УТВЕРЖДАЮ
Ректор ГОУ ВПО «МГТУ»
_____ В. М. Колокольцев
Ввести в действие с «10» 11 2010

Рабочая инструкция

**по организации парольной защиты
Государственного образовательного учреждения
высшего профессионального образования
«Магнитогорский государственный технический
университет им. Г.И. Носова»**

Настоящая инструкция регламентирует процессы парольной защиты в информационной системе персональных данных (далее – ИСПДн) Государственного образовательного учреждения высшего профессионального образования «Магнитогорский государственный технический университет им. Г.И. Носова», далее ГОУ ВПО «МГТУ».

1 Общие положения

1.1 Настоящая инструкция регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в информационной системе персональных данных (далее – ИСПДн) ГОУ ВПО «МГТУ», а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2 Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администраторов подсистем персональных данных и ответственных за безопасность персональных данных в подразделениях.

2 Термины и определения

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Компрометация – раскрытие, обнаружение или утеря пароля.

Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

3 Правила формирования паролей

3.1 Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее 6 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

3.2 Сотрудникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).

3.1 В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администраторов подсистем персональных данных.

3.3 Для обеспечения возможности использования имён и паролей некоторых сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), сотрудники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей ответственному за обеспечение безопасности персональных данных в запечатанном конверте. Конверты с паролями сотрудников должны храниться в сейфе, к которому исключён доступ других сотрудников ГОУ ВПО «МГТУ» и третьих лиц. Все конверты с паролями в обязательном порядке подписываются администратором подсистемы персональных данных и регистрируются в «Журнале учёта паролей пользователей информационной системы персональных данных» (Приложение А).

3.4 Ключ от сейфа должен храниться у работника, назначенного руководителем подразделения.

4 Ввод пароля

4.1 При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

5 Порядок смены личных паролей

5.1 Смена паролей должна проводиться регулярно, не реже одного раза в 12 месяцев, самостоятельно каждым пользователем.

5.2 В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

5.3 Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за обеспечение безопасности персональных данных, администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5.4 Администраторы подсистем персональных данных ведут «Журнал учета паролей пользователя информационной системы персональных данных» и отмечают причины внеплановой смены паролей пользователей.

5.5 Временный пароль, заданный администратором подсистем персональных данных при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

6 Хранение пароля

6.1 Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

6.2 Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

6.3 Запрещается входить в ИСПДн под учётной записью и паролем другого пользователя.

6.4 Запрещается регистрировать в ИСПДн нового пользователя с чужим (известным) паролем.

7 Действия в случае утери и компрометации пароля

7.1 В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

8 Ответственность при организации парольной защиты

8.1 Каждый пользователь ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учётной записи.

8.2 Ответственность за контроль проведения мероприятий по организации парольной защиты в подразделениях возлагается на администраторов подсистем персональных данных и ответственных за безопасность персональных данных.

8.3 За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, сотрудники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение Б – Лист ознакомления с Инструкцией СМК-РИ-08-10 на 1 л. в 1.экз.

Разработано:

Специалист по защите информации Н.М. Сухих

Согласовано:

Проректор по научной работе К.Н. Вдовин

Начальник УИТ и АСУ Н.Л. Левшова

Лист регистрации изменений

СМК – РИ – 08 – 10

Рабочая инструкция по организации парольной защиты Государственного образовательного учреждения высшего профессионального образования «Магнитогорский государственный технический университет им. Г.И. Носова»

Изм.	Номера страниц		Номер документа	Подпись	Дата	Срок введения изменения
	новых	аннулированных				

Приложение А

(обязательное)

Форма журнала учёта паролей пользователей информационной системы персональных данных

Инвентарный №_____

ЖУРНАЛ

учёта паролей пользователей информационной системы персональных данных

Начат:	
Окончен:	
Количество листов:	
Срок хранения:	5 лет

	ГОУ ВПО «МГТУ»		СМК – РИ – 08 – 10
	Управление информационных технологий и АСУ	Экземпляр № 1	**Лист** 7 **Всего листов** 8

№ п/п	Дата установки пароля	Ф.И.О. пользователя	Номер конверта с паролем	Причина изменения	Подпись пользователя
1	2	3	4	5	6

Приложение Б

(обязательное)

Лист ознакомления с Инструкцией СМК-РИ-08-10 от____________

Дата ознакомления	ФИО сотрудника, ознакомившегося с документом	Должность сотрудника, ознакомившегося с документом	Подпись сотрудника, ознакомившегося с документом