

МИНИСТЕРСТВО ЭНЕРГЕТИКИ, ПРОМЫШЛЕННОСТИ И СВЯЗИ
СТАВРОПОЛЬСКОГО КРАЯ
государственное бюджетное профессиональное образовательное
учреждение «Невинномысский химико-технологический колледж»
(ГБПОУ НХТК)



СВЕРЖДАЮ

Директор

Н.В. Фурса

2017

ПОЛОЖЕНИЕ

об ответственном за организацию защиты информации
ГБПОУ НХТК

1 Общие положения

1.1 Ответственный за организацию защиты информации (далее – Ответственный) является сотрудником государственного бюджетного профессионального образовательного учреждения «Невинномысский химико-технологический колледж» (далее – Учреждение).

1.2 Ответственный назначается приказом директора Учреждения.

1.3 Ответственный подчиняется непосредственно директору и проводит мероприятия по защите информации в интересах Учреждения.

1.4 Ответственный в своей деятельности руководствуется:

1) Конституцией Российской Федерации;

2) Федеральными законами Российской Федерации и нормативными правовыми актами органов государственной власти по вопросам защиты информации;

3) государственными стандартами Российской Федерации в области защиты информации;

4) руководящими и нормативными правовыми документами Федеральной Службы по техническому и экспортному контролю России;

5) локальными нормативными актами Учреждения по защите информации;

6) правилами внутреннего трудового распорядка;

7) настоящим Положением.

1.5 Деятельность Ответственного осуществляется согласно плану мероприятий по защите информации Учреждения на год.

2 Задачи

На Ответственного за организацию защиты информации возложены следующие задачи.

2.1 Организация внутреннего контроля за соблюдением работниками Учреждения норм законодательства Российской Федерации по защите информации, в том числе требований, предъявляемых к защите персональных данных.

2.2 Разработка, внедрение и актуализация локальных актов по вопросам защиты информации.

2.3 Доведение до сведения работников Учреждения, непосредственно осуществляющих обработку защищаемой информации, положений законодательства Российской Федерации по защите информации, локальных актов по вопросам защиты информации, требований к защите информации, и проведение обучения указанных работников.

2.4 Организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и осуществление контроля за приемом и обработкой таких обращений и запросов.

2.5 Организация комплексной защиты объектов информатизации Учреждения, а именно:

1) информационных ресурсов, представленных в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащих защищаемую информацию Учреждения;

2) средств и систем информатизации (средств вычислительной техники, информационно-вычислительных комплексов, локальных вычислительных сетей и корпоративных информационных систем), программных средств (операционных систем, систем управления базами данных, другого общесистемного и прикладного программного обеспечения), автоматизированных систем управления информационными, управленческими и технологическими процессами, систем связи и передачи данных, технических средств приёма, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорных устройств и других технических средств обработки графической, смысловой и буквенно-цифровой информации), используемых для реализации процессов ведения деятельности и обработки защищаемой информации Учреждения.

2.6 Организация защиты информации Учреждения.

2.7 Разработка и проведение организационных мероприятий, обеспечивающих безопасность объектов защиты Учреждения, своевременное выявление и устранение возможных каналов утечки информации.

2.8 Организация проведения работ по технической защите информации на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций Учреждения.

2.9 Реализация технических мер, обеспечивающих своевременное выявление возможных технических каналов утечки информации в подразделениях Учреждения.

2.10 Методическое руководство системой обеспечения информационной безопасности Учреждения.

2.11 Организация контроля состояния и проведение оценки эффективности системы обеспечения информационной безопасности, а также реализация мер по её совершенствованию.

2.12 Внедрение в информационную инфраструктуру Учреждения современных методов и средств обеспечения информационной безопасности.

3 Функции

Для решения поставленных задач Ответственный за организацию защиты информации осуществляет следующие функции.

3.1 Разработка и внедрение правовых, организационных и технических мер по комплексному обеспечению безопасности защищаемой информации.

3.2 Обеспечение соблюдения режима конфиденциальности при обработке защищаемой информации.

3.3 Планирование работы по защите информации на объектах Учреждения.

3.4 Контроль за выполнением мер по защите информации, анализ материалов контроля, выявление недостатков и нарушений. Разработка и реализация мер по их устранению.

3.5 Обеспечение взаимодействия с контрагентами по вопросам организации и проведения проектно-изыскательских, научно-исследовательских, опытно-конструкторских и других работ по защите информации. Участие в разработке технических заданий на выполняемые исследования и работы.

3.6 Контроль за выполнением плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите информации, выполняемых контрагентами.

3.7 Разработка и принятие мер по обеспечению финансирования работ по защите информации, в том числе выполняемых по договорам.

3.8 Проведение работ по технической защите информации на объектах информатизации Учреждения. Оценка эффективности принятых мер по технической защите информации.

3.9 Обеспечение выбора, установки, настройки и эксплуатации средств защиты информации в соответствии с организационно-распорядительной и эксплуатационной документацией.

3.10 Организация режима обеспечения безопасности помещений, в которых происходит обработка защищаемой информации, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в такие помещения.

3.11 Организация доступа работников Учреждения к защищаемой информации в соответствии с возложенными на них служебными обязанностями.

3.12 Разработка и внедрение локальных актов, определяющих перечень работников Учреждения, имеющих доступ к защищаемой информации.

3.13 Контроль размещения устройств ввода (отображения) информации, исключающего ее несанкционированный просмотр.

3.14 Обеспечение соответствия проводимых работ по защите информации технике безопасности, правилам и нормам охраны труда.

3.15 Проведение оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства по защите персональных данных.

3.16 Участие в разработке и применение политики по работе с инцидентами информационной безопасности.

3.17 Актуализация внутренней организационно-распорядительной документации по защите информации при изменении существующих и выходе новых нормативных правовых документов по защите информации.

4 Права

Ответственный за организацию защиты информации имеет следующие права.

4.1 Осуществлять контроль за деятельностью структурных подразделений Учреждения по выполнению ими требований по защите информации.

4.2 Составлять акты, докладные записки, отчёты для рассмотрения руководством Учреждения, при выявлении нарушений порядка обработки защищаемой информации.

4.3 Принимать необходимые меры при обнаружении несанкционированного доступа к защищаемой информации, как работниками Учреждения, так и третьими лицами, и докладывать о принятых мерах директору с предоставлением информации о субъектах, нарушивших режим доступа.

4.4 Вносить на рассмотрение директора предложения, акты, заключения о приостановлении работ в случае обнаружения каналов утечки (или предпосылок к утечке) информации ограниченного доступа.

4.5 Давать структурным подразделениям Учреждения, а также отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного.

4.6 Запрашивать и получать от всех структурных подразделений Учреждения сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного.

4.7 Составлять акты и другую техническую документацию о степени защищенности объектов информатизации.

4.8 Готовить и вносить предложения на проведение работ по защите информации; о привлечении к проведению работ по оценке эффективности защиты информации на объектах Учреждения (на договорной основе) учреждений и организаций, имеющих лицензию на соответствующий вид деятельности; о закупке необходимых технических средств защиты и другой спецтехники, имеющих в обязательном порядке сертификат соответствия.

4.9 Осуществлять визирование договоров с контрагентами с целью правового обеспечения передачи им защищаемой информации Учреждения в ходе выполнения работ по этим договорам.

4.10 Представлять интересы Учреждения при осуществлении государственного контроля и надзора за обработкой персональных данных Уполномоченным органом по защите прав субъектов персональных данных.

5 Взаимодействия (служебные связи)

5.1 Ответственный выполняет свои задачи осуществляя взаимодействие со всеми структурными подразделениями Учреждения.

5.2 Для выполнения своих функций и реализации предоставленных прав Ответственный взаимодействует с территориальными и региональными подразделениями Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, ФСТЭК России, ФСБ России, МВД России, другими представителями исполнительной власти и организациями, предоставляющими услуги и выполняющими работы в области защиты информации на законном основании.

6 Ответственность

6.1 Ответственный за организацию защиты информации несет ответственность за надлежащее и своевременное выполнение возложенных задач и функций по организации защиты информации Учреждения в соответствии с положениями законодательства Российской Федерации.

Начальник отдела автоматизации



О. А. Просвирина