Министерство культуры Российской Федерации
Кемеровский государственный институт культуры

П О Л О Ж Е Н И Е
от 18.11.2018 № 17 Ректор-01.08-10
Кемерово

У Т В Е Р Ж Д А Ю
Ректор Кемеровского
государственного института
культуры,
_____ А. В. Шунков
«28» ноября 2018 г.
М.П.

Политика безопасности
в информационных системах

Настоящее Положение «Политика безопасности в информационных системах» (в дальнейшем – Политика) федерального государственного бюджетного образовательного учреждения высшего образования «Кемеровский государственный институт культуры» (далее – Институт) разработано в соответствии с:

- Федеральным законом от 29.12.2012 № 273-ФЭ «Об образовании в Российской Федерации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Уставом Института;
- приказами ректора Института;
- другими локальными нормативными документами Института.

Политика безопасности в информационных системах определяет общие правила обеспечения информационной безопасности в информационных системах (далее - Системы) Института. Процедуры и правила использования тех или иных Систем могут быть установлены дополнительными локальными нормативными документами.

1 Термины

Администратор Системы – привилегированный пользователь, выполняющий функции сопровождения и администрирования Системы;

Владелец информационного ресурса – структурное подразделение Института, уполномоченное к управлению содержанием информационного ресурса и несущее ответственность за обеспечение его безопасности в части авторизации прав доступа;

Доменная учетная запись – учетная запись, от имени которой

субъект, осуществляет работу в Системе;

Доменное имя – обозначение символами, предназначенное для идентификации информационного ресурса пользователя;

Доступность – возможность получения и использования информации и смежным ресурсов авторизованных пользователей тогда, когда им это необходимо;

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Информационные ресурсы – различные виды университетской информации (образовательной, финансово-аналитической, кадрово-управленческой и пр.) на следующих фазах её жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение;

Конфиденциальность – обе спечение доступа к информации только для авторизованных пользователей;

Пользователь – субъект, осуществляющий работу в Системе;

Целостность – обеспечение полноты и точности информации и методов её обработки.

2 Общие положения

2.1 Информация может быть представлена в различных формах, сохранена на персональных компьютерах или серверах, передана по сети, распечатана или переписана на бумагу, пересказана собеседнику.

2.2 Информационная безопасность предусматривает защиту всех форм и средств обработки информации в целях гарантированного обеспечения её целостности, конфиденциальности и доступности.

2.3 Информация и Системы являются одним из жизненно важных ресурсов Института, обеспечивающих его эффективную работу. Несанкционированный доступ и несанкционированное использование Систем и информации может явиться причиной материального ущерба для Института.

3 Основные цели и задачи

3.1 Цель Политики – обеспечение комплексной безопасности в информационных системах Института.

3.2. Политики предназначена для решения следующих задач:

- обеспечить целостность, конфиденциальность и доступность информации и Систем Института;
- обеспечить непрерывность образования и минимизировать ущерб

Института путём предотвращения возможных инцидентов информационной безопасности;

- обеспечить соответствие мер, принимаемых в области защиты информации Института;

- предоставить сотрудникам Института рекомендации и содействие в области защиты информации.

4 Доступ к информационным ресурсам

4.1 Информационные 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 и др.), 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.).

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

4.3 Сотрудникам Института предоставляются права доступа к информационным ресурсам в соответствии с их служебными обязанностями. Каждому пользователю назначается уникальный идентификатор - Доменную учетную запись.

4.4 При обработке критичной информации должна обеспечиваться возможность определения авторства (протоколирование) каждой выполненной операции на основе идентификаторов пользователей.

4.5 Запрещается 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.

4.6 Сотрудникам запрещается работа в Системах под именами других пользователей и с использованием чужих паролей доступа, запрещается передача прав доступа к информационным ресурсам, а также несанкционированное копирование, изменение, уничтожение данных, хранящихся в Системах Института.

4.7 Основным средством доступа к информационным ресурсам Института является персональный компьютер. За каждым компьютером закрепляется ответственный пользователь, определяемый руководителем структурного подразделения.

4.8 Ответственный пользователь не должен допускать работы других пользователей на своем персональном компьютере под своей доменной УЗ, такая работа возможна только в случае служебной необходимости с разрешения руководителя структурного подразделения.

4.9 При передаче персонального компьютера другому пользователю локальный диск компьютера может быть переформатирован сотрудниками управления информатизации Института по усмотрению руководителя структурного подразделения, в котором этот компьютер эксплуатировался. Форматирование диска в этом случае должно производиться по согласованию и под контролем руководителя данного структурного подразделения с составлением акта (в свободной форме).

4.10 При подключении компьютера сотрудниками управления информатизации Института устанавливается стандартная конфигурация программного обеспечения.

4.11 Пользователям запрещается:

- самостоятельно изменять конфигурацию программных и аппаратных средств персонального компьютера, осуществлять установку и удаление прикладных программ, изменять системные параметры, уничтожать или добавлять файлы в системные директории;

- изменять установленное администратором состояние разделения дисковых ресурсов компьютера, т.е. создавать или удалять разделяемые ресурсы;

- изменять любые настройки доступа к сети.

4.12 Ответственный Пользователь несёт ответственность за наличие/отсутствие на локальном диске вверенного компьютера посторонних программ, установленных без участия специалистов управления информатизации Института.

4.13 Запрещается для хранения конфиденциальной информации использовать общедоступные сетевые диски.

4.14 Для пересылки электронных документов, содержащих закрытую информацию структурного подразделения, внутри Института Пользователь обязан использовать систему электронной почты, рекомендованную управлением информатизации Института.

4.15 При использовании портативных компьютеров (ноутбуков и т.п.) за пределами территории Института, ответственный пользователь несёт ответственность за безопасность и сохранность портативного компьютера, а также за конфиденциальность информации, обрабатываемой на нём.

4.16 При удаленном подключении к информационным ресурсам Института, Управлением информатизации должна быть обеспечена достаточная защита, направленная на минимизацию рисков кражи информации, несанкционированного раскрытия информации, несанкционированного удалённого доступа к системам Института, злоупотребления предоставленными ресурсами.

5 Использование носителей компьютерной информации

5.1 При необходимости записи конфиденциальной информации на

флэш-карты, лазерные диски или другие носители сотрудник должен получить соответствующее разрешение руководителя структурного подразделения, в котором он работает, если иное не определено его служебными обязанностями.

5.2 Пользователь обязан своевременно уничтожать утратившие актуальность копии документов, содержащих конфиденциальную информацию. Окончательное уничтожение информации на магнитных носителях выполняется путём полного форматирования последних.

5.3 Использование флэш-карт или других магнитных носителей информации возможно только после обязательной проверки их на наличие вирусов. В случае обнаружения вирусов на магнитном носителе или в памяти компьютера работа с данными устройствами прекращается до уничтожения вирусов. Институтские переносные магнитные носители подлежат обязательному учёту.

6 Пароли

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

6.2 В момент предоставления сотруднику прав доступа к Системе Пользователь получает логин и пароль. Пользователь обязан обеспечить конфиденциальность своих личных паролей. Запрещается разглашать и передавать свои пароли другим сотрудникам и иным лицам, а также размещать пароль в электронном виде на магнитных носителях.

6.3 В случае, если Пользователь самостоятельно выбирает последовательность символов для пароля, ему рекомендуется использовать в пароле сочетание букв верхнего и нижнего регистров, цифр и знаков пунктуации длиной не менее 7 (семи) знаков.

6.4 В качестве личного пароля сотруднику Института, осуществляющему работу с конфиденциальной информацией, запрещается использовать:

- последовательности символов, состоящие из одних цифр (в том числе даты, номера телефонов и т.д.);
- последовательности повторяющихся букв;
- подряд идущие в раскладке клавиатуры или в алфавите символы;
- имена и фамилии;
- имя пользователя в Системе (идентификатор) и общеупотребительные сокращения (ЭВМ, ЛВС, user, admin и т.д.);
- осмысленные английские или русские слова;
- ассоциированную с сотрудником информацию, которую легко узнать (адрес, марка автомобиля и т.д.).

6.5 В случае, если Пользователь забыл свой пароль и не может получить доступ к информационным ресурсам, восстановление пароля

осуществляют сотрудники научной библиотеки Института.

6.6 Пользователю разрешается использовать один и тот же пароль для входа в сеть, в систему электронной почты, другие Системы.

6.7 Пароли, установленные по умолчанию в приложениях и операционных системах (во время инсталляции), подлежат немедленной замене после начала использования системы (приложения).

7 Электронное архивирование информации

7.1 Электронное архивирование информации должно обеспечивать сохранение юридически значимой и другой представляющей ценность для Института информации, возможность разрешения спорных ситуаций и проведения расследований в случаях нарушений информационной безопасности.

7.2 Электронному архивированию подлежат:

- электронные документы; электронные образы бумажных документов; электронные протоколы (регистрационные журналы, log-файлы и т.п.) работы Систем;
- открытые ключи электронной цифровой подписи;
- любая другая информация в электронном виде, для которой определена необходимость архивирования.

7.3 Электронные архивы должны удовлетворять следующим требованиям:

- архив не доступен для записи или удаления информации любым лицом, кроме ответственного за ведение архива, определенного руководителем соответствующего структурного подразделения;
- документы в архиве хранятся со всеми возможными подтверждениями их подлинности, в частности, с электронной цифровой подписью (для документов, которые были подписаны электронной цифровой подписью);
- архив надёжно защищён от утраты и уничтожения (дублирование, хранение в сейфах, несгораемых шкафах, выбор носителей соответствующей надежности).

8 Обеспечение доступности информационных систем

8.1 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.

8.2 Сопровождение работы аппаратного и программного обеспечения

предусматривает:

- контроль за несанкционированной установкой аппаратного или программного обеспечения;

- контроль за несанкционированным изменением программ и прав доступа к ним;

- хранение эталонных копий программ, исходных текстов программного обеспечения, в том числе и предыдущих версий, в специальных библиотеках программного обеспечения;

- разделение технологических процессов разработки, тестирования, переноса в промышленную среду и эксплуатации программного обеспечения;

- контроль и документирование любых изменений аппаратной и программной частей Систем, отражение изменений в прикладном программном обеспечении в номере версии, системной документации и документации пользователей.

8.3 Резервное копирование информации должно удовлетворять следующим требованиям:

- обеспечивать возможность восстановления программ и данных в случае возникновения аварийной ситуации;

- копии программного обеспечения и данных должны располагаться в безопасном месте, защищенном от пожаров и иных угроз;

- периодически должна проверяться возможность восстановления информации с копий.

8.4 Периодичность резервного копирования должна позволять восстановить работу Систем без существенных потерь для Института в кратчайшее время. Периодичность резервного копирования общеинститутский систем определяется начальником управления информатизации.

8.5 Минимально необходимый и достаточный объём копируемой информации, вместе с точными и полными перечнями резервных копий и документированными процедурами восстановления, должен храниться удаленно и на достаточном расстоянии с целью предотвращения ущерба в случае аварии на основной серверной площадке.

8.6 Резервированию подлежит: серверное и сетевое оборудование; программное обеспечение; каналы связи; информационные базы данных.

9 Антивирусная защита

9.1 Антивирусная защита информационных ресурсов Института осуществляется централизованно усилиями Управления информатизации Института и должна обеспечивать контроль:

- информации, входящей из глобальных сетей во внутреннюю сеть Института;

- информации, хранящейся на файловых серверах Института;
- информации, хранящейся на персональных компьютерах сотрудников Института.

9.2 На всех файловых серверах Института должно быть установлено антивирусное программное обеспечение с проведением ежедневной проверки на вирусы всех программ и файлов данных на файловых серверах.

9.3 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.

9.4 Антивирусные программы и базы вирусных сигнатур должны централизованно обновляться.

9.5 Пользователи обязаны информировать Управление информатизации Института о любом обнаруженном вирусе, изменении конфигурации, необычном поведении компьютера или программы.

9.6 При обнаружении вируса должны быть приняты следующие меры:

- информировать Управление информатизации Института предупреждает всех пользователей, имеющих доступ к программам и данным, в которых обнаружен вирус, о возможном заражении их компьютеров;
- любой компьютер, который подозревается в заражении вирусом, немедленно отключается от сети;
- зараженный компьютер не подключается к сети до тех пор, пока сотрудники Управления информатизации Института не удостоверятся в успешном результате лечения (удалении) вируса;
- если вирус удалить не удается, все программы в компьютере удаляются, включая, при необходимости, операционную систему, жесткий диск форматируется;
- удалённые программы повторно устанавливаются из надежных источников и повторно проверяются на наличие вирусов;
- проводится анализ причин заражения вирусом и принимаются необходимые меры безопасности.

10 Требования к защите помещений

10.1 Помещения Института, в которых располагаются средства вычислительной техники, должны оборудоваться охранно-пожарной сигнализацией, а при необходимости средствами инженерной защиты и контроля доступа.

10.2 Помещения с серверным оборудованием, на котором обрабатывается критичная информация, должны быть оборудованы достаточными средствами кондиционирования, измерения и контроля температуры и влажности воздуха, средствами охранной сигнализации,

системой контроля доступа и автоматизированной системой пожаротушения, системой контроля состояния электроснабжения, при необходимости - средствами видеонаблюдения. Доступ в эти помещения предоставляется строго определенным лицам в соответствии с утвержденными служебными обязанностями, время входа и выхода из помещения должно фиксироваться в специальной базе данных.

10.3 Руководители структурных подразделений Института должны обеспечивать соблюдение соответствующего режима доступа в помещения с серверной вычислительной техникой, исключающего несанкционированное нахождение в них и несанкционированное использование вычислительной техники.

11 Функции по обеспечению информационной безопасности

11.1 Ведущую роль в разработке стратегии информационной безопасности Института играет Управление информатизации Института, которое:

- готовит для руководства Института предложения по формированию бюджета, направленного на обеспечение информационной безопасности;
- 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;
- проводит консультацию сотрудников Института в области информационной безопасности;
- оценивает риски информационной безопасности, контролирует действия пользователей;
- 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.

11.2 Сотрудники Института в рамках обеспечения информационной безопасности:

- выполняют требования информационной безопасности, изложенные в настоящей Политике и других локальных нормативных документах Института, в том числе связанных с защитой персональных данных;
- 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.

12 Ответственность и полномочия

12.1 Управление информатизации Института несёт первичную ответственность за состояние информационной безопасности в Институте.

12.2 Руководители структурных подразделений, использующих в своей работе информационные Системы, несут ответственность за нарушение подчиненными сотрудниками требований настоящей Политики.

12.3 Сотрудник Института несёт персональную ответственность за все действия, выполняемые им в Системах Института в соответствии с внутренними нормативными документами Института и законодательством РФ.

12.4 За нарушение настоящего Положения обучающиеся и сотрудники привлекаются к дисциплинарной и гражданско-правовой ответственности в рамках, предусмотренных действующим законодательством.

13 Заключительные положения

13.1 Настоящее положение принимается Ученым советом Института и вступает в силу с момента его утверждения ректором.

13.2 Все изменения и дополнения в настоящее принимаются Ученым советом Института.

Положение разработал:
Начальник управления информатизации  /В. Н. Борздун/

ПРИНЯТО
Ученым Советом
Кемеровского государственного
института культуры
(протокол № 4 от «28» 11 2018 г.)