

Государственное бюджетное профессиональное образовательное учреждение Самарской области «Сызранский колледж искусств и культуры им. О.Н. Носцовой»

Носцовой»

УТВЕРЖДАЮ:
Директор ГБПОУ СКИК
Алмаева Т.В. /

Приказ от «28» декабря 2022 г. № 296



ПОЛОЖЕНИЕ

ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

г.о Сызрань

1. ОБЩИЕ ПОЛОЖЕНИЯ

Положение об информационной безопасности (далее - Положение) Государственного бюджетного профессионального образовательного учреждения Самарской области «Сызранский колледж искусств и культуры им. О.Н. Носцовой» (далее – Учреждение) разработано в соответствии с требованиями Федерального закона от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Положение устанавливает:

- объекты защиты информации и субъекты доступа к информации информационных систем и ресурсов;
- основные угрозы информационной безопасности Учреждения;
- основные принципы построения системы защиты информации Учреждения;
- меры, методы и средства обеспечения информационной безопасности Учреждения.

В настоящем Положении используются следующие основные термины и понятия:

Информационный обмен - процесс передачи и получения информации между пользователями и информационной системой, а также между элементами информационной системы;

Авторизованный субъект доступа - сотрудник, которому предоставлены соответствующие права доступа к элементам ИСПДн;

Администратор безопасности - лицо или группа лиц, ответственных за реализацию мероприятий по защите информации и осуществляющих постоянную организационную поддержку функционирования применяемых средств защиты информации;

Атака на информационную систему - любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путем использования уязвимостей системы;

Безопасность информации - защищенность информации от нарушения конфиденциальности, нарушения целостности, утраты или снижения степени доступности, а также незаконного тиражирования;

Целостность информации – возможность внесения изменений только авторизованным субъектам доступа.

Доступность информации - возможность доступа к информации авторизованного субъекта доступа;

Внешний воздействующий фактор- воздействующий на систему фактор, внешний по отношению к объекту информатизации;

Внутренний воздействующий фактор - воздействующий на систему фактор, внутренний по отношению к объекту информатизации;

Вредоносные программы - программы, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы;

Угроза безопасности информации - потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию, которое наносит ущерб собственнику, или пользователю информации;

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию;

Организационные меры защиты - это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности информации;

Технические средства защиты - электронные устройства и специальные программы, выполняющие самостоятельно или в комплексе с другими средствами функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации);

Система информационной безопасности - совокупность организационных мероприятий, технических средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности;

Нарушитель - лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

2. ОБЪЕКТЫ, ПОДЛЕЖАЩИЕ ЗАЩИТЕ

В Учреждении обрабатывается информация, содержащая сведения ограниченного распространения (служебная информация, персональные данные), и открытые сведения. защите подлежат все информационные системы Учреждения, независимо от их местонахождения, числящиеся на бухгалтерском учете Учреждения.

2.1. Основные объекты, подлежащие защите:

- информационные системы персональных данных (далее ИСПДн), а также открытая (общедоступная) информация, необходимая для работы Учреждения, независимо от формы и вида ее представления;
- процессы обработки информации в информационных системах Учреждения, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

2.2. Особенности объектов, подлежащих защите:

- территориальная распределенность элементов информационных систем;
- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- необходимость обеспечения непрерывности функционирования органов Учреждения;
- высокая интенсивность информационных потоков;
- разнообразие категорий пользователей.

3.ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1.Субъекты доступа к информации.

Субъектами доступа к информации при обеспечении информационной безопасности техникума являются:

-структурные подразделения Учреждения, участвующие в информационном обмене;

-сотрудники Учреждения, в соответствии с возложенными на них должностными обязанностями;

-физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах Учреждения (в соответствии со ст.14 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных»);

-сотрудники внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем.

Перечисленным субъектам доступа к информации необходимо обеспечить:

-своевременность доступа к необходимой им информации (ее доступность);

-достоверность (полноту, точность, актуальность, целостность) информации;

-конфиденциальность (сохранение в тайне) определенной части информации, защиту от навязывания ложной (недостоверной, искаженной) информации;

-возможность осуществления контроля и управления процессами обработки и передачи информации;

-защиту информации от незаконного распространения.

3.2 Цели защиты информации.

Основной целью, на достижение которой направлено настоящее Положение, является защита от возможного нанесения субъектом доступа к информации материального, физического, морального или иного ущерба посредством

случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи.

3.3. Основные задачи системы обеспечения информационной безопасности Учреждения.

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности Учреждения должна обеспечивать решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем Учреждения;
- создание механизма оперативного реагирования на угрозы безопасности информации;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования систем Учреждения посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Учреждения - обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в системах Учреждения программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.4. Основные пути решения задач системы обеспечения информационной безопасности Учреждения достигаются:

- учетом всех подлежащих защите информационных систем Учреждения;
- полнотой, реальной выполнимостью и непротиворечивостью требований правовых актов Учреждения по вопросам обеспечения информационной безопасности;
- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности;

- наделением каждого сотрудника (пользователя) Учреждения минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Учреждения;
- четким знанием и строгим соблюдением всеми пользователями информационных системы Учреждения, требований правовых актов Учреждения по вопросам обеспечения информационной безопасности;
- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Учреждения;
- непрерывным поддержанием необходимого уровня защищенности элементов информационных систем Учреждения;
- применением программно-аппаратных средств защиты информации и непрерывной административной поддержкой их использования;
- эффективным контролем над соблюдением пользователями информационных ресурсов Учреждения требований по обеспечению информационной безопасности.

4.ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ

4.1. Существуют два вида угроз информационной безопасности:

- Искусственные угрозы – это угрозы, вызванные деятельностью человека;
- Естественные угрозы - это угрозы, вызванные воздействиями на информационную систему и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека.

4.2. Угрозы информационной безопасности и их источники.

Наиболее значимыми угрозами информационной безопасности техникума (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение функциональности компонентов информационных систем Учреждения, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных ресурсов Учреждения, а также фальсификация (подделка) документов;
- нарушение конфиденциальности (разглашение, утечка) персональных данных.

4.3. Основные источники угроз безопасности информации Учреждения:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационных систем Учреждения (в том числе сотрудников, отвечающих за обслуживание и администрирование элементов информационных систем), приводящие к непроизводительным затратам

времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем;

- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам Учреждения пользователей (в том числе работников, отвечающих за обслуживание и администрирование элементов информационных систем), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем Учреждения;

- удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего через сеть Интернет), через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к информационным ресурсам;

- ошибки, допущенные при разработке элементов информационных систем Учреждения и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации);

- технические сбои элементов информационных систем.

4.4. Пути реализации угроз информационной безопасности Учреждения.

4.4.1. Пути реализации непреднамеренных искусственных угроз информационной безопасности Учреждения.

Работники Учреждения, являющиеся авторизованными субъектами доступа информационных систем, а также работники, обслуживающие отдельные элементы информационных систем, являются внутренними источниками случайных воздействий.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности Учреждения (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неосторожные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем Учреждения;

- неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;

- разглашение, передача или утрата атрибутов разграничения доступа (ключей (логинов), паролей, ключевых носителей и т. п.);

- игнорирование установленных правил при работе с информационными ресурсами;

- проектирование алгоритмов обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для

функционирования информационных систем и информационной безопасности Учреждения;

- пересылка информации по ошибочному электронному адресу (устройства); ввод ошибочных данных;
- неосторожная порча носителей информации;
- неосторожное повреждение каналов связи;
- неправомерное отключение оборудования или изменение режимов работы элементов информационных систем;
- заражение компьютеров вирусами;
- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности элементов информационных систем или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных);
- некомпетентное использование, настройка или неправомерное отключение средств защиты.

4.4.2. Пути реализации преднамеренных искусственных (субъективных) угроз информационной безопасности.

Основные возможные пути умышленной дезорганизации работы, вывода элементов информационных систем из строя, несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить):

- умышленные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем Учреждения;
- действия по дезорганизации функционирования информационных систем Учреждения, хищение электронных документов и носителей информации; несанкционированное копирование электронных документов и носителей информации;
- умышленное искажение информации, ввод неверных данных;
- отключение или вывод из строя подсистем обеспечения функционирования элементов информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи);
- перехват данных, передаваемых по каналам связи и их анализ;
- незаконное получение атрибутов разграничения доступа (используя халатность пользователей, путем подделки, подбора пароля);
- несанкционированный доступ к ресурсам информационных систем с рабочих станций авторизованных субъектов доступа;
- хищение или вскрытие шифров криптозащиты информации;
- внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования элементов информационных систем Учреждения;
- незаконное использование элементов информационных систем, нарушающее права третьих лиц;
- применение подслушивающих устройств, фото и видео съемка для несанкционированного съема информации.

4.5. Пути реализации основных естественных угроз информационной безопасности:

- выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;
- выход из строя или невозможность использования линий связи;
- пожары и стихийные бедствия.

4.6. Модель возможных нарушителей.

4.6.1. Типы нарушителей:

С учетом категории лиц, мотивации, квалификации, наличия специальных средств:

Некомпетентный (невнимательный) *пользователь* – работник Учреждения (или подразделения внешней организации, занимающейся обслуживанием информационных систем Учреждения), предпринимая попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационных систем с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией, действуя по ошибке, некомпетентности или халатности без умысла и использующий при этом только штатные средства;

Любитель – работник Учреждения (или подразделения внешней организации, занимающейся обслуживанием информационных систем Учреждения), пытающийся нарушить систему защиты без корыстных целей, умысла или для самоутверждения. При этом используются различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств), нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства.

Внутренний (внешний) *злоумышленник* - авторизованный субъект доступа (постороннее лицо) действующий целенаправленно (в том числе в сговоре с лицами, не являющимися работниками Учреждения). При этом используются методы и средства взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Учреждения.

4.6.2. Внутренние нарушители:

Внутренним нарушителем может быть лицо из следующих категорий работников Учреждения:

- зарегистрированные пользователи и персонал, обслуживающий технические средства информационных систем Учреждения;

- работники, в том числе руководители, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам Учреждения, но имеющие доступ в здания и помещения;
- работники, в том числе руководители, задействованные в разработке и сопровождении программного обеспечения.

4.6.3. Внешние нарушители:

Внешним нарушителем может быть лицо из следующих категорий:

- работники Учреждения, с которыми прекращен (расторгнут) трудовой договор;
- представители внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием элементов информационных систем;
- члены преступных организаций или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в локальную вычислительную сеть Учреждения из внешних телекоммуникационных сетей (хакеры);
- администраторы автоматизированных систем Учреждения, имеющие неограниченный доступ к информационным ресурсам компонентов корпоративной информационной системы.

Администраторы автоматизированных систем могут относиться как к внешним, так и к внутренним нарушителям.

4.7. Утечка информации по техническим каналам При проведении мероприятий и эксплуатации технических средств устанавливаются следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств Учреждения и линий передачи информации;
- наводки информативного сигнала, обрабатываемого техническими средствами локальной вычислительной сети Учреждения, на провода и линии, выходящие за пределы контролируемой зоны Учреждения, в т.ч. на цепи заземления и электропитания;
- электрические сигналы или радиоизлучения, обусловленные воздействием на средства передачи информации высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их информативным сигналом;
- акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;
- вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на

строительные конструкции и инженерно-технические коммуникации выделенных помещений;

- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства («закладки»);

- перехват информации или воздействие на нее с использованием технических средств может вестись непосредственно из зданий, расположенных в непосредственной близости от объекта, мест временного пребывания, заинтересованных в перехвате информации или воздействии на нее лиц при посещении ими Учреждения, а также с помощью скрытно устанавливаемой автономной автоматической аппаратуры.

5. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ.

Построение системы защиты информации Учреждения и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

5.1. Законность.

Предполагает осуществление защитных мероприятий и разработку системы защиты информации Учреждения в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по информационной безопасности, утвержденных органами государственной власти.

Принятые меры информационной безопасности не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к ресурсам конкретных информационных систем. Все пользователи информационных систем Учреждения должны иметь представление об ответственности за правонарушения в области информации.

5.2. Системность.

Системный подход к построению системы защиты информации в учреждении предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности Учреждения. При создании системы защиты учитываются все слабые и наиболее уязвимые места информационных систем Учреждения, а также характер, возможные объекты и направления атак на неё со стороны нарушителей, пути несанкционированного доступа к информации. Система защиты должна строиться с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность.

Комплексное использование методов и средств защиты информационных систем предполагает согласованное применение программных и технических средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

5.4. Непрерывность защиты.

Для обеспечения этого принципа необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, перераспределение полномочий). Порядок получения доступа к информационным ресурсам регламентируется в Инструкции пользователя (Приложение № 1), осуществляющего обработку персональных данных на объектах вычислительной техники.

5.5. Своевременность.

Предполагается упреждающий характер мер обеспечения информационной безопасности, то есть постановка задач по комплексной защите информации и реализация мер обеспечения безопасности информации на ранних стадиях разработки информационных систем. Разработка системы защиты ведется параллельно с разработкой и развитием самой подлежащей защите информационной системы.

5.6. Преемственность и совершенствование.

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Учреждения и систем информационной защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.7. Персональная ответственность.

Предполагает возложение ответственности за обеспечение информационной безопасности на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.8. Минимизация полномочий.

Предполагает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объёме, если это необходимо работнику для выполнения его должностных обязанностей.

5.9. Гибкость системы информационной безопасности.

Предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления Учреждением своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры Учреждения;

- изменение существующих или внедрение принципиально новых информационных систем;
- ввод в эксплуатацию новых технических средств.

5.10. Простота применения средств защиты.

Механизмы и методы системы защиты информации должны быть понятны и просты в использовании. Применение средств и методов защиты не связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не требует от пользователя выполнения малопонятных ему операций.

5.11. Обоснованность и техническая реализуемость.

Предполагает, что информационные технологии, технические и программные средства, средства и меры защиты информации реализуются на современном техническом уровне и обоснованы для достижения заданного уровня безопасности информации и экономической целесообразности, а также соответствуют установленным нормам и требованиям по безопасности информации.

5.12. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты осуществляется профессионально подготовленными специалистами защиты информации Учреждения.

5.13. Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает санкционированные и несанкционированные действия пользователей. Выявленные работниками Учреждения недостатки системы защиты информации доводятся до сведения непосредственного руководителя. О существенных недостатках сообщается руководителю Учреждения.

6. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

6.1. Меры обеспечения информационной безопасности.

6.1.1. Законодательные (правовые) меры обеспечения информационной безопасности к правовым мерам обеспечения информационной безопасности

относятся действующие в Российской Федерации законодательные и иные нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры обеспечения информационной безопасности носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем Учреждения.

6.1.2. Технологические меры обеспечения информационной безопасности к данному виду мер обеспечения информационной безопасности относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.1.3. Организационные (административные) меры обеспечения информационной безопасности.

Организационные (административные) меры обеспечения информационной безопасности – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Организационными (административными) мерами обеспечения информационной безопасности являются:

- регламентация доступа в здание Учреждения;
- регламентация допуска работников к использованию информационных ресурсов;
- анализ требований к элементам системы на основе заявок пользователей на обслуживание и модификацию аппаратных и программных ресурсов;
- обеспечение и контроль физической целостности (неизменности конфигурации) средств вычислительной техники;
- обучение пользователей; деятельность по обеспечению информационной безопасности;
- условия обработки информационных ресурсов конфиденциального характера, ответственность за нарушения установленного порядка пользования информационными ресурсами Учреждения.

6.1.4. Физические меры обеспечения информационной безопасности.

Физические меры обеспечения информационной безопасности основаны на применении механических, электронных или электронно-механических устройств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к элементам информационных систем и защищаемой информации.

6.1.5. Технические меры обеспечения информационной безопасности.

Технические (аппаратно-программные) меры обеспечения информационной безопасности основаны на использовании электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

7. ОСОБЕННОСТИ ОБРАБОТКИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ.

7.1. Все персональные данные субъекта Учреждения следует получать у него самого (для обучающихся Учреждения от родителей – законных представителей). Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

Должностное лицо Учреждения должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению ПД и последствиях отказа дать письменное согласие на их получение.

7.2. Учреждение не имеет права получать и обрабатывать данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

7.3. Субъект персональных данных самостоятельно принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку.

7.4. Обработка указанных данных возможна без его согласия в соответствии со ст.6 Федеральным законом от 27.07.2006 №152 «О персональных данных».

7.5. Согласие на обработку персональных данных оформляется в письменном виде.

7.6. Письменное согласие на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных; цель обработки персональных данных;

перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

перечень действий с персональными данными на совершение которых дается согласие, общее описание

используемых оператором способов обработки персональных данных; срок, в течение которого действует согласие, а также порядок его отзыва.

7.7. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному запросу на имя директора Учреждения.

7.8. Субъект персональных данных имеет право на получение следующей информации:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения; сроки обработки персональных данных, в том числе сроки их хранения;

- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

7.9. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональных данных являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

7.10. Сведения о персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться в персональных данных, относящиеся к другим субъектам персональных данных.

7.11. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при получении письменного запроса субъекта персональных данных или его законного представителя. Письменный запрос должен быть адресован на имя директора Учреждения или уполномоченного руководителем лицо.

7.12. Субъект в праве обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия персональных данных должностных лиц Учреждения при обработке и защите его персональных данных.

8. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ.

8.1. руководитель Учреждения организует работу по построению системы защиты информационной системы. В частности:

- назначает ответственного за организацию защиты информации из числа сотрудников Учреждения;

- утверждает круг лиц, имеющих доступ к защищаемой информации и порядок их работы;

- утверждает комплект документов, определяющих политику в отношении защиты информации в учреждении, а также локальные акты, устанавливающих процедуры,

направленные на предотвращение и выявление нарушений законодательства РФ.

8.2. Ответственный за защиту информации:

- разрабатывает организационно-распорядительные документы по вопросам защиты информации при её обработке с помощью информационной системы;
- контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;
- обеспечивает защиту информации, циркулирующей на объектах информатизации;
- проводит систематический контроль работы систем защиты информации, применяемых в информационной системе, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- проводит инструктаж пользователей информационной системы;
- контролирует выполнение администратором информационной системы обязанностей по обеспечению функционирования систем защиты информации (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам информационной системы, антивирусная защита, резервное копирование данных и т.д.);
- контролирует порядок учёта и хранения машинных носителей конфиденциальной информации;
- участвует в работах по внесению изменений в аппаратно-программную конфигурацию информационной системы;
- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав информационной системы;
- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших доступ к информационной системе;
- требует устранения выявленных нарушений и недостатков, даёт обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- в случае выявления попыток несанкционированного доступа к информации или попыток хищения, копирования, изменения, незамедлительно принимает меры пресечения и докладывает руководителю Учреждения;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

8.3. Несоответствие мер установленным требованиям или нормам по защите информации, является нарушением и влечёт административное наказание ответственных лиц в соответствии с законодательством РФ.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.

9.1. Положение вступает в силу с момента его утверждения.

9.2. Положение является локальным актом образовательного Учреждения. Внесение изменений и дополнений в Положение осуществляется в порядке его принятия.

9.3. Настоящее Положение может быть изменено (дополнено) локальным актом образовательного Учреждения.

Инструкция пользователя при обработке персональных данных на объектах вычислительной техники в ГБПОУ СКИК

1. Общие положения

1.1. Данная Инструкция определяет основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (далее - ПЭВМ) государственного бюджетного профессионального образовательного учреждения Самарской области «Сызранский колледж искусств и культуры им. О.Н. Носцовой» (далее – учреждение).

1.2. Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

1.3. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации).

2. Основные обязанности пользователя

2.1. Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;

2.2. При работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;

2.3. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;

2.4. После окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ;

- 2.5. Оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- 2.6. Не допускать «загрязнение» ПЭВМ посторонними программными средствами;
- 2.7. Знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий.
- 2.8. Знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;
- 2.9. Помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;
- 2.10. Знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;
- 2.11. При применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

3. Требования к антивирусной безопасности

- 3.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.
- 3.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:
 - приостановить работу;
 - немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя;
 - оценить необходимость дальнейшего использования файлов, зараженных вирусом;
 - провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь техника вычислительного центра).

4. Пользователю запрещается

- 4.1. Записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

- 4.2. Удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
- 4.3. Самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;
- 4.4. Самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- 4.5. Осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;
- 4.6. Сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
- 4.7. Отключать (блокировать) средства защиты информации;
- 4.8. Производить какие-либо изменения в подключении и размещении технических средств;
- 4.9. Производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.
- 4.10. Оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

5. Права пользователя ПЭВМ Пользователь ПЭВМ имеет право

- 5.1. Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.
- 5.2. Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

6. Ответственность Пользователя ПЭВМ

Пользователи ПЭВМ несут ответственность за:

- 6.1. Надлежащее выполнение требований настоящей инструкции;
- 6.2. Соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;

- 6.3. Сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;
- 6.4. Сохранность персональных данных.

Инструкция для обучающихся ГБПОУ СО «Сызранский колледж искусств и культуры им. О.Н. Носцовой» обеспечению информационной безопасности при использовании сети «Интернет».

Настоящая инструкция устанавливает порядок работы обучающихся ГБПОУ СО «Сызранский колледж искусств и культуры им. О.Н. Носцовой» в сети Интернет.

Данная инструкция по обеспечению информационной безопасности при использовании сети Интернет разработана для обучающихся Учреждения, с целью урегулирования действия обучающихся во время пользования интернет – ресурсами.

Классным руководителям необходимо ознакомить обучающихся с правилами безопасности в Интернете, провести беседу.

Приведенные правила безопасности в сети Интернет обучающимся необходимо помнить и придерживаться их.

Не рекомендуется размещение личной информации в Интернет сети. Личная информация: номер вашего мобильного телефона, адрес электронной почты, домашний адрес и ваши фотографии, фотографии членов вашей семьи или друзей.

- ✓ Если вы выложите фото или видео в интернете — любой может посмотреть их.
- ✓ Никогда не отвечайте на «Спам» (нежелательную электронную почту).
- ✓ Нельзя открывать файлы, полученные от неизвестных Вам людей. Вы ведь не знаете, что в действительности содержат эти файлы в них могут находиться вирусы или фото/видео с «агрессивным» содержанием.
- ✓ Никогда не добавляйте незнакомых вам людей в свой список контактов в IM (ICQ, MSN messenger и т.д.).
- ✓ Не забывайте, что виртуальные друзья и знакомые могут быть не теми на самом деле, за кого себя выдают.
- ✓ Если около вас или поблизости с вами нет родственников, никогда не встречайтесь в реальности с людьми, с которыми вы познакомились в Интернет сети. Если ваш виртуальный друг в действительности тот, за кого себя выдает, он с пониманием отнесется к вашей заботе о собственной безопасности!
- ✓ В любое время можно рассказать взрослым, если вас кто-либо обидел.

Использование сети Интернет в Образовательном учреждении подчинено следующим принципам:

- соответствия образовательным целям;
- способствования гармоничному формированию и развитию личности;

- уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
- приобретения новых навыков и знаний;
- расширения применяемого спектра учебных и наглядных пособий;
- социализации личности, введения в информационное общество.

Учащимся предоставляется доступ к работе в сети Интернет в компьютерных кабинетах согласно расписанию занятий.

Пользователи сети Интернет имеют право:

- использовать сеть Интернет для работы с информационными ресурсами сети Интернет только в образовательных целях или для осуществления научных изысканий, выполнения гуманитарных и культурных проектов; любое нецелевое использование сети Интернет запрещено;
- производить поиск необходимой информации в сети Интернет;
- сохранять полученную информацию на съемном диске (дискете, CD-ROM, флешнакопителе); съемные диски должны предварительно проверяться на наличие вирусов;
- получать консультации по вопросам, связанным с использованием сети Интернет.

Пользователи сети Интернет обязаны:

- выполнять все требования преподавателя;
- использовать только собственные регистрационные имя (логин) и пароль;
- сохранять оборудование в целостности и сохранности;
- поставить в известность учителя при возникновении технических проблем.

Пользователям сети Интернет запрещается:

- осуществлять действия, запрещенные законодательством РФ;
- посещать сайты, содержащие информацию, запрещенную к распространению в Российской Федерации и/или не совместимую с задачами образования и воспитания в соответствии с утвержденными классификаторами;
- передавать информацию, представляющую коммерческую или государственную тайну; распространять информацию, порочащую честь и достоинство граждан;
- осуществлять действия, направленные на «взлом» любых компьютеров, находящихся как в локальной сети образовательного учреждения, так и за его пределами; использовать возможности сети Интернет для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации;

- работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции;
- устанавливать какое-либо дополнительное программное обеспечение и/или вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на сервере; производить запись информации на жесткий диск рабочей станции;
- работать с объемными ресурсами (video, audio, chat, игры и др.);
- изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем (заставки, фоновые рисунки рабочего стола, стартовые страницы браузеров);
- включать, выключать и перезагружать компьютер без согласования с преподавателем.

Пользователи сети Интернет несут ответственность:

- за содержание передаваемой, сознательно принимаемой и печатаемой информации;
- пользователи, не соблюдающие настоящий регламент работ, лишаются права работы в сети Интернет;
- при нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.