ПРИНЯТА
Ученым советом института
Протокол № 9
от «23» мая 2018 г.

УТВЕРЖДАЮ
Ректор
С.Е. Шиянов
«23» мая 2018 г.

ПОЛИТИКА
безопасности в информационных системах в Автономной некоммерческой организации высшего образования «Северо-Кавказский социальный институт»

Ставрополь, 2018

Содержание

1. Общие положения

1.1. Политика безопасности в информационных системах в институте (далее - Политика) определяет общие правила обеспечения информационной безопасности в информационных системах (далее - Системы) Северо-Кавказского социального института (далее - Институт). Процедуры и правила использования тех или иных Систем могут быть установлены дополнительными локальными нормативными документами.

1.2. Политика разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных»; Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»; Федеральным законом от 07.07.2003 №126-ФЗ «О связи»; уставом Института; правилами внутреннего трудового распорядка Института.

2. Цель и задачи Политики

2.1. Информация и Системы являются одним из жизненно важных ресурсов Института, обеспечивающих его эффективную работу.

2.2. Цели и задачи Политики:

2.2.1. Обеспечение целостности, конфиденциальности и доступности информации и Систем Института;

2.2.2. Обеспечение непрерывности образования путем предотвращения возможных инцидентов информационной безопасности.

3. Логический доступ к информационным ресурсам

3.1. Информационные системы и ресурсы Института могут использоваться сотрудниками Института только в служебных целях. Вся

информация, хранящаяся в Системах и предоставляемая Системами, является конфиденциальной (в т.ч. персональные данные) за исключением информации, доступ к которой не ограничивается в соответствии с законодательством Российской Федерации и локальными нормативными документами Института (сведения об образовательной организации и др.).

3.2 Необходимым условием доступа к информационным ресурсам и Системам Института является ознакомление сотрудника Института с данной Политикой.

3.3 Сотрудникам Института предоставляются права доступа к информационным ресурсам в соответствии с их служебными обязанностями. Каждому пользователю Системы системный администратор назначает уникальные учетные данные для доступа в закрытые части Системы.

3.4 Недопустимым является использование ресурсов, к которым у сотрудника нет прав доступа. Возможность доступа пользователя к ресурсам, не предусмотренным его служебными обязанностями, не означает получения права на их использование.

3.5 Работа в Системе с использованием чужих учетных данных, запрещается передача прав доступа к информационным ресурсам, а также несанкционированное копирование, изменение, уничтожение данных, хранящихся в Системе Института является нарушением.

3.6 Основным средством доступа к информационным ресурсам Института является персональный компьютер.

4. Использование носителей компьютерной информации

4.1. Запись конфиденциальной информация на переносные носители информации (флэш-карты, оптические диски и проч.) выполняется только по необходимости.

4.2 Пользователь обязан своевременно уничтожать утратившие актуальность копии документов, содержащих конфиденциальную информацию.

4.3 Использование флэш-карт или других переносных носителей информации возможно только после обязательной проверки их на наличие вирусов. В случае обнаружения вирусов работа с данными устройствами прекращается до уничтожения вирусов.

5. Учетные данные

5.1. Доступ к использованию ресурсов информационных систем предоставляется после ознакомления с настоящей Политикой.

5.2 В момент предоставления сотруднику прав доступа к Системе системный администратор сообщает сотруднику учетные данные (логин и пароль). Сотрудник обязан обеспечить конфиденциальность своих учетных данных. Запрещается разглашать и передавать свои учетные данные другим сотрудникам.

5.3 В случае, если сотрудник забыл свои учетные данные и не может получить доступ к информационным ресурсам Института, он должен обратиться к системному администратору Института.

6. Электронное архивирование информации

6.1 Электронное архивирование информации должно обеспечивать сохранение значимой и другой представляющей ценность для Института информации, возможность восстановления информации в случаях нарушений информационной безопасности, сбоях оборудования и программного обеспечения, непреднамеренного уничтожения информации.

6.2 Электронное архивирование общего сетевого каталога («Сервер») производится автоматизированными средствами системным администратором. Дополнительно может выполняться архивирование значимой информации самими сотрудниками.

6.3 Электронное архивирование информации, размещенной на компьютерах сотрудников выполняется самими сотрудниками.

7. Обеспечение доступности информационных систем

7.1. Для Систем, обрабатывающих критичную информацию, должно обеспечиваться сохранение (восстановление) их работоспособности при утере, уничтожении, несанкционированной модификации данных, программного обеспечения, выходе из строя оборудования и т.п.

7.2. Сопровождение работы аппаратного и программного обеспечения предусматривает:

- контроль за несанкционированным изменением программ (базового сетевого программного обеспечения, прикладного сетевого программного обеспечения) и прав доступа к ним;
- контроль функционирования базового сетевого аппаратного и серверного оборудования.

8. Антивирусная защита

8.1. Антивирусная защита информационных ресурсов Института осуществляется централизованно усилиями отдела развития информационных систем и должна обеспечивать контроль:

- информации, входящей из сети Интернет в локальную сеть Института;
- информации, хранящейся на файловом сервере Института;
- информации, хранящейся на персональных компьютерах сотрудников

Института.

8.2. На сервере Института должно быть установлено антивирусное программное обеспечение с проведением еженедельной проверки на вирусы всех программ и данных сервера.

8.3. Рабочие станции пользователей должны иметь резидентные антивирусные программы, обеспечивающие проверку на вирусы всех файлов при их загрузке в компьютер, а также антивирусные сканеры для полной проверки жёстких дисков.

8.4. Антивирусные программы и базы вирусных сигнатур должны периодически обновляться.

8.5. Пользователи обязаны информировать Системного администратора о любом обнаруженном вирусе, изменении конфигурации, необычном поведении компьютера или программы.

9. Функции по обеспечению информационной безопасности

9.1. Ведущую роль в разработке стратегии информационной безопасности Института играет отдел развития информационных систем, который:

- разрабатывает политики и процедуры информационной безопасности;
- разрабатывает технические, организационные и административные планы обеспечения реализации политики информационной безопасности;
- обеспечивает штатное функционирование комплекса средств информационной безопасности Института;
- обеспечивает мониторинг функционирования системы управления информационной безопасности Института;
- обеспечивает выбор средств и механизмов контроля, управления и обеспечения информационной безопасности Института;

- проводит расследование событий, связанных с нарушениями информационной безопасности (инцидентов безопасности);

- обеспечивает исполнение требований информационной безопасности, изложенных в настоящей Политике и других локальных нормативных документах Института.

9.2. Сотрудники Института в рамках обеспечения информационной безопасности:

- выполняют требования информационной безопасности, изложенные в настоящей Политике и других локальных нормативных документах Института;

- способствуют выполнению требований информационной безопасности третьими лицами, с которыми они контактируют в рамках своих должностных обязанностей, в том числе путём указания требований в контрактах/ соглашениях/ договорах с третьими лицами.

Лист согласования

Разработано:

Начальник ОРИС  Е.В.Иноземцев

Согласовано:

Начальник УМУ  Д.В. Гришин

Лист регистрации изменений

Номер изменения	Номер листа			Дата внесения изменения	Дата введения изменения	Всего листов в документе	Подпись ответственного за внесение изменений
	измененного	нового	изъятого				

Реестр рассылки

Экз. №	Структурное подразделение	ФИО	Подпись получателя
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			