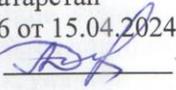


ПРИНЯТО:

Педагогическом советом
МБОУ «Бурнашевская средняя
общеобразовательная школа»
Апастовского муниципального района
Республики Татарстан
Протокол №6 от 15.04.2024 года
Председатель  Д.Х.Вилданова

УТВЕРЖДЕНО:

Директор МБОУ «Бурнашевская средняя
общеобразовательная школа»
Апастовского муниципального района
Республики Татарстан



Д.Х.Вилданова
Приказ № 41 от 15.04.2024 года

Положение о структурном подразделении ведомства, обеспечивающем информационную безопасность

1. Общие положения

1.1. Настоящее положение определяет цели, задачи и функции структурного подразделения ведомства обеспечивающего информационную безопасность ведомств (далее - Подразделение).

1.2. Подразделение в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, другими нормативными правовыми документами в сфере обеспечения информационной безопасности, указаниями руководства ведомства, настоящим положением и иными локальными актами ведомства.

1.3. Подразделение подчиняется сотруднику ведомству, ответственному за обеспечение информационной безопасности в ведомстве.

1.4. Контроль за деятельностью Подразделения осуществляет руководитель ведомства.

2. Цели и задачи деятельности подразделения

2.1. Деятельность Подразделения направлена:

- На исключение или существенное снижение негативных последствий (ущерба) в отношении ведомства вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления (далее - системы и сети) в результате реализации угроз безопасности информации;
- На обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;
- На повышение защищенности ведомства от возможного нанесения ведомству материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования систем и сетей ведомства или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;
- На обеспечение надежности и эффективности функционирования и безопасности систем и сетей, производственных процессов и информационно-технологической инфраструктуры ведомства;
- На обеспечение выполнения требований по информационной безопасности при создании и функционировании систем и сетей и информационно-телекоммуникационной инфраструктуры ведомства.

2.2. Основными задачами деятельности Подразделения являются:

Планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в ведомстве;

Выявление угроз безопасности информации и уязвимостей систем и сетей, программного обеспечения и программно-аппаратных средств;

Предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

Поддержание стабильной деятельности ведомства и производственных процессов ведомства в случае проведения компьютерных атак;

Взаимодействие с Национальным координационным центром по компьютерным инцидентам;

Обеспечение нормативно-правового обеспечения использования информационных ресурсов.

3. Функции подразделения

3.1. Подразделение выполняет следующие функции:

- Разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в ведомстве;

- Разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в ведомстве и представление их руководителю ведомства или сотруднику ведомства, ответственному за обеспечение информационной безопасности в ведомств.

- Выявление и проведение анализа угроз безопасности информации в отношении ведомства, уязвимостей систем и сетей, программного обеспечения программно-аппаратных средств и принятие мер по их устранению;

- Обеспечение в соответствии с требованиями по информационной безопасности, в том числе с целью исключения (невозможности реализации) негативных последствий, разработки и реализации организационных мер и применения средств обеспечения информационной безопасности;

- Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

- Представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах;

- Исполнение указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих ведомству либо используемых ведомством, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

- Проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации) основных процессов ведомства в целях обеспечения информационной безопасности в ведомстве;

- Подготовка отчетов о состоянии работ по обеспечению информационной безопасности в ведомстве;

- Организация развития навыков безопасного поведения в ведомстве, в том числе проведение занятий с руководящим составом и сотрудниками ведомства по вопросам обеспечения информационной безопасности;

- Взаимодействие с сотрудниками ведомства, ответственными за обеспечение безопасности персональных данных и за защиту информации в информационных системах при решении вопросов, связанных с созданием системы защиты информации информационных систем, их эксплуатацией и выводом из эксплуатации;

- Выполнение иных функций, исходя из поставленных руководством ведомства целей и задач в рамках обеспечения информационной безопасности в ведомстве;

4.Права подразделения

4.1.С целью реализации функций Подразделение имеет право:

- Знакомиться с локальными актами ведомства, регламентирующими процессы обработки информации.
- Запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений ведомства, необходимым для принятия решений по всем вопросам, отнесенным к компетенции Подразделения.
- Готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности.
- Контролировать деятельность любого структурного подразделения ведомства по выполнению требований к обеспечению информационной безопасности.
- Постоянно повышать профессиональные компетенции знания и навыки сотрудников в области обеспечения информационной безопасности.
- Участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций.
- Участвовать в работе комиссий ведомства при рассмотрении вопросов обеспечения информационной безопасности.
- Вносить предложения руководству ведомства о приостановлении работ в случае обнаружения факта нарушения информационной безопасности.
- Вносить представления руководству ведомства в отношении сотрудников ведомства при обнаружении фактов нарушения сотрудниками установленных требований безопасности информации в ведомстве, в том числе ходатайствовать о привлечении указанных сотрудников к административной или уголовной ответственности.
- Вносить на рассмотрение руководству ведомства предложения по вопросам деятельности Подразделения.
- Обращаться за необходимыми разъяснениями по вопросам обработки персональных данных к ответственному за организацию обработки персональных данных.

5.Взаимоотношения и связи подразделения

5.1.Подразделение осуществляет свои полномочия во взаимодействии со структурными подразделениями ведомства, а также в пределах своей компетенции с иными органами (организациями) и гражданами в установленном порядке.

5.2.По указанию руководства ведомства осуществляет взаимодействие с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и ведомством.

6.Показатели эффективности и результативности подразделения

6.1.Эффективность и результативность деятельности Подразделения определяются по итогам выполнения ведомством программы обеспечения информационной безопасности.

7.Ответственность

7.1.Сотрудники Подразделения несут ответственность:

- За ненадлежащее выполнение возложенных на них обязанностей в соответствии с утвержденными должностными регламентами и настоящим Положением;
- За разглашение информации в пределах, установленных действующим административным уголовным и гражданским законодательством Российской Федерации;
- За несоблюдение требований локальных актов ведомства по обеспечению информационной безопасности, в пределах, установленных трудовым договором (служебным контрактом).