБ, не приведший к негативным последствиям и совершенный сотрудником впервые, фиксируется в карточке данных об инциденте компьютерной безопасности (приложение №1) с присвоением статуса «Разбирательство не требуется»

3.4. В случае наличия признаков инцидента КБ, приведшего к негативным последствиям, администратор безопасности классифицирует инцидент, определяет предварительную степень важности инцидента КБ и принимает решение о необходимости проведения разбирательства, информирует начальника ЦКБ об инциденте КБ который инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

3.5. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте КБ, начальник ЦКБ по согласованию с руководителем соответствующего подразделения определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

4. Разбирательство инцидента компьютерной безопасности

4.1.Цели и этапы разбирательства инцидента КБ:

4.1.1. Целями разбирательства инцидентов КБ являются:

- выработка организационных и технических решений, направленных на снижение рисков нарушения компьютерной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
- защита прав КНИТУ, установленных законодательством Российской Федерации;
- защита репутации КНИТУ и ее информационных ресурсов;
- обеспечение безопасности защищаемой информации;
- обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых в КНИТУ;

- предотвращение несанкционированного доступа к конфиденциальной информации, и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Разбирательство инцидента КБ, состоит из следующих этапов:

- подтверждение/опровержение факта возникновения инцидента КБ;
- классификация инцидента КБ;
- подтверждение/корректировка уровня значимости инцидента КБ;
- уточнение дополнительных обстоятельств (деталей) инцидента КБ;
- получение (сбор) доказательств возникновения инцидента КБ, обеспечение их сохранности и целостности;
- минимизация последствий инцидента КБ;
- информирование и консультирование персонала КНИТУ по действиям обнаружения, устранения последствий и предотвращения инцидентов КБ;
- переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил КБ.

4.2. Порядок проведения разбирательства инцидента КБ:

4.2.1. В процессе проведения разбирательства инцидента КБ обязательными для установления являются:

- дата и время совершения инцидента КБ;
- ФИО, должность и подразделение нарушителя КБ;
- классификация инцидента;
- уровень критичности инцидента КБ;
- обстоятельства и мотивы совершения инцидента КБ;
- информационные ресурсы, затронутые инцидентом КБ;
- характер и размер реального и потенциального ущерба;
- обстоятельства, способствовавшие совершению инцидента КБ.

4.2.2. При инциденте КБ, затрагивающем не более одного структурного подразделения, ЦКБ информирует о факте инцидента руководителя соответствующего структурного подразделения.

4.2.3. При инциденте КБ, затрагивающим более одного структурного подразделения, ЦКБ информирует руководителей соответствующих подразделений и инициирует проведение разбирательства.

4.2.4. В случае проведения временного отключения прав доступа у предполагаемого нарушителя КБ информация об отключении прав доступа ЦКБ направляет руководителю предполагаемого нарушителя КБ.

4.2.5. ЦКБ в процессе проведения расследования инцидента КБ при необходимости запрашивает информацию в структурных подразделениях, запрос направляется на имя руководителя подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

4.2.6. После получения необходимой информации по инциденту КБ осуществляющий разбирательство ЦКБ проводит анализ полученных данных.

4.2.7. В течение 5 (пяти) рабочих дней с момента выявления инцидента КБ администратор КБ запрашивает у руководителя структурного подразделения объяснительную записку нарушителя КБ. Объяснительная записка должна быть составлена, подписана нарушителем в течение двух рабочих дней и представлена его непосредственным руководителем в ЦКБ в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа нарушителя предоставить объяснительную записку, начальник ЦКБ (руководитель подразделения нарушителя) составляет акт об отказе дать объяснительную записку. В акте необходимо указать причину, по которой запрашивались объяснения, а также указание на то, что объяснения не были даны. Такой акт составляется комиссией не менее трех человек. С актом нарушитель должен быть ознакомлен под роспись. Если нарушитель ставить свою подпись в акте отказался, то необходимо этот факт отказа отразить в акте.

4.2.8. ЦКБ совместно с заинтересованными подразделениями проводит оценку негативных последствий от реализации инцидента КБ. В ходе данной оценки учитываются;

- прямой финансовый ущерб;
- репутационный ущерб;
- потенциальный ущерб;
- косвенные потери, связанные с недоступностью сервисов, потерей информации;
- другие виды ущерба или аспекты негативных последствий для КНИТУ или субъектов защищаемой информации.

4.2.9. С целью минимизации последствий инцидента КБ возможно временное отключение прав доступа сотрудника к информационным ресурсам (ИР) на время проведения расследования. Подобное отключение инициируется ЦКБ с обязательным предварительным устным согласованием с руководителем сотрудника.

4.2.10. В случае, если у нарушителя КБ были отключены права доступа к ИР на время проведения разбирательства, то по его результатам ЦКБ по согласованию с руководителем нарушителя КБ принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имеющихся у нарушителя КБ прав доступа к ИР либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР. Если нарушение КБ было вызвано незнанием нарушителем правил (технологии) работы с информационными ресурсами, то основанием для возврата прав доступа является успешное прохождение инструктажа по компьютерной безопасности, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами КНИТУ.

4.2.11.Восстановление временно отключенных у нарушителя КБ прав доступа к ИР (разблокировка пользователя) может производиться только администратором безопасности.

5. Оформление результатов проведенного разбирательства

5.1. Собранная в процессе разбирательства инцидента КБ информация фиксируется ЦКБ в карточке данных об инциденте компьютерной безопасности (приложение №1) и учитывается при подготовке итогового заключения по инциденту КБ.

5.2. ЦКБ формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента КБ.

5.3. Итоговое заключение по инциденту КБ ЦКБ направляет руководителям структурных подразделений, затронутых инцидентом КБ.

5.4. Начальник ЦКБ фиксирует завершение разбирательства в регистрационной карточке инцидента и присваивает инциденту статус «Разбирательство завершено».

5.5. ЦКБ, при необходимости определения правовой оценки инцидента КБ, может обратиться за консультациями в юридическое подразделение КНИТУ.

5.6. В случае выявления в инциденте КБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, ЦКБ передает все материалы по инциденту КБ руководству КНИТУ для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

6. Завершение разбирательства, превентивные мероприятия

6.1. По завершению разбирательства инцидента КБ, ЦКБ передает копии имеющиеся материалов (в объеме, достаточном для принятия решения) вышестоящему руководителю нарушителя КБ для решения вопроса о целесообразности привлечения нарушителя КБ к дисциплинарной ответственности.

6.2. На основании полученных результатов разбирательства руководитель структурного подразделения совместно с ЦКБ в срок не более 3 (трех) рабочих дней организовывает проведение мероприятий, направленных на снижение рисков информационной безопасности в будущем:

- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя КБ;
- доведение до всех сотрудников структурного подразделения требований внутренних нормативных документов КНИТУ;
- обсуждение инцидента КБ на совещании руководителей или собрании коллектива;
- отмена неактуальных прав доступа к информационным ресурсам;

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

6.3. О результатах проведенного разбирательства инцидента КБ ЦКБ при необходимости инициирует подготовку сообщения об инциденте КБ в адрес руководства КНИТУ.

7. Права, обязанности и ответственность участников разбирательства

7.1. ЦКБ имеет право:

- по согласованию с непосредственным руководителем нарушителя КБ требовать предоставлений письменных объяснений по обстоятельствам инцидента КБ у нарушителя КБ;
- запрашивать и получать от сотрудников КНИТУ, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента КБ.
- инициировать отключение от информационных ресурсов сотрудников, нарушивших правила или требования КБ, на период проведений расследования инцидента КБ в случае если имеется существенный риск того, что продолжение работы сотрудника с ИР может повлечь значительное увеличение ущерба или новые инциденты КБ;
- по результатам расследования инцидента КБ инициировать изменения в информационных ресурсах КНИТУ с целью повышения их защищенности и снижения рисков инцидентов КБ;
- инициировать процедуры привлечения нарушителя КБ к дисциплинарной и (или) материальной ответственность согласно внутренним нормативным документам КНИТУ.

7.2. ЦКБ обязан:

- объективно проводить разбирательство каждого инцидента КБ;
- определять первоочередные меры, направленные на локализацию инцидента КБ и минимизацию негативных последствий;
- фиксировать в регистрационной карточке инцидента КБ всю исходную информацию об инциденте КБ и результаты его расследования;
- предоставлять отчеты и рекомендации по проведенным разбирательствам руководству КНИТУ;

- проводить анализ обстоятельств, способствовавших совершению каждого инцидента КБ, и на его основе, разрабатывать рекомендации и предложения по снижению ущерба от подобных инцидентов КБ и минимизации возможности их повторения в будущем.

7.3. Руководители структурных подразделений и сотрудники КНИТУ обязаны:

- предоставлять по запросам ЦКБ устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента КБ;
- информировать ЦКБ о выявленных инцидентах КБ;
- информировать ЦКБ имеющихся запросах и обращениях субъектов защищаемой информации.

Приложение 1
к Регламенту о реагировании на инциденты компьютерной безопасности в ФГБОУ ВО «КНИТУ

КАРТОЧКА
данных об инциденте компьютерной безопасности

Дата события _____ Номер события _____

Информация о сообщающем лице

Фамилия, имя, отчество _____;
Подразделение, должность _____;
Телефон, электронная почта _____;

Описание события КБ

Что произошло _____
_____;
Как произошло _____
_____;
Почему произошло_____
_____;
Пораженные компоненты _____
_____;
Негативное воздействие на защищаемую информацию _____
_____;
Любые идентифицированные уязвимости _____
_____.

Детали события КБ

Дата и время возникновения события _____ ;
Дата и время обнаружения события _____;
Дата и время сообщения о событии _____;
Классификация события _____
_____;

Закончилось событие? (отметить квадрат)	Да	Нет

Если «ДА», то уточнить, как долго длилось событие в днях/часах/минутах
_____

Тип инцидента КБ

(Отметить один квадрат, затем заполнить соответствующие поля ниже)

Действительный □

Попытка □

Подозрение □

Указать типы угрозы, один из:

Намеренная □

Хищение □
Мошенничество □
Саботаж/физический ущерб □
Вредоносная программа □
Хакерство/Логическое проникновение □
Неправильное использование ресурсов □
Другой ущерб □

Случайная □

Отказ аппаратуры □
Отказ ПО □
Отказ связи □
Отказ электропитания □
Пожар, наводнение □
Другие природные события □

Ошибка □

Операционная ошибка □
Ошибка аппаратной поддержки □
Ошибка поддержки ПО □
Ошибка пользователя □
Ошибка конструкции □
Другие случаи (включая ненамеренные ошибки) □

Неизвестно □

(Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат «неизвестно» и, по возможности, указать тип угрозы)

_____

_____

_____

___

Пораженные активы (если есть)

(Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности)

Информация/Данные _____
_____;

Аппаратура _____
_____;

Программное обеспечение _____
_____;

Средства связи _____
_____;

Документация _____
_____.

Негативное воздействие/влияние инцидента на финансовую структуру

(Сделать отметку в соответствующих квадратах для указанных ниже нарушений, затем в колонке «значимость» указать уровень негативного воздействия на активы по шкале 1- 10, используя следующие сокращения (указатели категорий): (ФП) – финансовые потери, (КИ) - коммерческие и экономические интересы, (ПД) – информация, содержащая персональные данные, (ПО) – правовые и нормативные обязательства, (М) – менеджмент, (ПП) – потеря престижа.

Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость»)

Качества информации, пострадавшие в результате инцидента	***Отметка о нарушении качеств информации***	**Значимость**	**Указатели**	**Стоимость**
Нарушение конфиденциальности *(несанкционированное раскрытие)*				
Нарушение целостности *(несанкционированная модификация)*				
Нарушение доступности *(недоступность*				
Нарушение неотказуемости				
Уничтожение				

Полные стоимости восстановления после инцидента

	Значимость	**Указатели**	**Стоимость**
Где возможно, необходимо указать общие расходы на восстановление после инцидента			

КБ в целом по шкале 1-10 для «значимости» и в деньгах для «стоимости»			

Разрешение инцидента

Дата начала расследования инцидента	
Должность, Фамилия, инициалы лица (лиц) проводившего (их) расследования инцидента	
Дата окончания инцидента	
Дата окончания воздействия	
Дата завершения расследования инцидента	
Место хранения отчета о расследовании	

Причастные к инциденту лица

(сделать отметку в таблице)

Лицо	
Организованная группа	
Легально учрежденная организация/учреждение	
Случайность	
Отсутствие нарушителя (*Например, природные факторы, отказ оборудования, ошибка человека)*	

Описание нарушителя

Действительная или предполагаемая мотивация

Криминальная/финансовая выгода	
Развлечение/хакерство	
Политика/Терроризм	
Месть	
Другие мотивы	

Действия, предпринятые для разрешения инцидента

(например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением…»)

Действия, запланированные для разрешения инцидента

(включая возможные приведенные выше действия)

Заключение

(Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения)

Значительный	Незначительный	Обоснование

Указать любые другие заключения:

Ознакомленные должностные лица с отчетом
(должность, фамилия, организация)

Привлеченные лица
(должность, фамилия, имя, отчество, в каком качестве привлекался к расследованию, подпись, дата)

Приложение № 4
к приказу ФГБОУ ВО «КНИТУ»
от _30.11.2021____ № ____889-о____

ПОЛОЖЕНИЕ
об антивирусной защите в федеральном государственном бюджетном образовательном учреждении высшего образования «Казанский национальный исследовательский технологический университет»

1. Общие положения

1.1. Настоящее Положение определяет требования к организации защиты информационных ресурсов федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (далее КНИТУ) от воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений за их выполнение.

1.2. Задачами антивирусной защиты являются:

- определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления;
- проведение профилактических работ с применением антивирусных диагностических средств;
- непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации информационных систем КНИТУ.

2. Термины и определения

Компьютерный вирус –вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, и распространять свои копии по разнообразным каналам связи

Зараженный диск – это диск, в загрузочном секторе которого находится программа - вирус. После запуска программы, содержащей вирус, становится возможным заражение других файлов.

Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS или BAT. Крайне редко заражаются текстовые и графические файлы.

Зараженная программа – это программа, содержащая внедренную в нее программу-вирус.

3. Организация мероприятий по антивирусной защите

3.1. К использованию в КНИТУ допускаются только лицензионные антивирусные средства, централизованно закупленные управлением информационных технологий (далее - УИТ) у разработчиков (поставщиков) указанных средств.

3.2. Установка средств антивирусной защиты на компьютерах в КНИТУ осуществляется сотрудниками УИТ (на абонентских пунктах федеральных информационных систем, а также автоматизированных рабочих местах предназначенных для обработки сведений составляющих государственную тайну и сведений ограниченного распространения – ДСП данные работы выполняются сотрудниками центра компьютерной безопасности). Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

3.3. Обновление антивирусных баз должно быть произведено не реже 1 раза в сутки автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную.

4. Профилактика вирусов

4.1. Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов в компьютере. К основным профилактическим работам и мероприятиям относятся:

- автоматическая проверка наличия вирусов при включении компьютера;
- проверка наличия вирусов на компьютере, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;
- создание резервной копии программного продукта сразу же после приобретения;
- ограничение доступа к компьютеру лиц, не являющихся сотрудниками или студентами КНИТУ.

4.2. При обнаружении вирусов на компьютере, работающем в локальной сети, проверке подлежат все компьютеры, включенные в эту сеть и работающие с теми же данными и программным обеспечением.

5. Обязанности пользователя

5.1. Пользователь при обнаружении вредоносного кода (срабатывании средства антивирусной защиты) обязан:

- прекратить (приостановить) работу;
- поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника и ответственного за эксплуатацию ПК;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов согласно раздела № 6 данного положения (при необходимости для выполнения требований данного пункта следует привлечь администратора системы);
- если вирус проник на компьютер со съемного носителя, то необходимо определить источник распространения и, если источник на съемном носителе находится в КНИТУ, то необходимо проверить на наличие вирусов съемный носитель, а также все компьютеры, которые работали с этим съемным носителем. Если источник съемного носителя - другая организация, то необходимо сообщить в эту организацию о факте выявления вирусов и в дальнейшем обратить особое внимание на носители информации, поступающие из этой организации.

5.2. Пользователю **ЗАПРЕЩАЕТСЯ** отключать средства антивирусной защиты информации.

5.3. Основные возможные источники вирусов:

- съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Интернет;
- жесткий диск, на который попал вирус в результате работы с зараженными программами.

6. Применение средств антивирусной защиты

6.1. Если вирус поразил какие-либо программы, то уничтожение вируса выполняется путем уничтожения программы на диске либо на съемном

носителе. После уничтожения зараженной программы необходимо переустановить данную программу.

6.2. Если вирус поразил файлы, то вирус уничтожается либо путем стирания этих файлов, либо путем использования специальных лечащих программ, входящих в состав антивирусной программы. Использование лечащих программ не дает полной гарантии восстановления файла. Поэтому после лечения необходима проверка восстановления данного файла. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы либо файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

6.3. В любом случае, после уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы. Если повторная проверка не выявила вирусов, то можно быть уверенным в отсутствии вирусов.

7. Ответственность

7.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством РФ и локальными нормативными актами КНИТУ.

Приложение № 5
к приказу ФГБОУ ВО «КНИТУ»
от __30.11.2021____ № __889-о_

ПОЛОЖЕНИЕ
об использовании программного обеспечения в федеральном государственном бюджетном образовательном учреждении высшего образования «Казанский национальный исследовательский технологический университет»

1. Общие положения

1.1. Настоящее Положение регулирует процесс эксплуатации программного обеспечения в деятельности профессорско-преподавательского состава, работников и студентов федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (далее КНИТУ). Положение разработано в соответствии с требованиями закона от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных», положениями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» и является составной частью политики компьютерной безопасности.

1.2. Настоящее Положение устанавливает правила использования программного обеспечения вычислительной техники в КНИТУ, а также определяет права и обязанности работников в процессе эксплуатации всех видов программного обеспечения в КНИТУ.

2. Основные термины, сокращения и определения.

АРМ – автоматизированное рабочее место пользователя для выполнения определенной задачи.

ИС – информационная система КНИТУ – система, обеспечивающая хранение, обработку, преобразование и передачу информации КНИТУ с использованием компьютерной и другой техники.

ПО – программное обеспечение вычислительной техники, базы данных.

Пользователь ИС – работник КНИТУ, использующий ПО (в составе АРМ) для выполнения своих трудовых обязанностей.

Администратор ИС – технический специалист, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО.

ПК – персональный компьютер – комплекс вычислительной техники с установленным ПО; используется одним или несколькими пользователями ИС.

3. Порядок эксплуатации программного обеспечения

3.1. В состав каждого АРМ входит набор ПО для выполнения определенного вида деятельности. ПО, не входящее в состав АРМ, не может быть установлено и использовано работниками КНИТУ без процедуры согласования с управлением информационных технологий (далее - УИТ).

3.2. Все операции по установке, сопровождению и поддержке, удалению ПО АРМ выполняются непосредственно администраторами ИС.

3.3. Все заявки на обслуживание (установку ПО, удаление ПО, ремонт АРМ и т.п.) направляются в управление информационных технологий через портал kstu.ru, раздел ТЕХНИЧЕСКИЙ СЕРВИС (https://www.kstu.ru/ekds/www_init_tus.jsp).

3.4. Порядок эксплуатации программного обеспечения в КНИТУ состоит из следующих этапов:

3.4.1. Определение потребности в ПО

Запрос на установку дополнительного ПО может быть инициирован как руководителем структурного подразделения, так и администратором ИС.

Запрос **руководителя структурного подразделения** на установку ПО производится в случаях:

- необходимости организации АРМ для нового работника;
- необходимости выполнения работниками новых (дополнительных) обязанностей, для которых требуется дополнительное ПО или полная замена АРМ;
- появления качественно нового (альтернативного) ПО, взамен используемого в составе АРМ.

Порядок согласования установки ПО:

- руководитель структурного подразделения готовит запрос на установку ПО (приложение №1);
- при наличии в КНИТУ запрошенного ПО, администратор ИС выполняет работы по его установке, за АРМ пользователя закрепляется лицензия установленного ПО;
- при отсутствии в КНИТУ вакантных лицензий на коммерческое ПО, Руководитель структурного подразделения готовит заявку на приобретение ПО в установленном порядке.

Запрос **администратора ИС** на установку ПО производится в случаях:

- устранения уязвимостей систем обеспечения информационной безопасности КНИТУ;

- плановой замены используемого пользователями ПО;
- внедрения новых информационных технологий.

Порядок согласования установки ПО:

- УИТ определяет наличие вакантных лицензий и осуществляет выделение (закрепление за АРМ или сервером) необходимых лицензий, обеспечивает выполнение работ по установке необходимого ПО;
- при необходимости закупки дополнительного ПО, УИТ определяет возможность его использования в ИС КНИТУ, готовит заявку на приобретение.

3.4.2. Поддержка и сопровождение ПО

Поддержка и сопровождение ПО выполняется техническими специалистами - администраторами ИС.

Поддержка и сопровождение ПО заключается в выполнении следующих видов работ:

- настройка и адаптация установленного ПО;
- установка обновлений ПО;
- регламентированное создание резервных копий (архивирование) ПО и пользовательских данных (электронных документов, баз данных);
- устранение неисправностей, связанных с использованием установленного ПО;
- консультирование пользователей ИС.

Работа по сопровождению ПО может быть инициирована пользователем ИС (руководителем структурного подразделения) либо непосредственно администратором ИС.

3.4.3. Удаление (вывод из эксплуатации) ПО

ПО выводится из эксплуатации в следующих случаях:

- окончание лицензионного срока использования ПО;
- замена используемого ПО на альтернативное;
- прекращение использования ПО вследствие отсутствия надобности, морального старения.

Вывод ПО из эксплуатации выполняется администраторами ИС:

- Выполняется удаление выводимого из эксплуатации ПО со всех ПК КНИТУ;
- При необходимости подготавливается и передается в бухгалтерию акт вывода из эксплуатации коммерческого ПО.

3.5. При эксплуатации программного обеспечения необходимо:

3.5.1. Соблюдать требования настоящего Положения.

3.5.2. Использовать имеющееся в распоряжении ПО исключительно для выполнения своих служебных обязанностей.

3.5.3. Обеспечивать сохранность переданных в составе АРМ носителей с ключевой информацией, сертификатов подлинности коммерческого ПО.

3.5.4. Содействовать администратору ИС в выполнении работ по установке, настройке, устранению неисправностей установленного ПО.

3.5.5. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения.

3.6. При эксплуатации программного обеспечения запрещено:

3.6.1. Использовать АРМ не по назначению.

3.6.2. Самостоятельно вносить изменения в конструкцию, конфигурацию АРМ ИС и другого оборудования ИС.

3.6.3. Изменять состав установленного на АРМ ПО (устанавливать новое ПО, изменять состав компонент пакетов ПО и удалять ПО).

3.6.4. Приносить на внешних носителях и не санкционированно запускать на своем или другом АРМ любые системные или прикладные программы, без согласования с УИТ.

4. Ответственность

4.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством РФ и локальными нормативными актами КНИТУ.

Приложение № 1
к «Положению об использовании
программного обеспечения…»

ЗАЯВКА
на установку/удаление программного обеспечения АРМ

Начальнику УИТ

«___» _____ 20__года

Прошу произвести установку/удаление следующего программного обеспечения:

_____
_____
_____

в связи с необходимостью/утратой необходимости решения следующих задач:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Руководитель _____

«___» _____ 20__г. _____/_____

Приложение № 6
к приказу ФГБОУ ВО «КНИТУ»
от __30.11.2021__ № ____889-о____

ПОЛОЖЕНИЕ
по использованию электронной почты в федеральном государственном бюджетном образовательном учреждении высшего образования «Казанский национальный исследовательский технологический университет»

1. Общие положения

1.1. Настоящее Положение устанавливает порядок использования электронной почты в федеральном государственном бюджетном образовательном учреждении высшего образования «Казанский национальный исследовательский технологический университет» (далее КНИТУ).

1.2. Действие настоящего Положения распространяется на работников и студентов КНИТУ.

2.Основные термины, сокращения и определения

- **АРМ** – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной, административной, научной или учебной задачи.
- **ИС** – информационная система КНИТУ – система, обеспечивающая хранение, обработку, преобразование и передачу информации КНИТУ с использованием компьютерной и другой техники.
- **ПК** – персональный компьютер.
- **ПО** – программное обеспечение вычислительной техники.
- **ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности информации.
- **Пользователь** – работник, студент КНИТУ, использующий электронную почту.
- **Почтовый клиент** – ПО, входящее в состав АРМ пользователя ИС, предназначенное для получения, написания, отправки и хранения сообщений электронной почты.
- **Почтовый сервер** – сервер электронной почты – ПО, осуществляющее обработку и передачу почтовых сообщений между АРМ ИС КНИТУ, а также общедоступных сетей – Интернет.
- **Отправитель** – пользователь, осуществляющий пересылку электронных сообщений получателю посредством электронной почты.

- **Получатель** – пользователь, которому адресовано электронное сообщение, пересылаемое отправителем посредством электронной почты.
- **Электронный документ** – документ, в котором информация представлена в электронно-цифровой форме.
- **Электронная почта** – сервис обмена электронными сообщениями в рамках ИС КНИТУ (внутренняя электронная почта) и общедоступных сетей Интернет (внешняя электронная почта).
- **Электронный почтовый ящик** – персональное пространство на почтовом сервере, в котором хранятся электронные сообщения.
- **Электронное почтовое сообщение** – сообщение, формируемое отправителем с помощью почтового клиента и предназначенное для передачи получателю посредством электронной почты.

3. Порядок использования электронной почты

3.1. Электронная почта используется для обмена в рамках ИС КНИТУ (внутренняя электронная почта) и общедоступных сетей (внешняя электронная почта) служебной информацией в виде электронных сообщений и документов в электронном виде.

3.2. Обеспечение функционирования сервиса электронной почты осуществляется специалистами управления информационных технологий.

3.3. Доступ пользователей к внутренней электронной почте предоставляется при подключении АРМ к ИС КНИТУ.

3.4. При трудоустройстве нового работника руководитель подразделения составляет заявку на организацию нового автоматизированного рабочего места (Приложение №1) и отправляет его на электронную почту директору по цифровым технологиям и административным сервисам Беркману Ю.В., начальнику управления кадров и документационного обеспечения Харисову И.Ш.

3.5. При использовании электронной почты необходимо:

3.5.1. Соблюдать требования настоящего Положения.

3.5.2. Использовать электронную почту исключительно для выполнения своих служебных обязанностей.

3.5.3. Перед отправкой сообщения проверять правильность введенного электронного адреса получателя.

3.5.4. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения.

3.6. При использовании электронной почты запрещено:

3.6.1. Использовать электронную почту в личных целях.

3.6.2. Передавать электронные сообщения, содержащие:

- Государственную тайну, служебную тайну (ДСП), конфиденциальную информацию, а также информацию, составляющую коммерческую тайну.

- Информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца.

- Информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также осуществить несанкционированный доступ, а также ссылки на вышеуказанную информацию.

- Угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной и религиозной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.

3.6.3. Переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей без подтверждения подлинности отправителя (по телефону или другим способом).

3.6.4. По собственной инициативе осуществлять рассылку (в том числе и массовую) электронных сообщений (если рассылка не связана с выполнением служебных обязанностей).

3.6.5. Использовать адрес электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением служебных обязанностей.

3.6.6. Предоставлять работникам КНИТУ (за исключением администраторов ИС) и третьим лицам доступ к своему электронному почтовому ящику.

3.7. КНИТУ оставляет за собой право доступа к электронным сообщениям работников с целью их архивирования и централизованного хранения, а также мониторинга выполнения требований настоящего Положения.

3.8. Все электронные сообщения и документы в электронном виде, передаваемые посредством электронной почты подлежат обязательной проверке на отсутствие вредоносного ПО.

4. Требования к оформлению электронного сообщения

4.1. При оформлении электронного сообщения необходимо заполнять следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (при необходимости, могут быть вложены различные файлы);

4.2. В почтовом клиенте существует возможность создания подписи и автоматической вставки ее в электронное сообщение. При необходимости можно создать несколько подписей для различных получателей.

4.3. При формировании ответов на полученные электронные сообщения можно использовать упрощенную подпись.

5. Ответственность

5.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами КНИТУ.

Приложение № 7
к приказу ФГБОУ ВО «КНИТУ»
от ___30.11.2021___№ ____889-о____

ПОЛОЖЕНИЕ
по использованию локальной сети и сети Интернет в федеральном государственном бюджетном образовательном учреждении высшего образования «Казанский национальный исследовательский технологический университет»

1. Общие положения

1.1. Настоящее Положение устанавливает порядок использования локальной сети и сети Интернет работниками и студентами федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (далее КНИТУ).

1.2. Действие настоящего Положения распространяется на работников и студентов КНИТУ.

2.Основные термины, сокращения и определения

- **Администратор ИС** – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО.
- **Адрес IP** – уникальный идентификатор АРМ, подключенного к ИС КНИТУ.
- **АРМ** – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной задачи.
- **Интернет** – глобальная ИС, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.
- **ИС** – информационная система КНИТУ – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
- **ПК** – персональный компьютер.
- **ПО** – программное обеспечение вычислительной техники, базы данных.
- **Пользователь** – работник, студент КНИТУ.

3. Порядок использования локальной сети и сети Интернет

3.1. Доступ к локальной сети и сети Интернет предоставляется работникам и студентам КНИТУ в целях выполнения ими своих служебных обязанностей, выполнения научных и учебных задач, требующих непосредственного подключения к внешним информационным ресурсам.

3.2. Операции по предоставлению доступа работников и студентов КНИТУ к локальной сети и сети Интернет и контролю использования выполняются непосредственно (при участии) администраторами ИС.

3.3. АРМ, используемые для обработки государственной тайны, служебной информации ограниченного распространения (ДСП), не могут быть подключены к сети Интернет.

3.4. При использовании локальной сети и сети Интернет необходимо:

3.4.1. Соблюдать требования настоящего Положения.

3.4.2. Использовать локальную сеть и сеть Интернет исключительно для выполнения своих служебных обязанностей (учебных и научных задач).

3.4.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения.

3.5. При использовании локальной сети и сети Интернет запрещено:

3.5.1. Использовать предоставленный КНИТУ доступ в локальную сеть и сеть Интернет в личных целях.

3.5.2. Использовать специализированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к локальной сети и сети Интернет.

3.5.3. Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС КНИТУ.

3.5.4. Публиковать, загружать и распространять материалы содержащие:

- Государственную тайну, служебную информацию ограниченного распространения (ДСП), конфиденциальную информацию, а также информацию, составляющую коммерческую тайну.

- Информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца.

- Вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера приобретенного КНИТУ коммерческого ПО и ПО для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам (если доступ к этим ресурсам был приобретен КНИТУ), а также ссылки на вышеуказанную информацию.

- Угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной и религиозной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.

3.5.5. Фальсифицировать свой IP-адрес, а также прочую служебную информацию.

3.6. КНИТУ оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, научной и учебной деятельности, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством.

3.7. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

4. Ответственность

4.1. Работники и студенты, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами КНИТУ.

Заявка на организацию нового автоматизированного рабочего места (АРМ)

1. Заполненную форму необходимо согласовать с непосредственным руководителем в следующих случаях:
2) Для стажеров: согласование с куратором + указать срок окончания стажировки.
3) Для командированных сотрудников: согласование с руководителем подразделения, либо лица от ВУЗА, ответственного за данного работника, в случае если он не является сотрудником "ВУЗА" + указать срок окончания командировки.
4) При выдаче автоматизированного рабочего места (АРМ). *Для обеспечения в МАРМ (мобильное автоматизированное рабочее место) требуется приложить обоснование + согласование Директора по ЦТиАС*
Не требуется согласование руководителя для выдачи стандартного АРМ для штатного сотрудника.
2. Согласованную руководителями форму + заявку направить ч/з технический сервис с пометкой "Организация нового рабочего места" (https://www.kstu.ru/ds/www_init_tus.jsp). На одного пользователя - одна заполненная форма заявки.
Заявка на новое рабочее место должна быть подана не менее чем за 7 рабочих дней до выхода сотрудника!
Несвоевременная подача заявки приводит к несвоевременной организации рабочего места.

1. Общие сведения *(* - ВСЕ ПОЛЯ ОБЯЗАТЕЛЬНЫ ДЛЯ ЗАПОЛНЕНИЯ)*

1.1. Инициатор (контактное лицо, оформившее данную заявку)	**Фамилия Имя Отчество***	Курбангалеева Адиля Рамилевна
	Контактный телефон*	XX-XX
1.2. Информация о новом сотруднике	**Фамилия Имя Отчество***	Иванов Иван Иванович
	Дата рождения*	
	Наименование организации*	ФГБОУ ВО КНИТУ
	Должность*	указать должность
	Дата выхода на работу*	01.01.2022
	Непосредственный руководитель / Куратор (ФИО)*	Сергеев Сергей Сергеевич
	Здание, кабинет*	К.Маркса 68, А155
	Срок окончания стажировки *(обязательно для стажеров)*	с xx.xx.xx по xx.xx.xx
	Срок окончания командировки *(обязательно для командированных сотрудников)*	с xx.xx.xx по xx.xx.xx
1.3. Дата заполнения заявки		**20 декабря 2021**

2. Предоставление средств связи и персонального компьютера

	При возникновении вопросов обратитесь в Техническую Поддержку: тел.+ ***7 917 240 0203, support@kstu.ru***	
2.1. Предоставление средств связи		☑ [redacted] ☐ [redacted] ☐ [redacted]
2.2. Предоставление компьютера	Для выдачи ноутбука требуется согласование линейного руководителя и Директора ЦТиАС	☑ [redacted] ☐ [redacted]

3. Предоставление доступа к Информационным Системам и сетевым ресурсам

	При возникновении вопроосов обратитесь в Техническую Поддержку: тел. ***+7 917 240 0203, support@kstu.ru***
3.1. Общедоступные ресурсы	**Для сотрудников Вуза и стажеров:** **1. Персональный электронный почтовый ящик** **2. Доступ к Корпоративному Порталу** **3. Доступ к сети Интернет.**
3.2. Предоставление доступа к корп. системам (ИС ПАРУС, ЭДО ПРАКТИКА, Сетевые папки, Sharepoint) **3.3. Предоставление доступа к Информационным Системам** **3.4. Предоставление доступа к общим папкам на диске "W:\"** **3.5. Установка специализированного программного обеспечения**	**ВНИМАНИЕ!!! Обращения на предоставление доступов и установки ПО подаются отдельно, после выдачи АРМ новому сотруднику.** **Для получения доступа к любым информационным системам обратитесь в техническую поддержку по адресу support@kstu.ru, или на номер 7 917 240 0203.**