МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДЕНО
Приказом Врио ректора
от 12.05.2026 № 1/409
Врио ректора университета
(приказ от 08.05.2026 г. №1/403)

_____ К.В. Савельев

«12» 05 2026 г.

ПОЛИТИКА

защиты информации в Федеральном государственном бюджетном образовательном учреждении высшего образования «Самарский государственный технический университет» (ФГБОУ ВО «СамГТУ»)

П-1236, 12.05.2026
номер, дата введения

Самара, 2026

Федеральное государственное бюджетное образовательное учреждение высшего образования "Самарский государственный технический университет"

Лист согласования

Наименование Положение № 11940 от 17.04.2026

Описание ПОЛИТИКА защиты информации в Федеральном государственном бюджетном образовательном учреждении высшего образования «Самарский государственный технический университет» (ФГБОУ ВО «СамГТУ»)

Инициатор Булгаков А. О., Специалист по информационной безопасности, Отдел информационной безопасности

Дата начала процесса 17.04.2026 13:25 **Дата завершения** 05.05.2026 11:56

Должность	Результат	Дата	Пользователь
Проректор по цифровому развитию	Согласовано	17.04.2026	Савельев К. В.
Заместитель начальника управления	Согласовано	17.04.2026	Григорьев А. А.
Начальник службы	Согласовано	20.04.2026	Смирнова Н. В.
Начальник управления	Согласовано	20.04.2026	Иванова А. Н.
Начальник управления	Согласовано	05.05.2026	Саушкин И. Н.

Настоящая Политика защиты информации (далее - Политика) в ФГБОУ ВО «СамГТУ» является собственностью ФГБОУ ВО «СамГТУ». Настоящая Политика не может быть полностью или частично воспроизведена, тиражирована и распространена в качестве официального издания без разрешения ФГБОУ ВО «СамГТУ»

1. Основные понятия

Информация - сведения (сообщения, данные) независимо от формы их представления;

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Информационная система персональных данных – информационная система, в которой осуществляется обработка персональных данных;

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

Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только те субъекты, которые имеют на это право;

Целостность – состояние информации, при котором изменять информацию могут только те субъекты, которые имеют на это право;

Доступность – состояние информации, при котором субъекты, имеющие право доступа к информации, могут осуществлять его беспрепятственно;

Информационная безопасность – состояние защищенности информации и информационных систем от угроз безопасности информации;

Защита информации – деятельность, направленная на предотвращение утечки информации, несанкционированного и (или) непреднамеренного воздействия на информацию;

Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения безопасности информации;

Риск информационной безопасности – возможность реализации угрозы безопасности информации и величина возможного ущерба.

Уязвимость – недостаток или слабое место в информационной системе, которое может быть использовано для реализации угрозы;

Инцидент информационной безопасности – событие или совокупность событий, нарушающих или создающих угрозу нарушения безопасности информации;

Доступ к информации – возможность получения информации и её использования;

Несанкционированный доступ – доступ к информации, нарушающий установленные правила разграничения доступа;

Субъект доступа – пользователь или процесс, осуществляющий доступ к информации;

Объект доступа – информация или ресурс, к которому осуществляется доступ;

Идентификация – присвоение субъекту доступа уникального идентификатора;

Аутентификация – проверка подлинности субъекта доступа;

Разграничение доступа – установление и реализация правил доступа субъектов к объектам;

Удаленный доступ – доступ к информационной системе с использованием сетей связи вне контролируемой зоны;

Мобильное устройство – переносное средство вычислительной техники, используемое для доступа к информационным системам;

Меры защиты информации – организационные и (или) технические меры, направленные на обеспечение безопасности информации;

Средства защиты информации – технические, программные или программно-аппаратные средства защиты информации;

Криптографическая защита информации – защита информации с применением криптографических методов;

Регистрация событий безопасности – фиксация действий пользователей и процессов, влияющих на безопасность информации;

Резервное копирование – создание копий для восстановления в случае утраты или повреждения;

Непрерывность функционирования – способность информационной системы выполнять заданные функции без недопустимых перерывов;

Локальный нормативный акт – внутренний документ, обязательный для исполнения.

2. Общие положения

1. Настоящая Политика определяет цели, принципы, основные требования и организационные меры по обеспечению защиты информации в Федеральном государственном бюджетном образовательном учреждении высшего образования «Самарский государственный технический университет»;

2. Политика разработана в соответствии с законодательством Российской Федерации, государственным стандартами и нормативными документами уполномоченных органов в области защиты информации, в том числе с требованиями федеральных законов, ГОСТ и нормативных документов ФСТЭК России;

3. Действие настоящей Политики распространяется на все виды конфиденциальной информации, обрабатываемой в ФГБОУ ВО «СамГТУ», независимо от формы ее представления, способов обработки и средств хранения;

4. Настоящая Политика применяется в отношении всех информационных систем, использующихся в ФГБОУ ВО «СамГТУ»;

5. Политика обязательная для исполнения всеми работниками ФГБОУ ВО «СамГТУ»;

6. Настоящая Политика не распространяется на организацию и порядок защиты информации, составляющей государственную тайну;

7. Настоящая Политика может изменяться в одностороннем порядке. Актуальная версия Политики размещена на официальном сайте ФГБОУ ВО «СамГТУ»;

8. Настоящая Политика подлежит пересмотру и актуализации при изменении законодательства Российской Федерации, требований регуляторов, структуры ФГБОУ ВО «СамГТУ», состава информационных систем или условий обработки информации.

3. Область действия политики

1. Настоящая Политика защиты информации определяет цели, принципы и основные требования по обеспечению информационной безопасности в Федеральном государственном бюджетном образовательном учреждении высшего образования «Самарский государственный технический университет» (далее — Университет) и распространяется на все процессы, связанные с созданием, обработкой, хранением, передачей и уничтожением информации в деятельности Университета.

2. Действие Политики распространяется на все структурные подразделения Университета, включая факультеты, институты, кафедры, административно-управленческие службы, а также на филиалы и представительства.

Требования настоящей Политики являются обязательными для исполнения всеми категориями пользователей информационных ресурсов Университета, в том числе:

- профессорско-преподавательским составом;
- административно-управленческим и техническим персоналом;
- обучающимися (студентами, магистрантами, аспирантами);

- иными лицами, получившими доступ к информационным ресурсам и системам Университета на законных основаниях.

3. Политика защиты информации распространяется на все виды информации, перечисленные в 8 подпункте данного раздела, независимо от формы её представления, включая электронную, бумажную, графическую, аудио-, видео- и иные формы, а также все этапы жизненного цикла информации: сбор, обработку, хранение, передачу, архивирование и уничтожение.

4. Настоящая Политика распространяется на все используемые в Университете информационные системы, перечисленные в 10 подпункте данного раздела, а также на информационные ресурсы Университета.

5. Настоящая Политика применяется ко всем техническим средствам обработки информации Университета, включая серверы, рабочие станции, мобильные устройства, МФУ и съёмные носители информации независимо от их принадлежности, если они используются при работе с конфиденциальной информацией.

Требования настоящей Политики обязательны к соблюдению при использовании обучающимися и работниками Университета как корпоративных, так и личных устройств в случаях, когда такие устройства применяются для доступа к информационным системам или ресурсам Университета.

6. Политика защиты информации распространяется на деятельность сторонних организаций и подрядчиков, привлекаемых Университетом, в части, касающейся их доступа к информационным ресурсам и системам Университета. Соответствующие требования должны быть закреплены в договорах, соглашениях о конфиденциальности, обязательствах о неразглашении конфиденциальной информации и иных документах.

7. Настоящая Политика действует совместно с иными локальными нормативными актами Университета в области информационной безопасности и не отменяет требований законодательства Российской Федерации, государственных стандартов и нормативных документов в области защиты информации.

8. Перечень конфиденциальной информации:

- Коммерческая тайна (Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»);

- Секрет производства (ноу-хау) (Статья 1465 Гражданского кодекса РФ (часть четвертая);

- Персональные данные (Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»);

- Информация о новых решениях и технических знаниях, полученных сторонами по договору подряда (Статья 727 Гражданского кодекса РФ (часть вторая);

- Сведения, касающиеся предмета договоров на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, хода их исполнения и полученных результатов, если иное не предусмотрено договорами (Статья 771 Гражданского кодекса РФ (часть вторая);

- Сведения о доходах, об имуществе и обязательствах имущественного характера, представляемые государственными и муниципальными служащими, а также иными лицами, указанными в части 1 статьи 8 Федерального закона от 25.12.2008 N 273-ФЗ «О противодействии коррупции»;

- Врачебная тайна (Статьи 13, 92 Федерального закона от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»);

- Служебная тайна в области обороны (ст. 3.1. Федерального закона от 31.05.1996 N 61-ФЗ «Об обороне»);

- Служебная информация ограниченного распространения;

- Сведения конфиденциального характера, признанные СамГТУ как подлежащие защите.

9. Действие настоящей Политики распространяется на все информационные системы Университета, в которых осуществляется обработка конфиденциальной информации, указанной в 8 подпункте данного раздела.

Политика применяется к информационным системам независимо от функционального назначения, уровня автоматизации и архитектуры, места размещения, принадлежности технических средств, режима эксплуатации.

Выделяются следующие категории информационных систем, на которые распространяется действие настоящей Политики:

- Информационные системы персональных данных (ИСПДн);

- Государственные и ведомственные информационные системы (ФИС, ГИС);

- Системы электронного документооборота;

- Информационные системы, обрабатывающие служебную информацию ограниченного доступа;

- Информационная система управления образовательной деятельность, обеспечивающая: проведение приемной кампании, сопровождение образовательного процесса, сопровождение научно-исследовательской деятельности, управление контингентом обучающихся и работников, ведение договоров об оказании платных образовательных услуг, управление аудиторным фондом, формирование аналитической отчетности;

- Научные и исследовательские информационные системы;

- Информационные системы административно-хозяйственной деятельности (в том числе системы, предназначенные для: автоматизации кадрового учета и расчета заработной платы, автоматизации рабочих процессов в гостиницах, оформления гостей при заезде, регистрации граждан, включая иностранных, ведения взаиморасчетов с гостями и контрагентами, для поиска и получения информации о торгах);

- Система контроля управления доступом.

10. В рамках настоящей Политики защиты информации под компонентами информационно-телекоммуникационной инфраструктуры понимаются программные, программно-аппаратные средства, а также телекоммуникационные сети и каналы связи, обеспечивающие функционирование информационных систем Университета, передачу, обработку, хранение и доступ к информации.

К компонентам информационно-телекоммуникационной инфраструктуры Университета относятся:

- Сетевые компоненты и средства передачи данных (локальные вычислительные сети, сетевое оборудование, беспроводные сети и т.д.);

- Серверная и вычислительная инфраструктура (физические серверы, виртуализированные серверные среды и т.д.);

- Программная инфраструктура и системное программное обеспечение (операционные системы серверов и рабочих станций, средства виртуализации, системы управления базами данных и т.д.);

- Пользовательские и периферийные компоненты (автоматизированные рабочие места пользователей, мобильные устройства, средства печати и сканирования, МФУ, съемные носители информации и т.д.).

4. Цели и задачи защиты информации

1. Цели защиты информации:

- обеспечение конфиденциальности, целостности и доступности информации;

- предотвращение несанкционированного доступа к информационным системам и содержащейся в них информации, обнаружение фактов несанкционированного доступа и реагирование на них;

- защита от утечки информации ограниченного доступа и иной конфиденциальной информации;

- предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации и реагирование на них;

- обеспечение устойчивости информационных систем к различного рода угрозам;
- обеспечение непрерывности основных бизнес-процессов Университета;

- минимизация ущерба от инцидентов информационной безопасности;

- соблюдение законодательных и нормативных требований в области обеспечения информационной безопасности;

- предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены и реагирование на них;

- предотвращение несанкционированного удаления информации и программного обеспечения, обнаружение фактов несанкционированного удаления и реагирование на них;

- недопущение использования информационных систем и содержащейся в них информации не по назначению;

- недопущение распространения с использованием информационных систем противоправной информации;

- обеспечение защиты информации при удаленном доступе пользователей к информационным системам.

2. Задачи защиты информации:

- разработка и актуализация положений, регламентов, инструкций и иных локально-нормативных актов, касающихся обеспечения информационной безопасности Университета;

- контроль за выполнением требований по обеспечению информационной безопасности работниками Университета;

- обучение работников Университета основам информационной безопасности, а также информирование работников Университета об актуальных угрозах, схемах мошенничества и рекомендаций от Министерства науки и высшего образования РФ в формате информационных сообщений;

- реализация организационных и технических мероприятий по защите конфиденциальной информации, в том числе: контроль физического доступа в помещения, где обрабатывается конфиденциальная информация, а также к носителям конфиденциальной информации, идентификация и аутентификация пользователей, разграничение прав доступа, регистрация и аудит событий безопасности, защита от вредоносного программного обеспечения посредством использования антивирусного программного обеспечения;

- снижение рисков информационной безопасности на основе анализа угроз и уязвимостей;

- поддержание заданного уровня защищенности информации за счет использования современных средств и методов защиты информации.

5. Принципы защиты информации

Принципы защиты информации:

- соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами, а также целостности и доступности информации;

- соблюдение конфиденциальности сведений, признанных Университетом подлежащими защите, а также целостности и доступности данных сведений;

- дифференцированный подход к обеспечению безопасности информации;

- принцип ответственности и отчетности СамГТУ перед гражданином (в том числе перед работником Университета) за обработку сведений, содержащих его персональные данные;

- учет и контроль всех этапов автоматизированной и неавтоматизированной обработки конфиденциальной информации;

- осведомленности работников Университета, осуществляющих обработку конфиденциальной информации, в вопросах информационной безопасности;

- персональная ответственность работников Университета за выполнение норм информационной безопасности;

- использование принципа минимальных привилегий: доступ конфиденциальной информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.

6. Перечень разрешенного и запрещенного для использования программного обеспечения

В целях обеспечения защиты информации, устойчивого и безопасного функционирования информационных систем и информационно-телекоммуникационной инфраструктуры Университета, а также во исполнение требований законодательства Российской Федерации и нормативных документов уполномоченных органов, в Университете установлены требования к использованию программного обеспечения.

Допускается использование исключительного программного обеспечения, которое:

- используется в рамках образовательной, научной или административно-хозяйственной деятельности;

- соответствует требованиям информационной безопасности;

- официально приобретено, лицензировано или распространяется на законных основаниях (в том числе свободное программное обеспечение);

- при необходимости соответствует требованиям по сертификации или оценке соответствия;

К разрешенному программному обеспечению могут относиться:

- операционные системы и системное программное обеспечение;

- офисные и прикладные программы;

- специализированное учебное и научное программное обеспечение;

- программное обеспечение для администрирования и мониторинга;

- средства защиты информации, в том числе средства криптографической защиты информации;

- программное обеспечение для организации дистанционного обучения;

- программное обеспечение для автоматизации бизнеса, охватывающее бухгалтерию, управление персоналом, торговлю и другие задачи.

Запрещенное к использованию программное обеспечение:

- не имеет законных оснований для использования (нелицензионное);

- «пиратское» программное обеспечение, которое может содержать вредоносный код либо представляет иную угрозу информационной безопасности;

- предназначено для обхода средств защиты информации;

- нарушает требования законодательства Российской Федерации и локально-нормативных актов Университета;

- программное обеспечение, предназначенное для несанкционированного доступа, перехвата или модификации информации;

- программное обеспечение, предназначенное для несанкционированного удаленного управления средствами вычислительной техники.

7. Ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации ими информационных систем

В целях обеспечения защиты информации, устойчивого функционирования информационных систем и предотвращения различного рода угроз информационной безопасности в Университете устанавливаются следующие ограничения и запреты действий пользователей при использовании и обеспечении эксплуатации ими информационных систем:

- использовать информационные системы в целях, не связанных с исполнением должностных обязанностей;

- предоставлять доступ к информационным системам третьим лицам, не имеющим соответствующих полномочий;

- использовать чужие учетные записи для работы в информационных системах либо передавать свои данные учетной записи другим лицам;

- осуществлять доступ к информации, которая не является необходимой для исполнения служебных обязанностей;

- обходить или пытаться обходить установленные меры и средства защиты (в том числе средства криптографической защиты информации);

- отключать, изменять или препятствовать функционированию средств защиты информации (в том числе средств криптографической защиты информации);

- вносить изменения в конфигурацию операционной систему, касающуюся информационной безопасности (отключать брандмауэр, препятствовать регистрации событий безопасности и т.д.).

8. Требования к защите мобильных устройств, планшетных, переносных компьютеров, применяемых пользователями для доступа к информационным системам (за исключением мобильных устройств, предназначенных для доступа к сайтам сети «Интернет» и иным публичным веб-ресурсам) (далее — мобильные устройства):

В целях предотвращения несанкционированного доступа к информации и обеспечения безопасности информационных систем Университета устанавливаются требования к защите мобильных устройств, планшетных компьютеров, ноутбуков и иных переносных средств вычислительной техники, используемых пользователями для доступа к информационным системам и информационным ресурсам Университета. Требования данного пункта являются обязательными для исполнения для всех работников Университета, использующих для исполнения должностных обязанностей личные мобильные устройства.

Доступ с мобильных устройств к информационным системам и информационным ресурсам Университета допускается только при выполнении следующих требований:

- идентификация и аутентификация пользователя перед доступом к информационным системам;

- использование сложны паролей, PIN-кодов либо иных средств аутентификации;

- автоматическая блокировка устройства при отсутствии активности пользователя в течении заданного временного промежутка;

- запрет использования общих учетных записей на одном и том же мобильном устройстве.

Требования к защите информации на мобильных устройствах:

- защита информации, хранимой на устройстве, от несанкционированного доступа;

- использование встроенных или специализированных средств защиты;

- запрет хранения на мобильных устройствах информации ограниченного доступа без служебной необходимости;

- при необходимости применение средств криптографической защиты информации для передачи данных;

- обеспечение возможности удаленной блокировки или удаления данных при утрате устройства.

Пользователи мобильных устройств обязаны:

- обеспечивать физическую сохранность устройств;

- не передавать устройства и средства аутентификации третьим лицам;

- незамедлительно информировать своего непосредственного руководителя или отдел информационной безопасности управления цифровой трансформации о фактах кражи, утраты или компрометации мобильного устройства.

9. Требования к защите физических и виртуальных устройств информационных систем, имеющих постоянный доступ к сети «Интернет»

К физическим и виртуальным устройствам, имеющим постоянный доступ к сети Интернет относятся: серверы, виртуальные машины, сетевые устройства и иные средства вычислительной техники, обеспечивающие функционирование сервисов Университета.

В целях предотвращения несанкционированного доступа, утечки информации и нарушения функционирования информационных систем устанавливаются следующие требования к защите физических и виртуальных устройств:

- физические устройства должны размещаться в специально выделенных и оборудованных помещениях, в которых обеспечивается ограничения физического доступа;

- виртуальные устройства должны размещаться в изолированных сегментах виртуальной инфраструктуры с разграничением доступа к средам управления виртуализацией;

- на физических и виртуальных устройствах должны быть реализованы следующие требования к программной защите:

• установлены актуальные версии операционных систем;

• применены все обновления безопасности;

• отключены неиспользуемые сервисы и службы;

• отключены небезопасные протоколы;

• используются средства защиты информации (при необходимости используются средства криптографической защиты информации);

- администрирование устройств осуществляют только уполномоченные лица, с использованием обязательной идентификацией и аутентификацией, а также с регистрацией и учетом всех административных действий.

10. Категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия

1. Проректор по цифровому развитию:

- Общий контроль и координация работ по обеспечению информационной безопасности, в том числе кибербезопасности Университета;

- Определяет структурное подразделение или назначает отдельных специалистов, на которых возлагаются обязанности (функции) по защите информации;

- Обеспечивает исполнением работниками Университета законов о защите и сохранности персональных данных, а также информации, составляющей служебную и коммерческую тайны.

2. Специалист по информационной безопасности:

- Принимает участие в разработке стратегических документов в области информационной безопасности;

- Ведет техническую документацию, связанную с эксплуатацией систем защиты автоматизированных систем;

- Обеспечивает защиту информации при выводе из эксплуатации автоматизированных систем;

- Обеспечивает защиту информации в автоматизированных системах в процессе их эксплуатации;

- Проводит диагностику систем защиты информации автоматизированных систем;

- Обнаруживает инциденты в процессе эксплуатации автоматизированной системы;

- Проводит оценку защищенности автоматизированных систем с помощью типовых программных средств;

- Администрирует системы защиты информации автоматизированных систем;

- Управляет защитой информации в автоматизированных системах;

- Осуществляет мониторинг защищенности информации в автоматизированных системах;

- Проводит аудит защищенности информации в автоматизированных системах;

- Устанавливает и настраивает средства защиты информации в автоматизированных системах;

- Разрабатывает организационно-распорядительные документы по информационной безопасности в автоматизированных системах;

- Внедряет организационные меры по информационной безопасности в автоматизированных системах;

- Разрабатывает проектные решения по информационной безопасности в автоматизированных системах.

3. Начальник управления информатизации и телекоммуникаций:

- Осуществляет руководство персоналом системы учета, управления и предоставления информационных ресурсов Университета и осуществляет контроль за их выполнением;

- Разрабатывает необходимую нормативную, регламентирующую и организационную документацию по информатизации, соответствующую требованиям Университета, а также законодательству Российской Федерации;

- Осуществляет руководство разработкой планов работы по обеспечению информационным ресурсами структурных подразделений Университета и осуществляет контроль за их выполнением;

- Организует взаимодействие с внешними поставщиками информационно-телекоммуникационных услуг и оборудования;

- Организует развитие единой компьютерной сети Университета, подключение ее к информационно-телекоммуникационной сети Интернет, и обеспечивает ее функционирование.

4. Начальник управления цифровой трансформации:

- Организует, контролирует и принимает участие в обеспечении надежности, эффективности функционирования и безопасности информационных систем и информационно-технологической инфраструктуры;

- Участвует в организации и координации работ, связанных с защитой информации, включая разработку политики информационной безопасности и организации мероприятий по ее реализации;

- Организует разработку нормативных документов Университета в области защиты информации.

.

11. Состав организационной системы управления деятельностью по защите информации и схема взаимодействия ее элементов

Организационная система управления защитой информации в Университете построена по иерархическому принципу с разделением функций стратегического управления, реализации и контроля.

Схема приведена в Приложении 1 к настоящей Политике.

12. Ответственность работников за нарушение требований о защите информации

1. Руководители структурных подразделений несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях, обязаны незамедлительно сообщать в отдел информационной безопасности управления цифровой трансформации обо всех инцидентах, связанных с нарушениями требований информационной безопасности;

За нарушение требований настоящей Политики, а также иной внутренней локально-нормативной документации в сфере информационной безопасности (в том числе инструкция пользования информационными системами) работники несут персональную ответственность;

2. За разглашение персональных данных, нарушение порядка работы с документами и (или) машинными носителями, содержащими такую информацию, и иные нарушения безопасности информации, обрабатываемой в информационных системах персональных данных Университета, работники могут быть привлечены к ответственности в соответствии с действующим законодательством Российской Федерации;

3. Работники несут персональную ответственность за использование идентификаторов и паролей, не соответствующих требованиям, установленным в соответствующей внутренней локально-нормативной документации, а также за разглашение парольной информации;

4. Работники несут персональную ответственность за своевременное информирование о произошедших инцидентах информационной безопасности своего непосредственного руководителя или отдела информационной безопасности управления цифровой трансформации;

5. Работники несут персональную ответственность в соответствии с действующим законодательством Российской Федерации за использование запрещенного или несанкционированного программного обеспечения;

6. Пользователи несут персональную ответственность в соответствии с действующим законодательством Российской Федерации за несоблюдение требований защиты информации при использовании мобильных устройств;

7. Нарушение пунктов обязательства о неразглашении конфиденциальной информации влечет наложение дисциплинарной, уголовной, административной, гражданско-правовой ответственности в соответствии с законодательством Российской Федерации;

8. Проректор по цифровому развитию несет ответственность за контроль исполнения требований настоящей политики, локальных нормативных актов по обеспечению информационной безопасности и законодательных актов в области защиты информации.

8. Отдел информационной безопасности управления цифровой трансформации несет ответственность за контроль исполнения настоящей Политики, обеспечение выполнения требований регуляторов и реагирование на инциденты информационной безопасности.

13. Заключительные положения

1. Настоящая Политика вступает в юридическую силу с момента ее утверждения приказом Ректора СамГТУ.

2. Дополнения и изменения в настоящую Политику принимаются и утверждаются приказом ректора ФГБОУ ВО «СамГТУ».

3. Политика после вступления в юридическую силу действует без определенного срока до принятия новой редакции.

Приложение 1

Схема взаимодействия элементов организационной системы управления деятельностью по защите информации