

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

РАБОЧАЯ ИНСТРУКЦИЯ

РИ 6.5-3

Инструкция по обеспечению информационной безопасности на автоматизированных рабочих местах

Регистрационный номер документа	
Структурное подразделение	
Уполномоченный по качеству	
Дата получения	

Комсомольск-на-Амуре
2015



РАБОЧАЯ ИНСТРУКЦИЯ

Система менеджмента качества

**ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
НА АВТОМАТИЗИРОВАННЫХ
РАБОЧИХ МЕСТАХ**

РИ 6.5-3

Введена впервые

СОГЛАСОВАНО

Первый проректор



И.В. Макурин
«28» сентября 2015 г.

УТВЕРЖДАЮ

Ректор университета


Э.А. Дмитриев
«29» сентября 2015 г.

Начальник ИТ-Управления


Е.Б. Абарникова
«28» сентября 2015 г.

Начальник организационно-
правового управления


Н.А. Лашкина
«28» сентября 2015 г.

Комсомольск-на-Амуре
2015



Система менеджмента качества
РИ 6.5-3
Инструкция по обеспечению информационной
безопасности на автоматизированных рабочих местах

с. 3 из 15

Содержание

1 Назначение и область применения	4
2 Нормативные ссылки	4
3 Термины, определения, сокращения	5
4 Ответственность	7
5 Общие требования к средствам вычислительной техники	8
6 Правила парольной защиты.....	9
7 Правила антивирусной защиты	11
8 Правила при работе в сети Интернет	12
9 Требования использования средств защиты информации.....	12
10 Правила хранения и использования ключей электронных подписей.....	13
11 Разработчики.....	14
Лист регистрации изменений.....	15



1 Назначение и область применения

1.1 Назначение

Настоящая инструкция определяет правила и требования по обеспечению информационной безопасности на автоматизированных рабочих местах ФГБОУ ВО «КнАГТУ». (Изм. № 1)

1.2 Сфера действия

Инструкция распространяется на все автоматизированные рабочие места сотрудников ФГБОУ ВО «КнАГТУ» за исключением СВТ, предназначенных исключительно для выполнения лабораторных работ и компьютерного практикума студентов ФГБОУ ВО «КнАГТУ», и обязательна к использованию во всех структурных подразделениях университета. (Изм. № 1)

1.3 Область применения

Указанные в настоящей инструкции правила и требования должны применять все сотрудники ФГБОУ ВО «КнАГТУ», использующие в своей работе автоматизированные рабочие места в соответствии и в рамках своих должностных обязанностей. (Изм. № 1)

2 Нормативные ссылки

Настоящая инструкция составлена на основе следующих нормативных документов:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Постановление Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119.

Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. № 21.

Приказ ФСБ России «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10 июля 2014 г. № 378.



3 Термины, определения, сокращения

3.1 Термины и определения

В настоящей инструкции применяются следующие термины с соответствующими определениями:

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

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

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.

Доступ к информации – возможность получения информации и её использования.

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

Информационная безопасность – состояние и режим эксплуатации средств хранения, доставки и автоматизированной обработки, при котором обеспечивается уровень защиты информационных ресурсов, достаточный для минимизации ущерба, вызванного возможными нарушениями безопасности.

Информационный ресурс – различная информация Университета на всех этапах ее жизненного цикла, обеспечивающая основную деятельность Университета и представляющая ценность с точки зрения достижения поставленных целей.

Информационная технология – это процесс, использующий совокупность средств и методов сбора, обработки и передачи данных для получения информации нового качества о состоянии объекта, процесса или явления.

Компрометация конфиденциальных ключей электронной подписи – случаи хищения, копирования, подмены, несанкционированного использования конфиденциальных ключей электронной подписи, возможность доступа, в том числе временная, к ним посторонних лиц, а также все случаи подозрения на то, что указанные события могли



иметь место.

Конфиденциальность – обеспечение доступности информации только ограниченному кругу лиц, имеющих соответствующие полномочия.

Конфиденциальный (секретный) ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Критичный информационный ресурс (критичная информация) – информация, создание, модификация и обработка которой связаны с повышенным риском информационной безопасности.

Критичные процессы/системы – процессы/системы, связанные с использованием критичных информационных ресурсов.

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.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В данном документе оператором выступает Университет.

Открытый (публичный) ключ электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

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

Пользователь – сотрудник университета, использующий АРМ.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Средства вычислительной техники – совокупность программных



и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом.

Университет – ФГБОУ ВО «КНАГТУ». (Изм. № 1)

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3.2 Сокращения

В настоящей инструкции применяются следующие сокращения:

- АВПО – антивирусное программное обеспечение;
- АРМ – автоматизированное рабочее место;
- АС – автоматизированная система;
- ЛВС – локальная вычислительная сеть;
- ПО – программное обеспечение;
- СЗИ – средства защиты информации;
- СВТ – средство вычислительной техники;
- ФСТЭК – Федеральная служба по техническому и экспортному контролю;
- ФСБ – Федеральная служба безопасности;
- ЭП – электронная подпись;
- SETUP BIOS – настройки базовой системы ввода-вывода.

4 Ответственность

4.1 Сотрудники университета, использующие автоматизированные рабочие места, несут ответственность за выполнение требований информационной безопасности.

4.2 Сотрудники университета, нарушающие требования информационной безопасности и руководители подразделений, не обеспечивающие их выполнение, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

4.3 Контроль над выполнением требований информационной безопасности возлагается на руководство университета, начальника ИТ-



управления, руководителей структурных подразделений университета, использующих автоматизированные рабочие места.

5 Общие требования к средствам вычислительной техники

5.1 На СВТ пользователей в настройках базовой системы ввода-вывода должны быть установлены пароли на вход в SETUP BIOS компьютера (административный пароль). При отсутствии на СВТ СЗИ с модулем доверенной загрузки рекомендуется устанавливать также пароль на включение СВТ. Пароль на SETUP BIOS устанавливается ответственным в подразделении сотрудником. Пароль на включение СВТ задается пользователем.

5.2 При установке пароля на включение компьютера и административного пароля на вход в настройки BIOS следует руководствоваться следующими правилами:

5.2.1 Пользовательский пароль пользователь выбирает и вводит единолично (не менее 6-ти символов). Если СВТ используется для коллективной или сменной работы, пароль на включение устанавливает ответственный за СВТ и сообщает этот пароль всем пользователям, допущенным к работе с СВТ. Передача пароля остальным пользователям запрещена.

5.2.2 Административный пароль (не менее 8-ми символов/максимальное количество символов, предусмотренных BIOS СВТ для административного пароля) вводится ответственным сотрудником подразделения. Ответственному сотруднику запрещается сообщать административный пароль пользователю.

5.3 Средствами SETUP BIOS на СВТ должна быть запрещена загрузка со всех устройств, кроме жесткого диска. При наличии возможности должна быть установлена защита от несанкционированной модификации загрузочного сектора жесткого диска, а так же отключена загрузка машины с сетевого ресурса, с внешних магнитных, оптических носителей (USB, CD\DVD и др.). Данные настройки осуществляет ответственный сотрудник подразделения или представитель ИТ-Управления.

5.4 В случае утраты административного пароля на SETUP BIOS или необходимости его оперативного изменения, представитель ИТ-Управления в присутствии ответственного сотрудника от подразделения может провести разблокировку пароля на SETUP по докладной записке/заявке в адрес ИТ-Управления, подписанной руководством пользователя и согласованной со службой информационной безопасности.

5.5 Средствами SETUP BIOS на СВТ необходимо отключить все устройства и порты, не являющиеся функционально необходимыми для эксплуатации СВТ на данном рабочем месте. Данные настройки осуществ-



ляет ответственный сотрудник подразделения или представитель ИТ-Управления.

5.6 При необходимости подключения отключенных устройств компьютера, их подключение производится представителем ИТ-Управления на основании докладной записки/заявки на открытие портов и устройств на СВТ, подписанной руководством пользователя и согласованной со службой информационной безопасности.

5.7 На рабочих местах пользователей должен использоваться храни- тель экрана (screensaver), защищенный паролем, с периодом ожидания не более 5 минут. При покидании рабочего места пользователь обязан произ- вести ручную блокировку своего СВТ не зависимо от времени планируе- мого отсутствия (одновременное нажатие клавиш Windows и L).

5.8 Категорически запрещается работа под чужими логинами.

5.9 Запрещается устанавливать и использовать любое нештатное ПО, в том числе ПО, не связанное с производственной необходимостью и/или полученное от сомнительного источника.

5.10 Корпус СВТ в месте вскрытия опечатывается представителем ИТ-Управления.

6 Правила парольной защиты

6.1 Личные пароли доступа создаются пользователям самостоятель- но. Пользователь несет полную ответственность за правильность исполь- зования паролей, которыми он владеет, а также ответственность за дей- ствия, совершенные от имени учетной записи пользователя в автоматизи- рованной системе.

6.2 Пароль должен быть известен только его владельцу и должен ис- пользоваться только владельцем. Запрещается сообщать пароль кому бы то ни было.

6.3 Полная плановая смена паролей в домен/АС проводится не реже одного раза в 40 дней. Техническая настройка периода действия паролей пользователей возлагается на администраторов домена/АС.

6.4 Пароли, используемые для доступа к СВТ (пользовательский па- роль на включение СВТ и/или административный пароль BIOS), заменя- ются в случае разглашения, а также в случае смены лица, ответственного за эксплуатацию СВТ.

6.5 При формировании паролей необходимо придерживаться следу- ющих правил:

6.5.1 Пароль не должен содержать имя учетной записи пользователя или какую-либо его часть.



Система менеджмента качества

РИ 6.5-3

Инструкция по обеспечению информационной безопасности на автоматизированных рабочих местах

с. 10 из 15

6.5.2 Пароль должен состоять не менее чем из 8 символов.

6.5.3 Пароли должны соответствовать требованиям безопасности (содержать прописные и строчные буквы; цифры; символы, не принадлежащие алфавитно-цифровому набору).

6.5.4 Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

6.5.5 Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

6.5.6 Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

6.5.7 Запрещается выбирать пароли, которые уже использовались ранее.

6.6 При вводе пароля пользователь должен придерживаться следующих правил:

6.6.1 Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

6.6.2 Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами.

6.7 Для хранения пароля пользователь должен придерживаться следующих правил:

6.7.1 Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

6.7.2 Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6.8 Лица, использующие паролирование, обязаны:

6.8.1 Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

6.8.2 Своевременно сообщать администратору безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.



7 Правила антивирусной защиты

7.1 На каждом АРМ и серверах должно быть установлено АВПО. Данная обязанность возлагается на ИТ-управление.

7.2 Антивирусные базы всегда должны быть в актуальном состоянии. Актуальным состоянием считается наличие установленных антивирусных баз, дата выпуск которых не превышает 7-ми календарных дней от текущей даты. Пользователь на ежедневной основе должен осуществлять контроль наличия актуальных антивирусных баз на рабочем месте. В случае превышения разницы между текущей датой и датой выпуска антивирусных баз более, чем на 7 календарных дней пользователь АРМ должен сообщить о данном факте в ИТ-Управление.

7.3 Пользователю запрещается работа на АРМ, подключенным к ЛВС университета, с выключенным или неработоспособным АВПО.

7.4 Пользователь должен обладать элементарными навыками работы с базовыми антивирусными программами:

- запуск антивирусной программы;
- выбор объектов сканирования;
- сканирование жесткого диска и внешних устройств.

7.5 Пользователь не должен устанавливать и запускать нелицензионное, не аттестованное установленным порядком ПО, а также файлы не относящиеся к выполнению им своих должностных обязанностей.

7.6 Пользователь должен в обязательном порядке проводить антивирусный контроль всех носителей информации (дискет, flash-устройств, компакт-дисков и т.п.), которые могут поступать из внешних организаций и других подразделений перед их непосредственным использованием.

7.7 Определение параметров и режимов работы средств антивирусного контроля осуществляется администратором безопасности в соответствии с руководствами по применению конкретных антивирусных средств.

7.8 В подразделениях необходимо на физическом (путем физического удаления) или логическом уровне (BIOS, Диспетчер устройств/реестр ОС) произвести отключение всех не используемых портов и устройств (USB, COM, LPT, CD\DVD и др.) в соответствии с отсутствием производственной необходимости, уменьшив, таким образом, число «точек подключения» и риск потенциального вирусного заражения. Руководителям подразделений необходимо определить их минимально необходимое количество, согласовать «точки подключения» с ИТ-управлением и своими силами произвести отключение неиспользуемых портов и устройств/направить запрос на отключение неиспользуемых портов и устройств в ИТ-управление.



7.9 Для исключения вирусного заражения не рекомендуется подключение к СВТ ЛВС университета мобильных устройств (в том числе для зарядки батарей), беспроводных интерфейсов, а также модемов, обеспечивающих возможность выхода в сеть Интернет в обход периметра безопасности.

7.10 Проверка на наличие вредоносного ПО на АРМ пользователей должна проводиться регулярно. Техническая настройка регулярной проверки возлагается на ИТ-Управление.

7.11 При возникновении подозрения на наличие вредоносного ПО (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан немедленно сообщить о своих подозрениях в ИТ-Управление. Сотрудник ИТ-Управления совместно с пользователем должен выполнить внеочередной антивирусный контроль.

8 Правила при работе в сети Интернет

8.1 Работа в сети Интернет пользователем должна проводиться только по служебной необходимости.

8.2 При работе в сети Интернет пользователю запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус, межсетевой экран);
- передавать по сети конфиденциальную информацию без использования средств шифрования;
- загружать и устанавливать нелицензионное программное обеспечение;
- посещать сайты сомнительной репутации (сайты, содержащие нелицензионно распространяемое ПО и т.п.) и загружать с этих сайтов файлы;
- сохранять пароли введенные в браузере (при предложении браузера сохранить пароль следует отвечать отрицательно).

9 Требования использования средств защиты информации

9.1 На АРМ, использующих критичные процессы/системы, должны быть установлены специальные средства защиты информации. К ним относятся:

- средства защиты от несанкционированного доступа;
- средства защиты с модулем доверенной загрузки;
- средства криптографической защиты;
- межсетевые экраны;



– антивирусные средства защиты.

9.2 Определения СЗИ необходимых к установке на АРМ, установка и настройка данных СЗИ возлагается на ИТ-Управление.

9.3 Все средства защиты информации, установленные в университете, а также эксплуатационная документация на них, подлежат учету. Учет осуществляют ответственные сотрудники ИТ-Управления.

9.4 Настройка средств защиты проводится в соответствии с эксплуатационной документацией и требованиями нормативных документов ФСТЭК и ФСБ России.

10 Правила хранения и использования ключей электронных подписей и ключей шифрования

10.1 В процессе всего периода использования и хранения конфиденциальных ключей ЭП должна быть обеспечена их надежная защита от компрометации. Ответственность за конфиденциальность сохранения ключа ЭП возлагается на владельца ключа ЭП.

10.2 Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, CD-диск, USB-flash накопитель, ТМ-носитель, e-token и др.). Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти средства вычислительной техники запрещено.

10.3 Носитель конфиденциальных ключей ЭП должен быть вставлен в считывающее устройство только на время выполнения средствами электронной подписи и средствами криптографической защиты операций формирования и проверки электронной подписи, зашифровывания и расшифровывания. Запрещено оставлять без контроля ключевой носитель.

10.4 Запрещено размещать на носителе конфиденциальных ключей ЭП иную информацию (в том числе рабочие и личные файлы).

10.5 При отсутствии необходимости использования носителей конфиденциальных ключей ЭП они должны храниться в сейфах (металлических шкафах), а при нахождении носителей вне сейфов владельцы ЭП должны принять необходимые меры, направленные на исключение компрометации конфиденциального ключа.

10.6 При хранении в сейфе (металлическом шкафу) коллективного пользования конфиденциальные ключи должны быть помещены в опечатанные конверты, тубусы, пеналы или другие средства, опечатанные личной металлической печатью владельца ЭП или оклеенные наклейкой и позволяющие обнаружить несанкционированный доступ к носителю ключа со стороны других пользователей сейфа.

10.7 Руководители подразделений должны обеспечить владельцев



Система менеджмента качества

РИ 6.5-3

Инструкция по обеспечению информационной безопасности на автоматизированных рабочих местах

с. 14 из 15

ЭП средствами хранения носителей конфиденциальных ключей ЭП (сейф, металлическая ячейка).

10.8 В случае увольнения владельца ЭП, перевода владельца ЭП на другой участок работы, смены фамилии владельца ЭП или прекращения производственной необходимости права удостоверения ЭП электронных документов руководитель подразделения владельца ЭП обеспечивает выполнение мероприятий по уничтожению конфиденциального ключа ЭП с носителя ключа ЭП и отправляет уведомления о выводе ключа в соответствующие удостоверяющие центры.

10.9 Передача носителей конфиденциальных ключей ЭП кому-либо запрещена. Носители ключевой информации должны использоваться только их владельцами либо уполномоченным лицом на использование данного носителя.

10.10 Владелец ЭП (уполномоченное лицо) несет ответственность за соблюдение правил хранения носителя с ключом ЭП и правильность его использования.

10.11 При компрометации или подозрении на компрометацию конфиденциального ключа ЭП владелец ключа (уполномоченное лицо) или другое лицо, установившее факт компрометации, обязано сообщить об этом руководителю своего подразделения и в ИТ-Управление. Владелец ключа ЭП обязан безотлагательно прекратить его использование.

10.12 Запрещено пересылать файлы с ключевой информацией для работы в системах электронного документооборота по сети Интернет или по внутренней сети (за исключением запросов на сертификат, сертификатов без привязки к конфиденциальному ключу и открытых ключей).

10.13 Правила хранения и использования ключей шифрования и иных криптографических ключей полностью соответствуют правилам хранения и использования ключей ЭП.

11 Разработчики

Данный документ разработали:

Начальник ИТ-Управления
Ведущий специалист по информационной безопасности ОССА ИТ-Управления

Е.Б. Абарникова

Д.С. Магола

