Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

И Н С Т Р У К Ц И Я О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Инструкция по организации антивирусной защиты

ОРИГИНАЛ

Содержание

УТВЕРЖДЕНА
Приказом ректора
(чем) (должность)
от «28» января 2022 г. № 40-О
(дата)

И Н С Т Р У К Ц И Я О Р Г А Н И З А Ц И И
СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Инструкция по организации антивирусной защиты — Введена впервые

1 Область применения

1.1 Настоящая инструкция определяет требования к организации антивирусной защиты в федеральном государственном бюджетном образовательном учреждении высшего образования «Иркутский национальный исследовательский технический университет» (далее - ФГБОУ ВО «ИРНИТУ») и устанавливает ответственность работников, использующих и сопровождающих информационные системы, за выполнение требований настоящей инструкции.

1.2 Требования данной инструкции распространяются на работников ФГБОУ ВО «ИРНИТУ», использующих в своей деятельности средства вычислительной техники и должны применяться для всех средств вычислительной техники, эксплуатируемой в ФГБОУ ВО «ИРНИТУ».

2 Нормативные ссылки

Настоящая инструкция разработана в соответствии и содержит ссылки на следующие нормативные документы:

Конституция Российской Федерации.

Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства Российской Федерации от 21.03.2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми.

Устав ФГБОУ ВО «ИРНИТУ».

СТО 002 Система менеджмента качества. Порядок управления документированной информацией (документами) СМК.

3 Термины, определения и сокращения

3.1 В настоящей инструкции применены следующие термины с соответствующими определениями:

Автоматизированное рабочее место – программно-технический комплекс,

располагающийся, непосредственно на рабочем месте сотрудника, предназначенный для автоматизации его работы и обработки информации.

Работник, использующий АРМ – работник ФГБОУ ВО «ИРНИТУ» применяющий АРМ в своей деятельности.

Работник, сопровождающий АРМ – работник ФГБОУ ВО «ИРНИТУ» обеспечивающий работоспособность АРМ.

Система антивирусной защиты – это совокупность управленческих и правовых действий, программно-аппаратных средств, объединяемых в единый комплекс для создания надежной антивирусной защиты информационных систем, находящихся в локальной сети.

Система менеджмента качества – часть системы менеджмента применительно к качеству.

Средство антивирусной защиты – специализированная программа для обнаружения компьютерных вирусов и нежелательных (считающихся вредоносными) программ, а также для предотвращения заражения (модификации) файлов или операционной системы и восстановления зараженных (модифицированных) такими программами файлов.

Средства вычислительной техники – компьютеры, к которым относятся используемые для общей работы персональные компьютеры, сетевые рабочие станции, серверы и другие типы компьютеров.

Стандарт организации – нормативный документ по стандартизации, разработанный, как правило, на основе согласия, характеризующегося отсутствием возражений по существенным вопросам у большинства заинтересованных сторон, устанавливающий комплекс норм, правил, требований к различным видам деятельности университета или их результатам и утвержденный приказом руководства университета.

Съемный носитель – переносное устройство хранения информации, временно подключаемое к компьютерам, ноутбукам, планшетам и т.д. через стандартные разъёмы.

Телекоммуникационный канал – внешний канал связи, который соединяет две или более сети.

3.2 В настоящей инструкции используются следующие сокращения:

АРМ – автоматизированное рабочее место;

САЗ – средство антивирусной защиты;

СМК – система менеджмента качества;

СТО – стандарт организации;

ФГБОУ ВО «ИРНИТУ» – Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский национальный исследовательский технический университет».

4 Ответственность

4.1 Ответственность за разработку, пересмотр, идентификацию внесенных изменений в данную инструкцию возложена на начальника отдела информационной безопасности и документооборота ФГБОУ ВО «ИРНИТУ».

4.2 Разработчик настоящей инструкции осуществляет периодическую проверку (пересмотр) данного документа в установленном порядке согласно СТО 002 Система менеджмента качества. Порядок управления документированной информацией (документами) СМК.

4.3 Ответственность за выполнение требований данной инструкции возлагается на все должностные лица и подразделения ФГБОУ ВО «ИРНИТУ», использующих в своей деятельности средства вычислительной техники.

5 Общие положения

5.1 Целью создания системы антивирусной защиты является обеспечение защищенности информационно-телекоммуникационной системы от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа работников и обучающихся ФГБОУ ВО «ИРНИТУ» к непродуктивным Интернет-ресурсам и защиты электронной переписки работников.

5.2 В ФГБОУ ВО «ИРНИТУ» допускается использование только лицензионных средств антивирусной защиты (далее – САЗ), официально приобретенных у поставщиков антивирусного программного обеспечения.

5.3 Для объектов информатизации, аттестованных по требованиям безопасности информации, необходимо применять САЗ, сертифицированные в установленном порядке.

5.4 Основным САЗ в ФГБОУ ВО «ИРНИТУ» является централизованная сетевая антивирусная система, функционирующая на всех АРМ, подключенных к корпоративной сети передачи данных ФГБОУ ВО «ИРНИТУ», обслуживаемая отделом информационной инфраструктуры.

5.5 Запрещается эксплуатация средств вычислительной техники без установленных САЗ, а также с установкой нескольких САЗ. При выявлении АРМ с несколькими установленными одновременно САЗ работниками отдела информационной безопасности и документооборота проводится внутреннее расследование с целью выявления работника, установившего второе САЗ. С данным работника проводится профилактическая беседа с целью разъяснения недопустимости данного действия. При повторном нарушении к работнику могут быть применены меры дисциплинарного характера.

5.6 Установка основного САЗ осуществляется работниками отдела информационной инфраструктуры при вводе в эксплуатацию нового средства вычислительной техники.

5.7 В случае обоснованной необходимости использования других САЗ, их применение необходимо согласовать с начальником управления информатизации с назначением ответственного за их эксплуатацию приказом ректора ФГБОУ ВО «ИРНИТУ». Установка альтернативного САЗ осуществляется работниками, сопровождающими данную АРМ.

5.8 На автоматизированных рабочих местах информационных систем (далее – АРМ) запрещается установка программного обеспечения, не связанного с выполнением служебных обязанностей пользователя АРМ.

5.9 Централизованное управление и мониторинг функционирования САЗ осуществляется работниками отдела информационной инфраструктуры. Работники отдела информационной безопасности и документооборота имеют право проводить мониторинг функционирования САЗ.

6 Применение средств антивирусной защиты

6.1 Обязательному антивирусному контролю подлежат все средства вычислительной техники, а также любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам и линиям связи, а также информация на съемных носителях. САЗ может не использоваться по решению работника ответственного за его эксплуатацию, в случаях, если системное программное обеспечение, установленное на средстве вычислительной техники, конфликтует с САЗ или делает его установку излишней.

6.2 Антивирусный контроль на АРМ должен проводиться ежедневно в автоматическом режиме при начальной загрузке и текущей работе АРМ (для серверов – при перезапуске).

6.3 Обновление баз антивирусных средств должно проводиться регулярно в автоматическом режиме, для чего должен быть настроен прямой доступ к серверам обновлений разработчика

антивирусного средства или доступ к локальному серверу антивирусной защиты. В случае невозможности настроить автоматическое обновление САЗ, необходимо один раз в неделю подключать данное средство вычислительной техники к локальной сети, в которой настроен доступ к серверу антивирусной защиты данного САЗ, или осуществлять обновление антивирусных баз с внешнего носителя и проверку средств вычислительной техники на наличие вирусов.

6.4 Антивирусный контроль входящей информации, в том числе при разархивировании, должен проводиться непосредственно после получения информации. Антивирусный контроль исходящей информации должен проводиться непосредственно перед отправкой (записью на съемный носитель).

6.5 На АРМ аттестованных по требованиям безопасности информации установка (изменение) системного и прикладного программного обеспечения должна осуществляться только работником, которому была предоставлена роль системного администратора для данного АРМ. Установка средств защиты информации должна осуществляться только работником, которому была предоставлена роль администратора информационной безопасности для данного АРМ Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. В случае, когда САЗ не имеет режима проверки в реальном времени или данный режим отключен, непосредственно после установки (изменения) системного программного обеспечения должна проводиться повторная антивирусная проверка.

7 Действия при обнаружении вирусов

7.1 При возникновении подозрения на наличие в системе компьютерного вируса (нетипичная работа программ, искажение данных, частое появление сообщений о системных ошибках и т.п.) должен быть проведён внеочередной антивирусный контроль средства вычислительной техники (самостоятельно или при необходимости вместе с работником отдела информационной инфраструктуры, либо отдела информационной безопасности и документооборота).

7.2 В случае обнаружения при проведении антивирусной проверки наличия в системе компьютерного вируса работники ФГБОУ ВО «ИРНИТУ» обязаны приостановить работу, отключить средство вычислительной техники от локальной сети и немедленно поставить в известность специалиста отдела информационной инфраструктуры (тел. 40-50-12).

7.3 В случае обнаружения наличия в системе компьютерного вируса работник, сопровождающий данную АРМ:

a) совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

b) провести лечение или уничтожение зараженных файлов;

c) в случае обнаружения вируса, не поддающегося автоматическому обнаружению применяемыми антивирусными средствами, передать зараженный вирусом файл разработчикам САЗ. Решение о дальнейшем использовании АРМ принимает работник ответственный за эксплуатацию САЗ.

Приложение 1 Лист согласования Инструкции по организации антивирусной защиты
(обязательное)

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Дата	Подпись
Проректор по цифровой трансформации	А.Н. Копайгородский	28.01.22	
Начальник управления информатизации	В.В. Шмелев	19.01.22	
Начальник отдела информационной инфраструктуры	П.И. Антонов	19.01.2022	
Заместитель начальника отдела мониторинга и качества образовательных услуг	О.С. Артемова	19.01.2022	

РАЗРАБОТАНО:

Начальник отдела информационной безопасности и документооборота	Л.В. Бархатова	19.01.2022	

Приложение 2 Лист регистрации изменений Инструкции по организации антивирусной защиты

(обязательное)

Порядковый номер изменения	**Основание (№ приказа, дата)**	**Дата введения изменения**	**Изменения внёс**	
			Фамилия, инициалы	**Подпись вносившего изменения, дата внесения**
1	2	3	4	5

Приложение 3 Лист ознакомления с Инструкцией по организации антивирусной защиты
(обязательное)

№	И.О. Фамилия	Должность	Дата	Подпись