МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА

СЕЛА ВОЗНЕСЕНСКОЕ АМУРСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ХАБАРОВСКОГО КРАЯ

|  |  |  |
| --- | --- | --- |
| ПРИНЯТОна заседании Педагогического советаПротокол № 1 от 30 августа 2019 г  |  | УТВЕРЖДЕНОприказом директораМБОУ СОШ с. Вознесенское№ 196 02 сентября 2019 г. |

Положение об ответственном лице, ответственном за обеспечение информационной безопасности

1. Общие положения

Лицо, ответственное за обеспечение информационной безопасности назначается приказом директора учреждения.

1. Задачи

Основные задачи лица, ответственного за обеспечение информационной безопасности заключаются в следующем.

1. Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
2. Обеспечение постоянного контроля за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
3. Разработка и внесение предложений директору учреждения по совершенствованию и развитию системы обеспечения безопасности и защиты информации, в том числе персональных данных.

3. Функции

Для выполнения поставленных задач лицо, ответственное за обеспечение информационной безопасности осуществляет следующие функции.

1. Готовит и представляет на рассмотрение директору учреждения проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.
2. Организует и проводит классификацию информационных систем на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных в соответствии с установленными требованиями.
3. Разрабатывает и реализует комплекс организационных и мер по обеспечению защиты информации от:
* неправомерного доступа;
* уничтожения;
* модифицирования;
* блокирования;
* копирования;
* предоставления;
* распространения;
* а также от иных неправомерных действий в отношении такой информации;
1. Для защиты информации, в том числе персональных данных от неправомерного доступа обеспечивает:

-контроль за строгим соблюдением Порядка доступа к конфиденциальной информации, в том числе к персональным данным;

-предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

-своевременное обнаружение фактов несанкционированного доступа к информации;

-предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

-возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

1. При создании и эксплуатации корпоративных информационных систем:
* самостоятельно разрабатывает и внедряет методы и способы защиты информации, соответствующие установленным требованиям.
1. Разрабатывает и реализует меры организационного и технического характера по недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
2. Разрабатывает и реализует меры по информированию и обучению персонала, в том числе вновь принимаемых на работу лиц, по вопросам защиты информации и персональных данных.
3. Контролирует выполнение установленных требований по:

-осуществлению обмена персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств:

-размещению информационных систем, специального оборудования и охране помещений, в которых ведется работа с персональными данными, организации режима обеспечения безопасности в этих помещениях в части обеспечения сохранности носителей персональных данных и средств защиты информации, а также исключения возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

-соблюдению парольной защиты;

-соблюдению установленного регламента работы с электронной почтой;

-соблюдению требований к программному обеспечению и его использованию.

В соответствии с установленными нормативно-правовыми актами требованиями обеспечивает:

* определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
* разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
* проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
* установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
* обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
* учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
* учет лиц, допущенных к работе с персональными данными в информационной системе;
* контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
* разбор и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
* описание системы защиты информации, в том числе персональных данных;
* ежегодное планирование работы по совершенствованию системы защиты информации, в том числе персональных данных;
* подготовку и предоставление отчётов директору учреждения, а также по требованию надзорных и иных уполномоченных органов об организационных и технических мероприятиях по защите информации, в том числе персональных данных;
* постоянный контроль за обеспечением уровня защищенности информации.

4. Ответственность

Лицо, ответственное за обеспечение информационной безопасности несет ответственность перед директором учреждения согласно действующему законодательству, нормативно-правовым и локальным нормативным правовым актам за обеспечение:

-выполнения поставленных задач и функций,

-работы с документами и их сохранности, своевременного и качественного исполнения поручений и обращений,

-выполнения требований правил внутреннего трудового распорядка.

*Согласовано с управляющим советом школы*

*Протокол № 1 от 30 августа 2019 г*

*Принято с учетом мнения родителей*

*(законных представителей)*

19