Экз. № 1

АКТ

проверки выполнения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием криптографических средств в ГБПОУ РО «Шахтинский медицинский колледж им. Г.В. Кузнецовой»

«19» апреля 2017 г. г. Шахты

Комиссией УФСБ России по Ростовской области в составе: ст. оперуполномоченного Кубата Е.С., офицера Резникова В.В. на основании распоряжения УФСБ России по Ростовской области № 115/Ш/1-3791 от 13 апреля 2017 г. о проведении внеплановой выездной проверки юридического лица 19 апреля 2017 г. проведена внеплановая выездная проверка выполнения организационных и технических мер по обеспечению безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных с использованием криптографических средств (далее – контроль за обеспечением безопасности ПДн) в ГБПОУ РО «Шахтинский медицинский колледж им. Г.В. Кузнецовой» (далее – Учреждение).

Контроль за обеспечением безопасности ПДн проводился на основании следующих нормативно-правовых актов, регламентирующих вопросы безопасности персональных данных в Российской Федерации:

1. Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (далее – Федеральный закон);

2. «Требований к защите персональных данных при их обработке в информационных система персональных данных», утвержденных постановлением Правительства Российской Федерации от 1 октября 2012 г. № 1119 (далее – Требования);

3. «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных с использованием СКЗИ, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утвержденных Приказом ФСБ России от 10 июля 2014 г. № 378, зарегистрированного в Министерстве юстиции Российской Федерации за

регистрационным № 33620 от 18 августа 2014 г. (далее – Состав и содержание организационных и технических мер);

4. «Положения о разработке производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденного Приказом ФСБ России от 9 февраля 2005 г. № 66, зарегистрированным в Министерстве юстиции Российской Федерации за регистрационным № 6382 от 3 апреля 2005 г. (далее – ПКЗ-2005);

5. «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной Приказом ФАПСИ от 13 июня 2001 г. № 152, зарегистрированным в Министерстве юстиции Российской Федерации за регистрационным № 2848 от 6 августа 2001 г. (далее – Инструкция).

Контроль за обеспечением безопасности ПДн со стороны ФСБ России в Учреждении ранее не проводился. В соответствии с Федеральным законом контроль за обеспечением безопасности ПДн осуществлялся без ознакомления с ПДн, обрабатываемыми в информационных системах персональных данных (далее – ИСПДн).

Проверкой установлено:

Учреждение является оператором, осуществляющим обработку персональных данных, зарегистрированным в Реестре Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за № 09-0076873 от 23 декабря 2009 г. В рамках обеспечения своей деятельности в Учреждении эксплуатируются следующие государственные информационные системы, в которых обрабатываются с использованием криптографических средств ПДн:

1. ИСПДн ГБПОУ РО «ШМК»: обрабатываются ПДн менее 100000 субъектов ПДн – преподавателей и обучающихся Учреждения.

2. ИСПДн «Бухгалтерия»: обрабатываются ПДн менее 100000 субъектов ПДн – преподавателей и обучающихся Учреждения.

Обработка персональных данных в ИСПДн ГБПОУ РО «ШМК» в системе ФИС «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» (далее – ФИС ФРДО) осуществляется с использованием сети «Интернет». Для защиты персональных данных абитуриентов в ИСПДн, передаваемых Учреждением в ФГБУ «Федеральный центр тестирования» по открытым каналам связи, используются средства криптографической защиты информации (далее – СКЗИ) ПАК «ViPNet Terminal» (сертификат ФСБ России от 06 ноября 2012 г. № СФ/124-1996).

Для защиты персональных данных в ИСПДн «Бухгалтерия», передаваемых учреждением по открытым каналам связи, Учреждением применяются следующие СКЗИ:

– в системе подачи электронной налоговой, пенсионной и статистической отчетности «ViPNet ЭДО Отчет» – СКЗИ «КриптоПро CSP 4.0», имеющее действующий сертификат соответствия ФСБ России от 30.12.2016 № СФ/114-3009. Услуги защищенного документооборота с контролирующими органами предоставляет ООО «ИнфоТеКС Интернет Траст» по контракту от 21 ноября 2016 г. № 24-264233;

– в АЦК «Финансы и планирование» ПО «ViPNet Client» версии 4.3 – СКЗИ «КриптоПро CSP3.9», имеющее действующий сертификат соответствия ФСБ России от 30.12.2016 № СФ/124-3011;

– в системе «Сбербанк Бизнес Онлайн» – СКЗИ «Бикрипт 4.0», имеющее действующий сертификат соответствия ФСБ России от 30.11.2015 № СФ/113-2763.

ИСПДн и СКЗИ Учреждения размещены в помещениях по адресу: г. Шахты, ул. Шевченко, д. 157. Все помещения оборудованы охранной сигнализацией, извещатели которой выведены на пульт централизованной охраны здания. Круглосуточную охрану здания осуществляют сотрудники Управления.

В ходе проверки выявлены нарушения обязательных требований нормативных правовых актов:

1. В нарушение ч. 3 ст. 19 Федерального закона «О персональных данных» от 27 июля 2006 г. № 152 (далее – Федеральный закон) для защиты персональных

данных в Учреждении применяется СКЗИ ПАК «ViPNet Terminal», не прошедшее в установленном порядке процедуру оценки соответствия средств защиты информации (срок действия сертификата соответствия требованиям ФСБ России к шифровальным (криптографическим) средствам от 06 ноября 2012 г. № СФ/124-1996 истек 06 ноября 2015 г.)

2. В нарушение ч. 1 п. 2 ст. 19 Федерального закона, Учреждением не определены угрозы безопасности персональных данных, характерных для ИСПДн.

3. В нарушение ч. 5 п. 2 ст. 19 Федерального закона, поэкземплярный учет машинных носителей персональных данных в Учреждении не осуществляется.

4. В нарушение п. 26 Инструкции и п. 48 ПКЗ-2005, поэкземплярный учет СКЗИ, ключевой информации, эксплуатационной и технической документации к ним в Учреждении не организован.

Вывод: в ГБПОУ РО «Шахтинский медицинский колледж им. Г.В. Кузнецовой» имеются нарушения в выполнении организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием шифровальных (криптографических) средств.

Рекомендации:

1. Исключить использование, для защиты ПДн, СКЗИ ПАК «ViPNet Terminal» с истекшим сроком действия сертификата соответствия требованиям ФСБ России к шифровальным (криптографическим) средствам. Для защиты ПДн применять СКЗИ, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

2. В порядке, предусмотренном Требованиями определить угрозы, характерные для эксплуатируемых в Учреждении ИСПДн, и уровни защищенности, которые необходимо обеспечить при построении системы защиты ПДн.

3. Организовать поэкземплярный учет машинных носителей персональных данных, путем заведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров.

4. В порядке, предусмотренном п. 26 Инструкции, произвести поэкземплярный учет криптоключей, используемых для работы СКЗИ.

О выполнении рекомендаций сообщить в УФСБ России по Ростовской области не позднее 19 июля 2017 г.

Проверку провели: Е.С. Кубата

В.В. Резников

При проверке присутствовал:
Инженер-программист
ГБПОУ РО «Шахтинский медицинский колледж им. Г.В. Кузнецовой» В.В. Семенов

С актом ознакомлена:
Директор ГБПОУ РО «Шахтинский медицинский колледж им. Г.В. Кузнецовой» Н.Ф. Никулина

«19» апреля 2017 г.

Министерство здравоохранения Ростовской области
государственное бюджетное профессиональное образовательное учреждение Ростовской области
«Шахтинский медицинский колледж им. Г.В. Кузнецовой»
(ГБПОУ РО «ШМК»)
346500, Ростовская область, г.Шахты, ул. Шевченко, 157
тел/факс (8636) 22-69-27
e-mail: shmu55@bk.ru
19 апреля 2017 г.
№ 246