МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР ОБРАЗОВАНИЯ № 27»

УТВЕРЖДАЮ:
директор МБОУ ЦО № 27
О.И. Маленков
приказ от 24.11.2016г.
№ 460-о

ПОЛОЖЕНИЕ
об информационной безопасности МБОУ ЦО № 27

2016
г. Тула

Маленков Олег Игоревич

Подписано цифровой подписью: Маленков Олег Игоревич
Дата: 2021.05.26 14:05:47 +03'00'

1. Введение

Настоящее Положение об информационной безопасности является официальным документом, в котором определена система взаимоувязанных понятий и принципов по обеспечению информационной безопасности МБОУ ЦО № 27. Необходимость разработки Положения обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов. Настоящее Положение определяет основные цели и задачи, а также общую стратегию построения системы защиты информации. Положение разработано в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты, с позиции комплексного применения технических и организационных мер и средств защиты. Под информационной безопасностью понимается защищённость данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности, а также к прогнозированию и предотвращению таких воздействий.

Положение служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности МБОУ ЦО № 27, а также нормативных и методических документов, обеспечивающих её реализацию. Положение является методологической основой для формирования и проведения единой политики в области обеспечения информационной безопасности,принятия управленческих решений и разработки практических мер по воплощению политики безопасности и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз,координации деятельности структурных подразделений МБОУ ЦО № 27 при проведении работ по развитию и эксплуатации информационных систем с соблюдением требований обеспечения безопасности, разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения информационной безопасности,область применения положения распространяется на подразделения МБОУ ЦО № 27, эксплуатирующие технические и программные средства обработки информации,правовой базой для разработки настоящего положения служат

требования действующих в России законодательных и нормативных документов по обеспечению информационной безопасности.

2. Общие положения

Настоящее положение определяет основные цели и задачи, а также общую стратегию построения системы защиты данных МБОУ ЦО № 27. Положение определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Система информационной безопасности представляет собой совокупность организационных и технических мероприятий для защиты данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ними.

Безопасность данных достигается путём исключения несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение данных, а также иных несанкционированных действий.Система защиты данных (СЗД) включает организационные меры и технические средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки информации. Эти меры призваны обеспечить конфиденциальность информации (защита от несанкционированного ознакомления), целостность информации (актуальность и непротиворечивость информации, еёзащищённость от разрушения и несанкционированного изменения),доступность информации (возможность за приемлемое время получить требуемую информационную услугу). Организационные меры предусматривают создание и поддержание правовой базы в актуальном состоянии.

3. Задачи системы защиты данных.

Основной целью СЗД является минимизация ущерба от возможной реализации угроз безопасности. Для достижения основной цели система безопасности должна обеспечивать эффективное решение следующих задач: защиту от вмешательства в процесс функционирования посторонних лиц (возможность использования информационной системой и доступ к её ресурсам должны иметь только зарегистрированные установленным порядком пользователи),разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения,защиту информации от утечки по

техническим каналам при её обработке, хранении и передаче по каналам связи; своевременное выявление источников угроз безопасности, создание механизма оперативного реагирования на угрозы безопасности и негативные тенденции,создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц.

4. Основные принципы построения системы комплексной защиты информации.

Построение системы обеспечения безопасности данныхМБОУ ЦО № 27 и её функционирование должны осуществляться в соответствии со следующими основными принципами: законность,предполагает осуществление защитных мероприятий и разработку СЗД в соответствии с действующим законодательством в области защиты информации, утверждённых органами государственной власти и управления в пределах их компетенции. Пользователи и обслуживающий персонал СЗДМБОУ ЦО № 27 должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за несоблюдение установленных правил. Системность. Системный подход к построению СЗД центра предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки данных, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределённые системы и НСД к информации. Система защиты должна строиться с учётом не только всех известных каналов проникновения и НСД к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности. Комплексность. Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов. Создание защитных рубежей осуществляется с учётом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Непрерывность защиты. Защита данных - не разовое мероприятие и не простая совокупность проведённых мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла. В соответствии с этим принципом должны приниматься меры по недопущению перехода СЗД в незащищённое

состояние. Своевременность. Предполагает упреждающий характер мер обеспечения безопасности данных, то есть постановку задач по комплексной защите и реализацию мер обеспечения безопасности данных на ранних стадиях разработки СЗД в целом и её системы защиты информации, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Преемственность и совершенствование. Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования СЗД и её системы защиты с учётом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области. Персональная ответственность. Предполагает возложение ответственности за обеспечение безопасности СЗД и системы их обработки 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 чётко известен. Доступ к информации должен предоставляться только в том случае и объёме, если это необходимо сотруднику для выполнения его должностных обязанностей. Взаимодействие и сотрудничество. Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность СЗДМБОУ ЦО № 27, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности администратора системы. Простота применения средств защиты. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций. Обязательность контроля. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

5. Правила доступа к ресурсам Интернет и работы с электронной почтой.

- Доступ в Интернет предоставляется с санкции начальника структурного подразделения для выполнения прямых должностных обязанностей, делового общения и сбора информации по ключевым задачам деятельности;
- Вся переписка должна вестись строго с использованием официального электронного адреса;
- Пользуясь электронной почтой и ресурсами Интернета с рабочего места, сотрудник обязан соблюдать принципы делового общения и этикета;
- Запрещается передавать по электронной почте конфиденциальную информацию.

6. Права и обязанности.

Обязанности руководителей:

- Руководители структурных подразделений обязаны обеспечивать строгое соблюдение настоящего положения;
- Руководители структурных подразделений обязаны заранее уведомлять инженера-программиста об увольнении, принятии на работу, отпуске, кадровых перемещениях и других изменениях в штатном расписании.

Пользователь информационных ресурсов имеет право:

- При невозможности выполнения порученной ему работы имеющимися программно-аппаратными средствами сообщить об этом непосредственному руководителю структурного подразделения;
- Обращаться к инженеру-программисту за консультацией по вопросам функционирования информационных ресурсов МБОУ ЦО № 27;
- Сменить свой пароль доступа к информационным ресурсам, не используемым совместно с другими сотрудниками компании;
- Требовать от системного администратора своевременного обеспечения доступа к необходимым информационным ресурсам;

Пользователь информационных ресурсов обязан:

- Исполнять все обязанности, описанные в Положении обинформационной безопасности МБОУ ЦО № 27, инструкциях и других нормативных актах центра образования, описывающих работу пользователей с информационными ресурсами;
- Входить в сеть при каждом сеансе работы с использованием персонального пароля и имени пользователя;
- Информировать системного администраторао обнаружении вирусов, попыток несанкционированного доступа или каких-либо подозрительных действий.

Пользователю информационных ресурсов запрещается:

- Устанавливать, модифицировать или хранить на машинных носителях любое программное обеспечение без согласования с инженером-программистом;
- Самостоятельно разбирать системный блок или проводить работы по установке или обслуживанию любых других аппаратных средств.
- Самостоятельно устанавливать (менять) пароли на доступ к информационным ресурсам МБОУ ЦО № 27, используемым совместно с другими сотрудниками компании, без предварительного оповещения;
- Передавать кому бы то ни было свой пароль, а так же хранить свой пароль в легкодоступном месте и в явной форме;
- Запрашивать и получать из Интернета программные продукты, мультимедийные данные или изображения, кроме случаев, связанных с производственной необходимостью;
- При работе с электронной почтой запрещается открывать сообщения сомнительного содержания, или пришедшие от неизвестного отправителя;
- Использовать любые программные и аппаратные средства, которые могут привести к перегрузке сети или иным способом негативно повлиять на её работу;
- Использовать программы подбора паролей пользователей других компьютеров сети, сканирования адресов других пользователей, подделки служебной информации о компьютере;
- Использовать программы выявления неисправности конфигураций других компьютеров и устройств, подключённых к сети;
- Вносить изменения в информационные ресурсы, не принадлежащие самому пользователю;
- Использовать компьютеры для любых видов противозаконной деятельности.

Ответственность:

- Пользователь несёт ответственность за целостность и сохранность вверенных ему информационных ресурсов;
- Пользователь несёт полную ответственность за все действия, совершенные от его имени, с использованием его учётной записи;
- Пользователь несёт полную ответственность за противоправные действия и действия, нарушающие нормативные акты МБОУ ЦО № 27, в соответствии с нормативными документами компании и законодательством РФ;
- При несоблюдении пользователями условий настоящегоположения к ним применяется административные меры наказания, вплоть до увольнения, в соответствии со степенью вины, установленной служебным расследованием.