РОССИЙСКИЙ ХИМИКО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ имени Д.И. Менделеева
Классический университет

D.Mendeleev University of Chemical Technology of Russia

СТО РХТУ 11.1-01-2022

СТАНДАРТ ОРГАНИЗАЦИИ

Система менеджмента качества

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

г. Москва – 2022 г.

Предисловие

1. Разработан Федеральным государственным бюджетным образовательным учреждением высшего образования «Российский химико-технологический университет имени Д.И. Менделеева» (далее – РХТУ им. Д.И. Менделеева).
2. Утвержден и введен в действие приказом Ректора РХТУ им. Д.И. Менделеева от «30» ноября 2022 года № 178 ОД.
3. Введен взамен СТО РХТУ 7.5-04-2020.
4. Периодическая проверка производится представителем руководства по качеству с интервалом, не превышающим три года.

Содержание

СОГЛАСОВАНО
Начальник _____ВП МО РФ

_____

«___» _____ 2022 г.

УТВЕРЖДАЮ
И.о. ректора РХТУ им. Д.И. Менделеева

_____И.В. Воротынцев

«___» _____ 2022 г.

СТО РХТУ 11.1-01-2022

СТАНДАРТ ОРГАНИЗАЦИИ

Система менеджмента качества

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Дата введения _____._____.2022

1 Область применения

1.1 Настоящий стандарт организации (СТО) РХТУ им. Д.И. Менделеева:

– определяет порядок организации и выполнения работ по защите информации об образцах военной продукции, учитывающий характер и условия выполнения оборонного заказа при несанкционированном воздействии на информацию, циркулирующую в технических каналах;

– определяет требования к управлению информационной безопасностью в организации.

1.2 РХТУ им. Д.И. Менделеева не разрабатывает и не производит изделия информационных технологий в защищенном исполнении, предназначенные для применения в военной продукции, в связи с этим процедуры обеспечения и контроля безопасности технологий их разработки и производства в соответствии с требованиями п. 4.3.4 ГОСТ РВ 0015-002 не разрабатывались.

1.3 Настоящий стандарт разработан с учетом требований ГОСТ Р ИСО 9001 и ГОСТ РВ 0015-002.

1.4 При разработке стандарта были использованы отдельные положения ГОСТ Р ИСО/МЭК 27001.

1.5 РХТУ им. Д.И. Менделеева сохраняет за собой право изменять содержание СТО.

1.6 Корректировать СТО имеет право Ректор или начальник отдела качества по поручению Ректора. Откорректированный стандарт утверждает Ректор.

1.7 Копии СТО и изменений к нему рассылает менеджер по качеству согласно «Списку рассылки». Оригинал СТО на бумажном носителе информации хранится в службе качества организации.

1.8 При отсутствии на момент применения данного стандарта в штатном расписании организации должности, упоминаемой в нём, функции (обязанности), предусмотренные стандартом применительно к такой должности возлагаются приказом Ректора на одного из сотрудников.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

Постановление Совета Министров Правительства Российской Федерации от 15 сентября 2003 г. № 912-51 Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от утечки по техническим каналам

ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования

ГОСТ РВ 0015-002-2020 Система разработки и постановки на производство военной техники. Системы менеджмента качества. Общие требования

ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ РВ 50859

ГОСТ РВ 50934

Приказ ФСТЭК России от 20 октября 2016 г. № 025 Требования по технической защите информации, содержащей сведения, составляющие государственную тайну

РК РХТУ 4.3-01-2022 СМК Руководство по качеству

СТО РХТУ 7.5-01-2022 СМК Управление документированной информацией

Примечание – При пользовании настоящим стандартом целесообразно проверять действие ссылочных стандартов. Если ссылочный стандарт заменён (изменён), то при пользовании настоящим стандартом следует руководствоваться заменяющим (изменённым) стандартом. Если ссылочный стандарт отменён без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте используются следующие термины и их определения:

3.1 **требование:** потребность или ожидание, которое установлено, обычно предполагается или является обязательным.

3.2 **доступность**: свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

3.3 **несоответствие**: невыполнение требования.

3.4 **коррекция**: действие, предпринятое для устранения обнаруженного несоответствия.

3.5 **корректирующее действие**: действие, предпринятое для устранения причины обнаруженного несоответствия или другой нежелательной ситуации.

3.6 **предупреждающее действие**: действие, предпринятое для устранения причины потенциального несоответствия или другой потенциально нежелательной ситуации

3.7 **конфиденциальность**: свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

3.8 **информационная безопасность (ИБ)**: свойство информации сохранять конфиденциальность, целостность и доступность.

3.9 **событие информационной безопасности**: идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

3.10 **инцидент информационной безопасности**: любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание – инцидентами информационной безопасности являются:

– утрата услуг, оборудования или устройств;

– системные сбои или перегрузки;

– ошибки пользователей;

– несоблюдение политики или рекомендаций ИБ;

- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушения правил доступа.

4 Обозначения и сокращения

В настоящем СТО использованы следующие обозначения и сокращения:

ВП – военное представительство;

ДС – документы по стандартизации;

ИБ – информационная безопасность;

ОБИ – обеспечение безопасности информации;

ПДТК – постоянно действующая техническая комиссия;

СМК – система менеджмента качества;

СТО – стандарт организации.

5 Ответственность и контроль

5.1 Ответственность за разработку данного стандарта, за организацию и выполнение работ по защите информации об образцах военной продукции возлагается на начальника отдела защиты информации.

5.2 Ответственность за организацию соблюдения режима секретности в организации согласно Инструкции [2] несет Ректор.

5.3 Ответственность за организацию управления информационной безопасностью организации возлагается на проректора по науке.

5.4 Контроль выполнения требований стандарта возлагается на начальника первого отдела.

6 Описание процедуры

6.1 Общие положения

6.1.1 Порядок организации и выполнения работ по защите информации (относящейся к сведениям, составляющим государственную тайну) об образцах военной продукции, учитывающий характер и условия выполнения оборонного заказа при несанкционированном воздействии на информацию, циркулирующую в технических каналах, изложен в Инструкции по обеспечению режима секретности, разработанной с учетом требований [1] – [4], ГОСТ РВ 0043–001–2019 и ГОСТ РВ 0043–002–2019.

6.1.2 Процедура управления информационной безопасностью организации в отношении активов, не относящимся к сведениям, составляющим государственную тайну, изложена в настоящем стандарте.

6.1.3 Цель процедуры управления информационной безопасностью – обеспечить конфиденциальность, целостность и доступность информации, циркулирующей в организации с конечной целью защиты активов организации.

6.1.4 Основные задачи процедуры:

– обеспечение участия высшего руководства организации в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями организации, законами и нормативными актами;

– предотвращение несанкционированного физического доступа, повреждений и воздействий на имущество и информацию организации, а также имущества, принадлежащего потребителю (заказчику);

– предотвращение потерь, повреждений, хищений или компрометации активов и прекращение деятельности организации;

– обеспечение надлежащего и безопасного функционирования средств обработки информации;

– защита целостности программного обеспечения и массивов информации;

– предотвращение несанкционированного разглашения, модификации, удаления или уничтожения активов и прерывание процессов СМК;

– обнаружение несанкционированных действий, связанных с обработкой информации;

– предотвращение несанкционированного доступа пользователей, а также компрометацию или кражу информации и средств обработки информации;

– обеспечение оперативного оповещения о событиях информационной безопасности и нарушениях, связанных с информационными системами, а также своевременное проведение коррекции и корректирующих действий.

6.1.5 Действия по управлению информационной безопасностью включает в себя:

– планирование;

– выявление событий и инцидентов ИБ;

– идентификацию и регистрацию событий и инцидентов ИБ;

– анализ событий и инцидентов ИБ;

– планирование и осуществление необходимых корректирующих и предупреждающих действий;

– оценку результативности принятых действий.

6.1.6 ВП имеет беспрепятственный доступ к носителям сведений, составляющих государственную тайну (включая записи, сведения и другие информационные ресурсы) в части выполнения ГОЗ.

Доступ ВП к документации, содержащей сведения, составляющие государственную тайну, осуществляется в соответствии с требованиями закона [1] и инструкции [2].

7 Сведения, составляющие коммерческую тайну

7.1 В общем случае к коммерческой тайне организации относятся:

– сведения о состоянии банковских счетов и проводимых финансово-хозяйственных операциях;

– сведения о кредиторской задолженности организации, за исключением задолженности по выплате заработной платы и иных социальных выплат;

– сведения о плановых и фактических показателях финансово-хозяйственной деятельности;

– сведения о рентабельности организации;

– сведения о структуре и масштабах производства, производственных мощностях, запасах сырья, материалов, комплектующих и готовой продукции;

– сведения о подготовке, принятии и исполнении отдельных решений руководства организации по коммерческим, организационным, производственным и научно-техническим вопросам;

– сведения о планах расширения или свертывания производства различных видов продукции;

– сведения о рыночной стратегии организации;

– систематизированные сведения о внутренних и зарубежных заказчиках, поставщиках, потребителях, спонсорах и других партнерах деловых отношений организации;

– систематизированные сведения о внутренних и зарубежных предприятиях, как о потенциальных конкурентах в деятельности организации;

– сведения о подготовке, проведении и результатах переговоров с деловыми партнерами организации;

– сведения, условие конфиденциальности которых установлено в договорах и других обязательствах организации;

– сведения о методах, расчетах, структуре, уровне реальных цен на продукцию;

– сведения о целях, задачах, программах перспективных научных исследований, ключевые идеи научных разработок;

– сведения об особенностях используемых и разрабатываемых технологий и специфике их применения;

– конструкторская документация на выпускаемую продукцию.

7.2 К сведениям, составляющим коммерческую тайну организации, также может относиться конструкторская, программная и технологическая документация на выпускаемую продукцию.

7.3 В соответствии с Постановлением правительства от 5 декабря 1991 г. № 35 не могут составлять коммерческую тайну:

– учредительные документы (решение о создании организации или договор учредителей) и Устав;

– документы, дающие право заниматься предпринимательской деятельностью (документы, подтверждающие факт внесения записей о юридических лицах в Единый государственный реестр юридических лиц, свидетельства о государственной регистрации индивидуальных предпринимателей, лицензии, патенты);

– сведения по установленным формам отчетности о финансово - хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему;

– документы о платежеспособности;

– сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

– документы об уплате налогов и обязательных платежах;

– сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства и размерах причиненного при этом ущерба;

– сведения об участии должностных лиц организации в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

8 Организация работ со сведениями, составляющими коммерческую тайну

8.1 Для обеспечения работ, связанных с использованием сведений, составляющих коммерческую тайну, а также для организации мероприятий по защите коммерческой тайны в организации назначен начальник общего отдела.

8.2 Доступ к сведениям, составляющим коммерческую тайну, осуществляется начальником общего отдела в соответствии с данным стандартом организации и другими ДС.

8.3 Все работы с документами, содержащими коммерческую тайну, осуществляются начальником общего отдела исключительно на территории организации.

9 Реализация требований по защите информации

9.1 Режим конфиденциальности в организации обеспечивается:

– проведением соответствующих организационных мероприятий (организация работы отдела защиты информации, разработка соответствующих регламентирующих документов, принятием сотрудниками организации обязательств по неразглашению коммерческой тайны и др.);

– соблюдением сотрудниками организации требований нормативных документов, регламентирующих правила допуска к коммерческой тайне и ведения секретного делопроизводства;

– ведением в организации документооборота в соответствии с требованиями СТО РХТУ 7.5-01-2022;

– использованием организационных и программных мер по предотвращению несанкционированного доступа к информации (конструкторской документации), выполненной на электронных носителях, и находящейся в электронном архиве организации.

10 Обязанности и полномочия должностных лиц по обеспечению защиты коммерческой тайны и конфиденциальности работ

10.1 Обязанности сотрудников отдела защиты информации определены в должностных инструкциях.

10.2 Каждый сотрудник организации обязан:

– строго хранить в тайне сведения, ставшие известными по работе или иным путем;

– пресекать действия других лиц, которые могут привести к разглашению сведений, составляющих коммерческую тайну;

– неукоснительно соблюдать установленные в организации пропускной режим, оказывать содействие в их обеспечении;

– неукоснительно выполнять требования, регламентирующие выполнение мер при проведении закрытых совещаний, встрече и работе с иностранцами, а также при командировании на другие объекты (режимные, совместные предприятия и иностранные фирмы);

– информировать Ректора о попытках получения информации о деятельности организации в закрытых областях, о попытках контактов со стороны иностранцев.

10.3 Сотрудникам организации запрещается:

– снимать копии с документов, составляющих коммерческую тайну;

– выполнять работы, связанные с коммерческой тайной дома;

– находиться в помещениях сверх установленного времени, без разрешения соответствующих должностных лиц организации.

Библиография

[1] Закон Российской Федерации от 21 июля 1993 г. №5485-1 «О государственной тайне»

[2] Инструкция по обеспечению режима секретности в Российской Федерации (утверждена постановлением Правительства Российской Федерации от 5 января 2004 г. №3-1)

[3] Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от утечки по техническим каналам (утверждено постановлением Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №912-51)

[4] Требования (утверждены приказом ФСТЭК России от 20 октября 2016 г. №025

Лист регистрации изменений

Номер извещения	Номера листов (страниц)				Подпись	Расшифровка подписи	Дата внесения изменения
	измененных	замененных	новых	аннулированных			

Лист согласования

Должность	Подпись, дата	Расшифровка подписи
Разработчик стандарта:		
Начальник отдела защиты информации		
Согласовано:		

Лист ознакомления

Должность	Подпись, дата	Расшифровка подписи