УТВЕРЖДАЮ
Ректор БГТУ им. В.Г. Шухова
_____ С.Н. Глаголев
«16» января 2024 г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

РАБОЧАЯ ИНСТРУКЦИЯ

Защита информационных ресурсов при автоматизированной обработке данных в Белгородском государственном технологическом университете им. В.Г.Шухова

СК-РИ- 55-04-24

Белгород 2024

Сведения о документе

Настоящий документ (Рабочая инструкция) является частью документации системы менеджмента качества, разработанной в соответствии с требованиями ГОСТ Р ИСО 9001–2015 «Системы менеджмента качества. Требования».

Рабочая инструкция (РИ) - документ, подробно описывающий действия исполнителя в рамках одного процесса.

Обозначение документа: СК-РИ-55-04-24, где СК – указывает принадлежность данного документа к системе менеджмента качества; РИ – вид документа, рабочая инструкция; 55 – индекс подразделения; 04- порядковый номер рабочей инструкции в подразделении; 24 – год разработки.

Разработал:

Начальник УиИК _____ И.Н.Гвоздевский

Введено впервые.

Утверждено и введено в действие 16.01.2024 г.

1. Общие положения

1.1. Инструкция по защите информационных ресурсов при автоматизированной обработке данных (далее – Инструкция) определяет меры и порядок организации работы по обеспечению защиты информационных ресурсов, обрабатываемых при помощи автоматизированных систем в федеральном государственном бюджетном образовательном учреждении высшего образования «Белгородский государственный технологический университет имени В.Г. Шухова» (далее – университет).

1.2. Настоящая Инструкция разработана в соответствии с Конституцией Российской Федерации, федеральными законами и иными нормативно-правовыми актами Российской Федерации в сфере защиты информации, информационных ресурсов и обеспечения безопасности персональных данных при их обработке.

1.3. Термины и определения, употребляемые в настоящей Инструкции:

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций посредством информационных систем **(ИС)** или их модулей.

Администратор локальной вычислительной сети университета – специалист, ответственный за функционирование локальной вычислительной сети (ЛВС) университета в штатном режиме.

Администратор информационного ресурса – сотрудник университета, ответственный за бесперебойное функционирование информационного ресурса.

Антивирусные базы – файлы, используемые антивирусным программным обеспечением при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного ПО.

Антивирусное программное обеспечение – набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для предотвращения заражения файлов или операционной системы вредоносным кодом.

Антивирусный контроль – проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ.

Аутентификация - процедура проверки подлинности прав доступа субъекта доступа к информационным ресурсам.

Вредоносная программа – компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информационный ресурс с целью причинения вреда университету и (или) субъекту доступа.

Защита информации – деятельность, направленная на предотвращение несанкционированных и непреднамеренных воздействий на защищаемые информационные ресурсы.

1. Общие положения

1.1. Инструкция по защите информационных ресурсов при автоматизированной обработке данных (далее – Инструкция) определяет меры и порядок организации работы по обеспечению защиты информационных ресурсов, обрабатываемых при помощи автоматизированных систем в федеральном государственном бюджетном образовательном учреждении высшего образования «Белгородский государственный технологический университет имени В.Г. Шухова» (далее – университет).

1.2. Настоящая Инструкция разработана в соответствии с Конституцией Российской Федерации, федеральными законами и иными нормативно-правовыми актами Российской Федерации в сфере защиты информации, информационных ресурсов и обеспечения безопасности персональных данных при их обработке.

1.3. Термины и определения, употребляемые в настоящей Инструкции:

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций посредством информационных систем **(ИС)** или их модулей.

Администратор локальной вычислительной сети университета – специалист, ответственный за функционирование локальной вычислительной сети (ЛВС) университета в штатном режиме.

Администратор информационного ресурса – сотрудник университета, ответственный за бесперебойное функционирование информационного ресурса.

Антивирусные базы – файлы, используемые антивирусным программным обеспечением при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного ПО.

Антивирусное программное обеспечение – набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для предотвращения заражения файлов или операционной системы вредоносным кодом.

Антивирусный контроль – проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ.

Аутентификация - процедура проверки подлинности прав доступа субъекта доступа к информационным ресурсам.

Вредоносная программа – компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информационный ресурс с целью причинения вреда университету и (или) субъекту доступа.

Защита информации – деятельность, направленная на предотвращение несанкционированных и непреднамеренных воздействий на защищаемые информационные ресурсы.

Защищаемый компьютер – электронно-вычислительная машина (персональный компьютер, сервер и др.), используемая для работы с защищаемыми информационными ресурсами.

Информационный ресурс (ИР) – массив данных, обрабатываемый с помощью автоматизированных систем.

Информационная система (ИС) – взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели.

Идентификация – сравнение предъявляемого субъектом доступа к ИР идентификатора с закрепленным за ним перечнем идентификаторов.

Идентификатор доступа – уникальный признак субъекта доступа к ИР.

Конфиденциальный ИР – ИР, содержащий коммерческую тайну; сведения о фактах, событиях и обстоятельствах частной жизни сотрудников, обучающихся и абитуриентов университета, позволяющие идентифицировать их личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях; любые другие закрытые данные, являющиеся собственностью государства (сведения о научно-исследовательских, опытно-конструкторских, проектных работах и технологиях); сведения, относящиеся к деятельности подразделений университета, несанкционированное распространение которых может привести к отрицательным экономическим, этическим или иным последствиям для университета.

Локальная вычислительная сеть (ЛВС) – средства(о) информационных технологий и телекоммуникаций, обеспечивающие доступ к ИР.

Персонал АС – технические специалисты, разрабатывающие и обслуживающие компоненты АС, другие пользователи АС.

Программное обеспечение (ПО) – совокупность программ на носителях данных, предназначенная для отладки, функционирования и проверки работоспособности компонентов АС.

Собственник ИР – структурное подразделение университета, в полном объеме реализующее полномочия владения, пользования и распоряжения ИР.

Субъект доступа – сотрудник университета или иное лицо, входящее в состав персонала АС.

Съемный носитель ИР – носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (съемные винчестеры, флэш-память, оптические лазерные диски (CD, DVD), дискеты и др.).

1.4. Требования настоящей Инструкции обязательны для выполнения персоналом АС и субъектами доступа, имеющими соответствующие права доступа к ИР автоматизированных систем университета.

1.5. Администраторы различных ИР университета назначаются приказом ректора по представлению руководителя структурного подразделения – владельца ИР.

2. Основные виды угроз безопасности и цели защиты ИР

2.1. Основными видами угроз безопасности ИР являются:

а) противоправные и (или) ошибочные действия персонала АС и третьих лиц;

б) отказы и сбои ПО и технических средств АС, ЛВС, приводящие к модификации, блокированию, уничтожению или несанкционированному копированию ИР, а также нарушению правил эксплуатации защищаемого компьютера, компонентов ЛВС;

в) стихийные бедствия, техногенные аварии, сбои и отказы технических средств АС и ЛВС, иные обстоятельства непреодолимой силы.

2.2. Целью защиты ИР является:

а) предотвращение утечки, хищения, утраты, подделки ИР, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию, предотвращение других форм незаконного вмешательства в ИР как объект собственности;

б) защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в ИР;

в) сохранение конфиденциальных ИР в соответствии с законодательством Российской Федерации;

г) обеспечение прав субъектов доступа к ИР при разработке и эксплуатации АС.

3. Обеспечение сохранности ИР

3.1. Для обеспечения сохранности ИР определяются следующие требования:

а) руководитель структурного подразделения, обслуживающего ИР, инициирует назначение администратора ИР;

б) администратор ИР выполняет обслуживание и резервное копирование ИР в соответствии с локальной нормативной документацией;

в) администратор ИР восстанавливает ИР в случае его сбоя или порчи из резервных копий в соответствии с существующей документацией и с составлением соответствующего акта (приложение 2);

г) на защищаемом компьютере, используемом при работе с ИР, устанавливается антивирусное ПО;

д) для копирования ИР не используются носители информации, не проверенные на наличие компьютерных вирусов и других вредоносных программ.

3.2. Субъектам доступа запрещается:

3.2.1. Самовольное изменение характеристик компонентов защищаемых компьютеров и ЛВС:

а) самовольное подключение, отключение и переключение любых сетевых устройств;

б) установка и использование на защищаемых компьютерах вредоносных программ, а также программ, ведущих к блокированию работы сети, таких как:

- ПО, назначающее клиентские IP-адреса внутри заданного диапазона на определенный период (DHCP-сервер), в том числе и ПО со встроенным DHCP-сервером;
- ПО для перехвата информации;
- ПО для взлома и блокирования сети и сетевых служб;
- ПО, использующее для своей работы в большом объеме широковещательные технологии передачи данных (передача данных большому числу защищаемых компьютеров);

в) самовольное изменение настроек защищаемого компьютера, подключенного к ЛВС:

- IP-адрес;
- программный модуль, обеспечивающий определение IP-адреса по полному имени (DNS-клиент);
- ПО для сопряжения компонентов ЛВС (шлюз);
- уникальный идентификатор, сопоставляемый с различными типами оборудования для компонентов ЛВС (mac- адрес);
- сетевые настройки ПО для просмотра веб-сайтов (веб-браузеров), почтовых программ;

г) вскрытие блоков, модернизация или модификация компонентов защищаемых компьютеров и установленного на нем ПО, компонентов ЛВС.

При необходимости изменения характеристик все действия согласуются с администратором ИР и администратором ЛВС

3.2.2. Несанкционированная передача защищаемых компьютеров. В случае необходимости передачи защищаемых компьютеров из одного подразделения в другое производится обязательное уведомление об этом факте:

а) администратора ЛВС, если защищаемый компьютер подключен к ЛВС;

б) администратора ИР, если защищаемый компьютер содержит ИР.

3.2.3. Осуществление несанкционированного доступа к ИР.

3.2.4. Отключение средств антивирусной защиты и самостоятельное внесение изменений в настройки антивирусного ПО на защищаемых компьютерах.

3.3. Сведения, содержащиеся в ИР, используются только в служебных целях в рамках полномочий субъекта доступа.

4. Организация мероприятий по защите ИР

4.1. Защита от несанкционированного доступа к ИР осуществляется посредством следующих мероприятий:

4.1.1. Формирование документов для обоснования прав доступа к ИР.

Доступ к ИР осуществляются на основании заявки сотрудника университета, согласованной руководителем структурного подразделения заявителя, и руководителем структурного подразделения – владельца ИР.

Прекращение прав доступа осуществляется на основании заявки руководителя структурного подразделения, сотрудник которого ранее имел доступ к ИР.

4.1.2. Назначение или прекращение прав доступа.

Назначение или прекращение прав доступа субъекта доступа к ИР осуществляет администратор ИР или иное лицо, уполномоченное администратором ИР, на основании согласованной заявки. За субъектом доступа закрепляется идентификатор (имя пользователя) и персональный признак доступа (пароль). Пароль субъект доступа формирует самостоятельно. Ответственность за неразглашение пароля возлагается на субъект доступа.

4.1.3. Выполнение общепринятых требований к паролю, используемому субъектом доступа:

а) длина пароля не менее 8 символов;

б) пароль не должен включать в себя «пустые» данные, простые данные типа «123», «111» и им подобные, а также личные и персональные данные субъекта доступа либо его близких родственников, которые могут быть определены на основании общедоступных сведений о субъекте доступа;

в) недопустимо хранение (запись) паролей на бумаге, предметах, в файлах, электронной записной книжке и других носителях, доступ к которым не ограничен субъектом доступа;

г) данные пароля рекомендуется периодически менять, периодичность смены определяется администратором ИР;

д) при компрометации пароля или подозрении на компрометацию он подлежит немедленной смене.

В отдельных случаях требования к парольной защите могут регламентироваться иными локальными нормативными документами, содержащими требования не ниже, чем приведенные в данной инструкции

4.1.4. Ведение журнала об ознакомлении субъекта доступа с настоящей Инструкцией.

Администратор ИР ведет журнал ознакомления субъекта доступа с настоящей Инструкцией (приложение 1). Процедура проводится для субъекта доступа, первично получающего права доступа к ИР.

4.1.5. Авторизация субъектов доступа при работе с ИР.

В автоматизированной системе, посредством которой осуществляется доступ к ИР, реализуются механизмы идентификации и аутентификации.

4.2. Защита от непреднамеренных изменений и разрушений ИР осуществляется посредством следующих мероприятий:

4.2.1. Для каждого ИР при необходимости разрабатываются регламентирующие документы по выполнению процедур резервного копирования, архивирования и восстановления, описывающие мероприятия по защите ИР от основных видов угроз.

4.2.2. Администратор ИР отвечает за выполнение процедур, предусмотренных регламентирующими документами.

4.3. Установка и использование антивирусного ПО на защищаемых компьютерах.

4.3.1. Порядок и процедура установки осуществляется в соответствии с регламентирующими документами.

4.3.2. Персонал АС, работающий с ИР, обязан:

а) проводить регулярную актуализацию антивирусных баз и проверку критических областей, дисков и файлов, заражение которых вредоносными программами может привести к серьезным негативным последствиям на защищаемых компьютерах;

б) обеспечивать постоянную работу средств антивирусной защиты;

в) проверять на наличие вредоносных программ всё ПО, устанавливаемое на защищаемые компьютеры;

г) не реже одного раза в две недели проводить полную проверку всех файлов, хранящихся на жестких дисках защищаемого компьютера;

д) проводить внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера:

- после установки или изменения ПО;
- после подключения защищаемого компьютера к локальной вычислительной сети;
- при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);

е) в случае обнаружения при проведении антивирусной проверки вредоносных программ:

- приостановить все операции, связанные с обработкой ИР;

- поставить в известность о факте обнаружения вредоносных программ руководителя структурного подразделения, владельцев зараженных или поврежденных вредоносными программами ИР, а также смежные подразделения, использующие эти ИР в работе;
- провести лечение или уничтожение зараженных ИР.

5. Ответственность за выполнение требований Инструкции

5.1. Ответственность за соблюдение требований по защите ИР возлагается на персонал АС, администраторов ИР и субъектов доступа в соответствии с назначенными им правами доступа.

5.2. Ответственность за организацию мероприятий по защите ИР несут руководители структурных подразделений, осуществляющих разработку, сопровождение процессов автоматизированной обработки ИР.

5.3. Нарушение требований настоящей Инструкции влечет за собой ответственность, определяемую в зависимости от тяжести наступивших последствий.

Начальник УИиК _____ (подпись) И.Н. Гвоздевский

Согласовано:

Первый проректор _____ (подпись) Е.И. Евтушенко

Начальник правового управления _____ (подпись) О.В.Владимирова

Директор департамента образовательной политики _____ (подпись) Е.А.Дороганов

Приложение 1

Журнал ознакомления с инструкцией по защите информационных ресурсов при автоматизированной обработке данных

С настоящей Инструкцией ознакомлен, предупрежден о неразглашении пароля и полученных данных, а также о персональной ответственности, предусмотренной за нарушение правил информационной безопасности в соответствии с законодательством Российской Федерации и требованиями данной Инструкции:

№ п/п	Ф.И.О. работника, должность, наименование структурного подразделения	Дата ознакомления	Подпись

Приложение 2

АКТ
о восстановлении информационных ресурсов

Мною, _____
(Ф.И.О., должность администратора информационного ресурса)

Дата выявления сбоя: _____

Проведена проверка _____
(вид ИР)

В результате чего выявлено: _____
(указывать вид и причины)

_____

_____

Способ восстановления: _____

Используемая документация: _____

Подпись администратора

Дата

Лист регистрации изменений

Изм. №	Глава/ Страница	Дата изм. и ревизии	Причина изменения и ревизии	Провел*	Утвердил*

*Подписи только у последнего изменения.