АДМИНИСТРАЦИЯ СМОЛЕНСКОЙ ОБЛАСТИ
ДЕПАРТАМЕНТ СМОЛЕНСКОЙ ОБЛАСТИ ПО КУЛЬТУРЕ
ОГБОУ ВО «СМОЛЕНСКИЙ ГОСУДАРСТВЕННЫЙ
ИНСТИТУТ ИСКУССТВ»

УТВЕРЖДАЮ:
И.о. ректора института
_____ Е.Е. Подгузова
«02» декабря 2021г

ПОЛОЖЕНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОГБОУ ВО «СМОЛЕНСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ ИСКУССТВ»

УТВЕРЖДЕНО
на заседании Ученого совета института
Протокол №3 от «2» декабря 2021 г.
Ученый секретарь _____ Паламаржа А.Ю.

РАССМОТРЕНО
на заседании научно-методического совета
Протокол №3 от «25» ноября 2021 г.
Председатель научно-методического совета _____ Горбылева Е.В.

Смоленск, 2021

1. Общие положения

1.1. Положение по информационной безопасности образовательной организации (далее – Положение) регламентирует вопросы информационной безопасности в образовательной организации (далее - институт).

1.2. Настоящее Положение разработано в соответствии с:

– Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Уставом ОГБОУ ВО «Смоленский государственный институт искусств» и иными локальными нормативными актами.

1.3. Под информационной безопасностью понимается состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений.

1.4. Под субъектами информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры. К поддерживающей инфраструктуре относятся не только компьютеры, но и помещения, системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и обслуживающий персонал.

1.5. Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим группам:

– персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;

– обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения образовательного процесса;

– защищенная законом интеллектуальная собственность.

1.6. Обеспечение информационной безопасности осуществляется по следующим направлениям:

– правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

– организационная защита – это регламентация деятельности образовательной организации и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

– инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

2. Угрозы информационной безопасности

2.1. Спецификой обеспечения информационной безопасности в образовательной организации является состав характерных угроз. К ним относится не только возможность хищения или повреждения данных хакерами, но также деятельность обучающихся, которые могут сознательно или ненамеренно повредить оборудование или заразить систему вредоносными программами.

2.2. Угрозам намеренного или ненамеренного воздействия могут подвергаться следующие группы объектов:

– компьютерное и другое оборудование образовательной организации, в отношении которого возможны воздействия вредоносного программного обеспечения, физические и другие воздействия;

– программное обеспечение, применяемое в образовательном процессе или для работы системы;

– данные, которые хранятся на жестких дисках или портативных носителях;

– обучающиеся, которые могут подвергаться стороннему информационному воздействию;

– персонал, поддерживающий работу ИТ-системы.

2.3. Угрозы информационной безопасности образовательной организации могут носить непреднамеренный и преднамеренный характер.

2.4. К непреднамеренным угрозам относятся:

– аварии и чрезвычайные ситуации – затопление, отключение электроэнергии и т. д.;

– программные сбои;

– ошибки работников;

– поломки оборудования;

– сбои систем связи.

2.5. Особенностью непреднамеренных угроз является их временное воздействие. В большинстве случаев результаты их реализации достаточно эффективно и быстро устраняются подготовленным персоналом.

2.6.К более опасным относятся угрозы информационной безопасности намеренного характера, результаты реализации которых, невозможно предвидеть. Намеренные угрозы могут исходить от обучающихся, работников образовательной организации, хакеров. Наиболее уязвимыми являются сети с удаленным в пространстве расположением компонентов, связи между которыми легко нарушаются, что приводит к выведению системы из строя.

2.7. Существенную угрозу представляет хищение интеллектуальной собственности и нарушение авторских прав.

2.8. Внешние атаки на компьютерные сети образовательной организации могут предприниматься для воздействия на сознание обучающихся с целью вовлечения их в криминальную или террористическую деятельность.

3. Цели и задачи обеспечения безопасности информации

3.1. Главной целью обеспечения безопасности информации, циркулирующей в образовательной организации, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды образовательной организации.

3.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки и информации, циркулирующей в образовательной организации;

– предотвращение нарушений прав личности обучающихся, педагогических работников и других сотрудников образовательной организации на сохранение конфиденциальности информации;

– предотвращение несанкционированных действий по блокированию информации.

3.3.Основными задачами обеспечения безопасности информации являются:

– соответствие положениям законодательных актов и нормативным требованиям по защите информации;

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам образовательной организации, нарушению нормального функционирования и развития образовательной организации;

– создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

– эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

– развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

– развитие и совершенствование защищенного юридически значимого электронного документооборота;

– создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;

– создание механизмов управления системой информационной безопасности.

4. Правовые нормы обеспечения информационной безопасности

4.1. Образовательная организация имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников образовательной организации, требовать от своих работников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

4.2. Образовательная организация обязана обеспечить сохранность конфиденциальной информации.

4.3. Администрация образовательной организации:

– назначает ответственного за обеспечение информационной безопасности;

– имеет право включать требования по обеспечению информационной безопасности в коллективный договор;

– имеет право включать требования по защите информации в договоры по всем видам деятельности;

– разрабатывает перечень сведений конфиденциального характера;

– имеет право требовать защиты интересов образовательной организации со стороны государственных и судебных инстанций.

4.4.Организационные и функциональные документы по обеспечению информационной безопасности:

– приказ руководителя образовательной организации о назначении ответственного за обеспечение информационной безопасности;

– перечень защищаемых информационных ресурсов и баз данных;

– инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней работников образовательной организации и др.

4.5.Порядок допуска работников образовательной организации к информации предусматривает:

– принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

– ознакомление работника с нормами законодательства РФ и образовательной организации об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

– контроль работника ответственным за информационную безопасность, при работе с информацией конфиденциального характера.

5. Организация системы обеспечения информационной безопасности

5.1. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в образовательной организации устанавливаются:

– защита интеллектуальной собственности образовательной организации;

– защита компьютеров, локальных сетей и сети подключения к системе Интернет;

– организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся образовательной организации;

– учет всех носителей конфиденциальной информации;

– контроль над использованием электронных средств информационного обеспечения деятельности образовательной организации по прямому назначению;

– противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности образовательной организации нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;

– принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;

– обучение работников образовательной организации по вопросам обеспечения информационной безопасности;

– контроль за правильностью использования имеющихся в образовательной организации средств телефонной и радиосвязи.

6. Организация работы с информационными ресурсами и технологиями

6.1.Система организации делопроизводства:

– учет всей документации образовательной организации, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

– регистрация и учет всех входящих (исходящих) документов образовательной организации в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

– регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);

– особый режим уничтожения документов.

6.2. В ходе использования, передачи, копирования и исполнения документов необходимо соблюдать определенные правила:

6.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

6.2.2. Документы, дела и издания с грифом «Для служебного пользования»(«Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах.

При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

6.2.3. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.

6.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства/начальника управления делами.

6.2.5.Запрещается выносить документы с грифом «Для служебного пользования» за пределы образовательной организации.

6.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

6.3. Все программное обеспечение устанавливается только с разрешения ответственного за информационную безопасность.

ЛИСТ СОГЛАСОВАНИЯ

ФИО	Должность	Дата согласования	Подпись
Гнездова Ю.В.	И.о. проректора по научной работе	01.12.21	
Горбылева Е.В.	Проректор по учебной и воспитательной работе	01.12.21	
Азарова В.В.	Начальник учебно-методического управления	01.12.21	
Кожекин М.В.	Юрисконсульт	01.12.21	

ЛИСТ СОГЛАСОВАНИЯ
С ПРЕДСТАВИТЕЛЯМИ ОБУЧАЮЩИХСЯ

ФИО	Должность	Дата согласования	Подпись
Кузнецова Александра Витальевна	Председатель студенческого профкома	01.12.2021	
Шитикова Наталья Александровна	Председатель совета родителей	01.12.2021	

ЛИСТ ОЗНАКОМЛЕНИЯ

ФИО	Должность	Дата ознакомления	Подпись
Асриева С.В.	И.о. зав. кафедрой социально-культурной деятельности, режиссуры театрализованных представлений и актерского искусства	01.12.2021	
Бутеев Д.В.	И.о.декана факультета культуры и искусств, дополнительного профессионального образования	01.12.2021	
Иванова Ю.В.	Зав. кафедрой гуманитарных и социально-экономических наук	01.12.2021	
Мертенс Е.С.	Зав. кафедрой библиотечно-информационной деятельности и музеологии	01.12.2021	
Сычугов А.М.	Зав. кафедрой музыкального искусства	01.12.2021	
Цаплина С.П.	Зав. кафедрой народной художественной культуры	01.12.2021	

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

Номер изменения (дополнения)	Дата изменения (дополнения)	Страницы (пункты) с изменениями (дополнениями)	Краткое содержание изменений (дополнений)	Лицо, ответственное за внесение изменений (дополнений)		
				ФИО	Должность	Подпись

ЛИСТ ПЕРИОДИЧЕСКИХ ПРОВЕРОК

Должностное лицо, проводившее проверку (ФИО, должность, подпись)	Дата проверки	Потребность в корректировке (да/нет)	Перечень пунктов, страниц, разделов, требующих изменений или дополнений


Прошито
страница(а)