РАССМОТРЕНО
На заседании Общего собрания
(Конференции) работников
И обучающихся ГБПОУ СО «ИТАТиУ»
Протокол №
«2» 16 ноября 2024 г.

УТВЕРЖДАЮ
Директор ГБПОУ СО «ИТАТиУ»
_____ И.Н. Кузовенкова
Приказ №117 от «16» ноября 2024 г.

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
в ГБПОУ СО «Ивантеевский техникум агропромышленных технологий и управления»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Положение об информационной безопасности (далее - Положение) Государственного бюджетного профессионального образовательного учреждения «Ивантеевский политехнический лицей» (далее - лицей) 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 лицея;

• основные принципы построения системы защиты информации лицея;

• меры, методы и средства обеспечения информационной безопасности лицея.

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 техникуме обрабатывается информация, содержащая сведения ограниченного распространения (служебная информация, персональные данные), и открытые сведения. Защите подлежат все информационные системы лицея, независимо от их местонахождения, числящиеся на бухгалтерском учете лицея.

2.1.Основные объекты, подлежащие защите:

• информационные системы персональных данных (далее ИСПДн), а также открытая (общедоступная) информация, необходимая для работы лицея, независимо от формы и вида ее представления;

• процессы обработки информации в информационных системах лицея, 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 лицея;

• 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 лицея являются:

-структурные подразделения лицея, участвующие в информационном обмене;

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

-физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах лицея (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 лицея.

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности лицея 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 лицея;

- 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 лицея посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам лицея - 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 лицея 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 лицея достигаются:

-учетом всех подлежащих защите информационных систем лицея;

-полнотой, реальной выполнимостью и непротиворечивостью требований правовых актов лицея по вопросам обеспечения информационной безопасности;

-подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности;

-наделением каждого сотрудника (пользователя) лицея минимально необходимыми для

выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам лицея;

-четким знанием и строгим соблюдением всеми пользователями информационных систем лицея требований правовых актов лицея по вопросам обеспечения информационной безопасности;

-персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам лицея;

-непрерывным поддержанием необходимого уровня защищенности элементов информационных систем лицея;

-применением программно-аппаратных средств защиты информации и непрерывной административной поддержкой их использования;

-эффективным контролем над соблюдением пользователями информационных ресурсов лицея требований по обеспечению информационной безопасности.

4. ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЦЕЯ

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 техникума, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

- нарушение целостности (искажение, подмена, уничтожение) информационных ресурсов техникума, а также фальсификация (подделка) документов;

-нарушение конфиденциальности (разглашение, утечка) персональных данных.

4.3. Основные источники угроз безопасности информации лицея:

- 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 лицея (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 техникума пользователей (в том числе сотрудников, 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 техникума;

- 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 лицея 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 непреднамеренных искусственных угроз информационной безопасности лицея.

Сотрудники лицея, являющиеся авторизованными субъектами доступа информационных систем, а также сотрудники, обслуживающие отдельные элементы информационных систем, являются внутренними источниками случайных воздействий.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации лицея (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 лицея;

- 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 лицея;

-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.

Пути реализации преднамеренных искусственных (субъективных) угроз информационной безопасности:

Основные возможные пути умышленной дезорганизации работы, вывода элементов информационных систем лицея 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 лицея;

-действия по дезорганизации функционирования информационных систем лицея, 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 лицея;

-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 безопасности информации:

-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. Типы нарушителей.

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

- *Некомпетентный (невнимательный) пользователь* - сотрудник лицея (или внешней организации, занимающейся обслуживанием информационных систем лицея), предпринимающий 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* - сотрудник лицея (или внешней организации, занимающейся обслуживанием информационных систем лицея), 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 нарушитель* - лицо из следующих категорий сотрудников лицея:

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

- сотрудники, в том числе руководители, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам лицея, но имеющие доступ в здания и помещения;

- сотрудники, в том числе руководители, задействованные в разработке и сопровождении программного обеспечения.

- *Внешний нарушитель* - лицо из следующих категорий:

- сотрудники лицея, 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 лицея из

внешних телекоммуникационных сетей (хакеры).

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 лицея и линий передачи информации;

- наводки информативного сигнала, обрабатываемого техническими средствами локальной вычислительной сети лицея, на провода и линии, выходящие за пределы контролируемой зоны лицея, в т.ч. на цепи заземления и электропитания;

- электрические сигналы или радиоизлучения, обусловленные воздействием на средства передачи информации высокочастотных сигналов, создаваемых с помощью 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 объектов лицея, мест временного пребывания заинтересованных в перехвате информации или воздействии на нее лиц при посещении лицея, а также с помощью скрытно устанавливаемой автономной автоматической аппаратуры.

5. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ТЕХНИКУМА

5.1. Законность.

Предполагает осуществление защитных мероприятий и разработку системы защиты информации лицея в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по безопасности информации, 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 лицея должны иметь представление об ответственности за правонарушения в области информации.

5.2. Системность.

Системный подход к построению системы защиты информации в лицее предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной

безопасности лицея.

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).

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.

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 лицея 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 сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников 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 объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

5.9. Гибкость системы информационной безопасности предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления мэрией своей деятельности. В число таких изменений входят:

-изменения организационной и штатной структуры техникума;

-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 структурного подразделения защиты информации лицея.

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 сотрудниками лицея недостатки системы защиты информации доводятся до сведения руководителей соответствующего уровня. О существенных недостатках сообщается соответствующему руководителю лицея.

6. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1 Организованное подключение средства защиты, обеспечивающего контроль и фильтрацию сетевого трафика.

6.2 Принятие мер по разграничению доступа между сетями, взаимодействующими с сетью «Интернет» через самостоятельно организованное подключение, и имеющими несанкционированного доступа потенциальных нарушителей безопасности информации и вредоносного ПО КСПД, RSNet, и иным сторонним ресурсам.

6.3 Соблюдение парольной политики, установленной для конкретного ресурса его создателем.

6.4 Использование актуальных версий средств защиты информации.

РАЗРАБОТАНО

Должность	ФИО	Подпись	Дата
Заместитель директора по учебно-производственной работе	Баданов Ю.Н.		1.09.2022