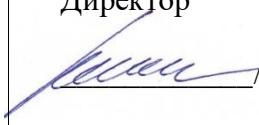
Принято на заседании педагогического совета Протокол №_1 от «29» августа 2018г.	Утверждаю: Директор  /Лещёва Т.И./ Приказ № 23.2 от «29» августа 2018г.

Положение по информационной безопасности Негосударственного общеобразовательного частного учреждения «Православный Центр непрерывного образования во имя преподобного Серафима Саровского»

1. Общие положения

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности

1.2. Данное положение разработано в соответствии с Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.). Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации". Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных".

1.3. Под информационной безопасностью Негосударственного общеобразовательного частного учреждения «Православный Центр непрерывного образования во имя преподобного Серафима Саровского» (далее – Центра) следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.4. К объектам информационной безопасности в Центре относятся:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- информацию, защита которой предусмотрена законодательными актами РФ в т. ч. персональные данные;
- средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

1.5. Система информационной безопасности (далее - СИБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата):
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.6 Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая зашита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе:
- организационная зашита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба:
- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2.Правовые нормы обеспечения информационной безопасности

2.1. Центр имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Центра, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

2.2. Центр обязан обеспечить сохранность конфиденциальной информации.

2.3. Администрация Центра:

- назначает ответственного за обеспечение информационной безопасности;
- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
- имеет право включать требования по защите информации в договоры по всем видам деятельности;
- разрабатывает перечень сведений конфиденциального характера;
- имеет право требовать защиты интересов Центра со стороны государственных и судебных инстанций.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора Центра о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Центра и др.

2.5.порядок допуска сотрудников Центра к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и Центра об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3. Мероприятия по обеспечению информационной безопасности

Для обеспечения информационной безопасности в Центре требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности Центра;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;
- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Центра;
- учет всех носителей конфиденциальной информации.

4. Организация работы с информационными ресурсами и технологиями

4.1. Система организации делопроизводства:

- учет всей документации Центра, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов Центра в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

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

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

4.2.2. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

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

4.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

4.2.5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы Центра.

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

4.3.Для организации делопроизводства приказом директора Центра назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором Центра. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

5. О системном администрировании и обязанностях ответственного за информационную безопасность

5.1. Задачи связанные с мерами системного администрирования, обеспечивающего информационную безопасность являются частью работы системного администратора в Центре.

5.2. Для решения задач информационной безопасности системный администратор должен:

следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);

- обеспечивать функционирование программно-аппартного комплекса защиты по внешним цифровым линиям связи;
- обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;
- обеспечивать нормальное функционирование системы резервного копирования.

6. Антивирусная защита

Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.) Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта.

В связи с этим не допускается работа без организации антивирусной защиты.

Антивирусная защита организуется на уровне рабочих станций и сервера посредством лицензионного антивирусного программного обеспечения.

Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

За своевременное обновление антивирусного программного обеспечения отвечает системный администратор.