

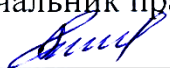
	Система менеджмента качества РИ С.004-2023 Инструкция по антивирусной защите ФГБОУ ВО «КнАГУ»	с. 1 из 10
--	---	------------


РАБОЧАЯ ИНСТРУКЦИЯ

Система менеджмента качества
ИНСТРУКЦИЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ
ФГБОУ ВО «КнАГУ»

РИ С.004-2023
Введена впервые

СОГЛАСОВАНО

Начальник правового управления
 А.В. Ременников
«02» ноября 2023 г.

Начальник ИТ-Управления
 Е.Б. Абарникова
«1» 11 2023 г.

УТВЕРЖДАЮ

Ректор университета
 Э.А. Дмитриев
«03» 11 2023 г.



Комсомольск-на-Амуре
2023

	Система менеджмента качества РИ С.004-2023 Инструкция по антивирусной защите ФГБОУ ВО «КнАГУ»	с. 2 из 10
--	---	------------

Содержание

1 Назначение и область применения	3
1.1 Назначение	3
1.2 Сфера действия	3
1.3 Область применения.....	3
2 Нормативные ссылки	3
3 Термины и определения.....	3
4 Ответственность.....	4
5 Требования к антивирусным средствам.....	5
6 Права и обязанности	6
7 Порядок и периодичность обновления антивирусных баз	6
8 Порядок и периодичность проведения антивирусного контроля	7
9 Порядок действий при обнаружении вирусов	8
10 Разработчики.....	9
Лист регистрации изменений	10

	Система менеджмента качества РИ С.004-2023 Инструкция по антивирусной защите ФГБОУ ВО «КнАГУ»	с. 3 из 10
--	---	------------

1 Общие положения

1.1 Назначение

Настоящая Инструкция по антивирусной защите (далее – Инструкция) ФГБОУ ВО «КнАГУ» (далее – Университет) регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля. Инструкция устанавливает требования и ответственность при организации защиты информации от разрушающего воздействия вредоносных программ – компьютерных вирусов.

1.2 Сфера действия

Инструкция распространяется на все автоматизированные рабочие места сотрудников ФГБОУ ВО «КнАГУ» и обязательна к использованию во всех структурных подразделениях университета.

1.3 Область применения

Указанные в настоящей инструкции правила и требования должны применять все сотрудники ФГБОУ ВО «КнАГУ», использующие в своей работе автоматизированные рабочие места в соответствии и в рамках своих должностных обязанностей.

2 Нормативные ссылки

Настоящая инструкция составлена на основе следующих нормативных документов:

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

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

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

3 Термины и определения

В настоящей инструкции применяются следующие термины с соответствующими определениями:

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая инфор-

	Система менеджмента качества РИ С.004-2023 Инструкция по антивирусной защите ФГБОУ ВО «КнАГУ»	с. 4 из 10
--	---	------------

мационную технологию выполнения установленных функций.

Автоматизированное рабочее место (АРМ) - программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

Антивирусная программа (антивирус) - специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов, а также предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Данные - информация, представленная в электронной форме.

Интернет - всемирная система объединённых компьютерных сетей для хранения и передачи информации.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь - сотрудник университета, использующий АРМ.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

4 Ответственность

Пользователи и Ответственный за обеспечение безопасности ПДн в ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

	Система менеджмента качества РИ С.004-2023 Инструкция по антивирусной защите ФГБОУ ВО «КнАГУ»	с. 5 из 10
--	---	------------

5 Требования к антивирусным средствам

5.1 В Университете к применению допускаются только лицензионные антивирусные программные и (или) программно-аппаратные средства (антивирусные средства), закупленные у разработчика указанных средств или его официальных дилеров.

5.2 Антивирусные средства должны функционировать в течение всего времени работы средств вычислительной техники (от момента загрузки операционной системы до момента ее выгрузки).

5.3 Антивирусное средство не должно существенно затруднять работоспособность средств вычислительной техники информационных систем персональных данных (далее – ИСПДн).

6 Права и обязанности

6.1 Антивирусной защите подлежит вся, обрабатываемая информация в Университете, при помощи средств вычислительной техники, независимо от ограничений доступа к ней.

6.2 Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

6.3 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

6.4 В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

6.5 Сопровождение (регулярное обновление, антивирусный контроль, выявление фактов заражения и проведение служебных расследований) правил антивирусной защиты возлагаются на ответственного за обеспечение безопасности ПДн в ИСПДн.

6.6 Основные задачи ответственного за обеспечение безопасности ПДн в ИСПДн:

- организация процесса установки антивирусных средств в ИСПДн;
- сопровождение антивирусных средств (обновление, антивирусный контроль, сопровождение действий пользователей в случаях обнаружения вирусов, обеспечение работоспособности антивирусных средств);
- контроль состояния системы антивирусной защиты информации в Университете.

6.7 Ответственный за обеспечение безопасности ПДн в ИСПДн несет ответственность за:

- за своевременную установку антивирусных средств;
- за эксплуатацию (антивирусный контроль, работоспособность ан-

	Система менеджмента качества РИ С.004-2023 Инструкция по антивирусной защите ФГБОУ ВО «КнАГУ»	с. 6 из 10
--	---	------------

тивирусных средств, сопровождение действий пользователей в случаях обнаружения вирусов) системы антивирусной защиты информации;

- за своевременное обновление лицензий на антивирусные средства;
- за своевременное обновление антивирусных баз.

6.8 Ответственный за обеспечение безопасности ПДн в ИСПДн имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации;
- принимать участие в планировании мероприятий по антивирусной защите информации и планировании оснащения антивирусными средствами;
- осуществлять контроль состояния средств антивирусной защиты информации в Университете;
- инициировать служебные проверки и участвовать в проведении расследований по фактам заражения вирусами ИСПДн и средств вычислительной техники;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты.

6.9 Пользователь антивирусного средства – лицо, на рабочем месте которого применяется антивирусное средство.

6.10 Пользователям антивирусных средств запрещается:

- менять настройки или отключать средства антивирусной защиты во время работы;
- использовать средства антивирусной защиты, отличные от установленных средств;
- без разрешения ответственного за обеспечение безопасности ПДн в ИСПДн копировать любые файлы на съемные носители информации, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

7 Порядок и периодичность обновления антивирусных баз

7.1 Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

7.2 Установке обновлений должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

7.3 Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий указанного программного обеспечения.

	Система менеджмента качества РИ С.004-2023 Инструкция по антивирусной защите ФГБОУ ВО «КнАГУ»	с. 7 из 10
--	---	------------

7.4 Периодичность обновления антивирусных баз:

- обновление антивирусных баз для всех ИСПДн, имеющих подключение к сетям общего пользования и сетям международного информационного обмена, должно быть ежедневным. Источник обновления – сервер разработчика антивирусного средства, либо собственный централизованный сетевой источник обновлений, получающий обновления с сервера разработчика антивирусного средства.

- обновление антивирусных баз для ИСПДн, не имеющих подключение к сетям общего пользования и сетям международного информационного обмена, обновление должно быть не менее 1 раза в неделю. Источником обновления в данном случае являются антивирусные базы, записанные на предварительно учтенный в установленном порядке съемный машинный носитель информации.

8 Порядок и периодичность проведения антивирусного контроля

8.1 Объектами антивирусного контроля являются:

- жесткие магнитные диски рабочих станций и серверов ИСПДн;
- сетевые хранилища (системы хранения данных);
- оперативная и системная память средств вычислительной техники;
- съемные машинные носители информации;
- входящий и исходящий контент (веб-трафик);
- файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена;
- почтовые сообщения электронной почты.

8.2 Антивирусный контроль входящей информации со съемных машинных носителей информации необходимо проводить до переноса информации на жёсткий магнитный диск рабочей станции или сетевой диск. Информация, получаемая по телекоммуникационным каналам, должна проверяться во время, или сразу после получения. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

8.3 Виды и периодичность антивирусных проверок представлены в таблице 1.

Таблица 1

№ п/п	Объект контроля	Вид проверки	Периодичность проверки
1	Жесткие магнитные диски рабочих станций и серверов ИСПДн	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю
2	Сетевые хранилища (системы хранения данных)	Полная проверка	1 раз в месяц

	Система менеджмента качества РИ С.004-2023 Инструкция по антивирусной защите ФГБОУ ВО «КнАГУ»	с. 8 из 10
--	---	------------

№ п/п	Объект контроля	Вид проверки	Периодичность проверки
3	Оперативная и системная память средств вычислительной техники	Полная проверка	1 раз в месяц
		Быстрое сканирование	1 раз в неделю
4	Съемные машинные носители информации	Полная проверка	При каждом подключении
5	Веб-трафик	Минимально необходимое требование - настройка антивирусного средства по умолчанию	Постоянно
6	Файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена	Полная проверка	При каждом получении и отправке
7	Почтовые сообщения электронной почты	Минимально необходимое требование - настройка антивирусного средства по умолчанию	При каждом получении и отправке

9 Порядок действий при обнаружении вирусов

9.1 Основными путями проникновения вирусов в ИСПДн являются: любые съемные машинные носители информации, электронные почтовые сообщения, трафик, получаемый из сетей общего пользования и сетей международного информационного обмена, ранее зараженные рабочие станции и сервера.

9.2 В случае обнаружения вирусов при входном контроле съемных машинных носителей информации, файлов или электронных почтовых сообщений, пользователь должен:

- немедленно приостановить все работы на своей рабочей станции;
- сообщить ответственному за обеспечение безопасности ПДн в ИСПДн о факте обнаружения вируса;
- принять согласованные с ответственным за обеспечение безопасности ПДн в ИСПДн меры по локализации и удалению вируса с использованием антивирусных средств.

9.3 При невозможности ликвидации последствий вирусного заражения ответственному за обеспечение безопасности ПДн в ИСПДн необходимо:

- сообщить о факте обнаружения программных вирусов в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;
- заархивировать зараженные файлы и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирус-

	Система менеджмента качества РИ С.004-2023 Инструкция по антивирусной защите ФГБОУ ВО «КнАГУ»	с. 9 из 10
--	---	------------

ной защиты информации.

9.4 При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению ответственного за обеспечение безопасности ПДн в ИСПДн.

9.5 Факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ – все это относится к значимым нарушениям безопасности информации и должны быть проанализированы посредством проведения служебного расследования.

9.6 Служебное расследование проводится комиссией, назначаемой приказом ректора Университета. В состав комиссии в обязательном порядке включается администратор ИСПДн, ответственный за обеспечение безопасности ПДн в ИСПДн, непосредственный руководитель работника, допустившего факт компрометации. При необходимости в состав комиссии могут включаться другие работники.

9.7 Результаты работы комиссии оформляются актом.

9.8 В процессе работы комиссии обязательными для установления являются:

- дата и время заражения (обнаружения заражения);
- ФИО, должность и подразделение работника, техническое средство которого заражено вирусной программой;
- уровень критичности заражения;
- обстоятельства, способствовавшие заражению;
- информационные ресурсы, затронутые заражением;
- характер и размер реального и потенциального ущерба.

9.9 В ходе своей работы комиссия может запрашивать объяснительные записки от работников, подозреваемых в виновности заражения (путем письменного запроса их непосредственным руководителям). Объяснительная записка должна быть представлена комиссии в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа предоставить объяснительную записку, данный факт отражается в акте.

9.10 Уничтожение материалов расследования фактов заражения осуществляется в соответствии с установленными требованиями инструкции по делопроизводству и номенклатурой дел.

10 Разработчики

Начальник ИТУ
Специалист по защите
информации ОССА

Е.Б. Абарникова
А.А. Аверин

