ПРОТОКОЛ
заседания Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе – Югре
№ 1/17

г. Ханты-Мансийск 8 февраля 2017 года

ПРЕДСЕДАТЕЛЬСТВОВАЛ
Руководитель Аппарата Губернатора – заместитель Губернатора Ханты-Мансийского автономного округа – Югры, председатель Совета Белоножкина Ольга Игоревна

В заседании Совета по технической защите информации приняли участие должностные лица, определенные постановлением Губернатора Ханты-Мансийского автономного округа – Югры от 29 апреля 2011 года № 59.

1. О результатах контроля (мониторинга) и анализа эффективности деятельности по вопросам обеспечения безопасности информации ограниченного доступа в исполнительных органах государственной власти (органах местного самоуправления) автономного округа и мерах по совершенствованию системы защиты информации в государственных (муниципальных) информационных системах.

(Тумаев М.А.)

РЕШИЛИ:

1.1. Информацию Тумаева М.А. принять к сведению.

1.2. Управлению защиты информации и специальной документальной связи Аппарата Губернатора автономного округа:

1.2.1. Подготовить и направить в адрес исполнительных органов государственной власти (далее – ИОГВ) и органов местного самоуправления (далее – ОМСУ) Ханты-Мансийского автономного округа – Югры (далее – автономный округ) состав недостатков, выявленных в ходе анализа отчетных материалов, представленных ИОГВ и ОМСУ по результатам деятельности по защите информации за 2016 год.

Провести внутренний аудит состояния готовности ИОГВ к контрольным мероприятиям Управления ФСТЭК России по УрФО.

Срок: до 10.03.2017

1.2.2. Разработать совместно с Депинформтехнологий Югры предложения по совершенствованию информационной безопасности Территориальной информационной системы автономного округа (ТИС Югры) путем внедрения (модернизации) систем: защиты от вредоносных программ и вирусов, обнаружения вторжений (предотвращения компьютерных атак), управления событиями безопасности, антиспам, контент-фильтрации;

1.2.3. Разработать проект «Соглашения об информационном взаимодействии с 6-м отделением Центра специальной связи и информации ФСО России в Тюменской области».

Срок: до 01.05.2017

1.2.4. Организовать оказание информационно-методической помощи руководству государственных и муниципальных учреждений автономного округа по реализации пункта 1.3.1. настоящего протокола.

Срок: до 15.12.2017.

1.3. Руководителям исполнительных органов государственной власти, Главам городских округов и муниципальных районов автономного округа:

1.3.1. Поручить руководителям подведомственных государственных и муниципальных учреждений автономного округа (далее – учреждения):

1.3.1.1. Обеспечить выполнение требований следующих нормативных правовых актов:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

- постановления Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление № 1119);

- постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (далее – Постановление № 211);

- приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Приказ № 17);

- постановления Губернатора автономного округа от 17.07.2003 № 151 «О системе технической защиты информации» (далее – Постановление № 151).

1.3.1.2. Назначить из числа заместителей руководителя учреждения должностное лицо, ответственное за руководство работами по защите информации в учреждении *(согласно п. 19 постановления № 151)*.

Включить данную функцию в его должностной регламент;

1.3.1.3. Создать в учреждении структурное подразделение (назначить специалистов из числа штатных работников) по технической защите информации (далее – ТЗИ). Возложить на подразделение (специалистов из числа штатных работников) функцию по реализации мероприятий в области ТЗИ, в т.ч. за организацию обработки персональных данных в учреждении *(согласно пункта 1 части 1 статьи 18.1. Федерального закона № 152-ФЗ, постановления № 211, п. 19 постановления № 151)*;

1.3.1.4. Сформировать коллегиальный орган, осуществляющий координацию деятельности структурных подразделений учреждения по вопросам обеспечения безопасности информации – Постоянно действующую техническую комиссию по защите информации *(согласно п. 19 постановления № 151)*;

1.3.1.5. Подчинить заместителю руководителя учреждения, ответственному за руководство работами по ТЗИ, подразделение (специалистов из числа штатных работников) по ТЗИ и постоянно действующую техническую комиссию по защите информации учреждения;

1.3.1.6. Организовать обучение (повышение квалификации) должностных лиц, указанных в пунктах 1.3.1.2 и 1.3.1.3 настоящего протокола по учебным программам, согласованным со ФСТЭК России;

1.3.1.7. Определить уровень защищенности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) *(согласно п. 8 Постановления № 1119)*;

1.3.1.8. Провести оценку эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн с составлением заключения о работоспособности применяемых средств защиты информации *(согласно пп. 4 п. 2 ст. 19 ФЗ-152)*;

1.3.1.9. Классифицировать автоматизированные системы, обрабатывающие информацию с пометкой «Для служебного пользования» и провести мероприятия по их защите согласно «Специальным требованиям и рекомендациям по защите конфиденциальной информации» утвержденным приказом Гостехкомиссии России от 30.08.2002 № 282;

1.3.1.10. Определить актуальные угрозы безопасности ПДн, на их основе разработать модель угроз безопасности ПДн;

1.3.1.11. Организовать учет машинных носителей, содержащих ПДн *(согласно п. 5 части 2 ст. 19 ФЗ-152 обеспечение безопасности ПДн достигается в том числе учетом машинных носителей ПДн)*;

1.3.1.12. Разработать подсистему защиты ИСПДн, предусматривающую применение организационных и технических мер (с учетом актуальных угроз безопасности ПДн) по обеспечению безопасности ПДн в ИСПДн *(создание системы защиты ИСПДн регламентировано п. 2 части 2 ст. 19 ФЗ-152 и п. 2 Постановления № 1119.*

1.3.1.13. Организовать периодический контроль за выполнением требований к защите ПДн при их обработке в ИСПДн *(согласно п. 17 Постановления № 1119 контроль организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации)*;

1.3.1.14. Разработать порядок резервирования баз данных ИСПДн *(согласно п. 7 части 2 ст. 19 ФЗ-152 обеспечение безопасности ПДн достигается в том числе восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним)*;

1.3.1.15. Разработать порядок ведения электронных журналов аудита обращений сотрудников к ПДн *(согласно п. 8 части 2 ст. 19 ФЗ-152 обеспечение безопасности ПДн достигается, в частности обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн)*;

1.3.1.16. Разработать и утвердить в установленном порядке организационно-распорядительные документы, предусмотренные Постановлением № 211;

1.3.1.17. Организовать контроль (анализ) защищенности государственных информационных систем (далее – ГИС), муниципальных информационных систем (далее – МИС) в т.ч. тестирование их подсистемы защиты информации;

1.3.1.18. Провести классификацию ГИС (МИС) по требованиям защиты информации *(согласно п. 14.2. Приказа № 17)*;

1.3.1.19. Использовать сертифицированные средства защиты информации (средства обнаружения вторжений, межсетевого экранирования, средства защиты виртуальной инфраструктуры, средства защиты от несанкционированного доступа);

1.3.1.20. Исключить подключение к ГИС (МИС) внешних 3G/4G usb-модемов, с целью организации доступа к сети «Интернет»;

1.3.1.21. Провести аттестацию ГИС (МИС) по требованиям защиты информации *(аттестация ГИС (МИС) предусматривает проведение комплекса организационных и технических мероприятий (аттестационных испытаний) в результате которых подтверждается соответствие системы защиты ГИС требованиям Приказа № 17)*;

1.3.1.22. Обеспечить согласование с Управлением защиты информации и специальной документальной связи Аппарата Губернатора автономного округа документации о закупках товаров, работ, услуг по созданию систем защиты информации и (или) поставку отдельных их элементов;

1.3.1.23. Обеспечить конфиденциальное делопроизводство (оборот документов с пометкой «Для служебного пользования» в соответствии с разделом XI «Инструкции по делопроизводству в государственных органах Ханты-Мансийского автономного округа – Югры и исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры», утвержденной постановлением Губернатора автономного округа от 30.1.2012 № 176 и (или) муниципальными нормативными документами (ведомственными инструкциями), разработанными с учетом требований вышеуказанного постановления;

1.3.1.24. Обеспечить работу со средствами криптографической защиты информации в соответствии с требованиями формуляров и специальных документов по их эксплуатации;

1.3.1.25. Учитывать при проведении работ по совершенствованию системы защиты информации, циркулирующей в информационных системах общего пользования, базу данных уязвимостей информационных систем, представленных в банке данных угроз безопасности информации ФСТЭК России (адрес: www.bdu.fstec.ru);

1.3.1.26. Принять к сведению и руководству в работе (в части касающейся) решение Совета по вопросам ТЗИ автономного округа (пункты 1.3.1.-1.3.3. протокола заседания от 21.12.2016 № 3/16).

Срок: до 15.12.2017.

1.3.2. Заслушать руководителей подведомственных учреждений по результатам практической реализации ими пункта 1.3.1. настоящего протокола на итоговом заседании ПДТК по защите информации в ИОГВ (ПДТК по защите государственной тайны в ОМС).

Срок: до 30.12.2017.

1.3.3. Направить в Управление защиты информации и специальной документальной связи Аппарата Губернатора автономного округа информационную справку о результатах реализации в подведомственных учреждениях пункта 1.3.1. настоящего протокола (отдельно за каждое учреждение).

Срок: до 01.02.2018.

2. О реализации на территории Ханты-Мансийского автономного округа – Югры требований постановления Правительства Российской Федерации от 29.08.2001 № 633 «О порядке размещения и использования на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации иностранных технических средств наблюдения и контроля».

(Поляков И.В.)

РЕШИЛИ:

2.1. Информацию Полякова И.В. принять к сведению.

2.2. Руководителям исполнительных органов государственной власти, Главам городских округов и муниципальных районов автономного округа, руководителям государственных и муниципальных учреждений:

2.2.1. При заключении (планировании заключения) международных договоров и соглашений, предметом которых является поставка технических средств иностранного производства, в обязательном порядке учитывать требования постановления Правительства Российской Федерации от 29.08.2001 № 633 «О порядке размещения и использования на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации иностранных технических средств наблюдения и контроля»;

2.2.2. Провести анализ заключенных (планируемых к заключению) международных договоров и соглашений, предметом которых является поставка технических средств иностранного производства;

2.2.3. Информацию о наличии (отсутствии) иностранных технических средств наблюдения и контроля направить в Управление защиты информации и специальной документальной связи Аппарата Губернатора автономного округа.

Срок: до 10.12.2017

3. О согласовании мероприятий по технической защите информации, реализуемых в 2017 году.

(Чиликов А.Ю.)

РЕШИЛИ:

3.1. Информацию Чиликова А.Ю. принять к сведению.

3.2. Управлению защиты информации и специальной документальной связи Аппарата Губернатора автономного округа организовать проведение следующих мероприятия по технической защите информации:

3.2.1. Оказание услуг цифровой АТС «Hicom» и правительственной междугородной связи.

Сроки: разработка и согласование ТЗ – до 15.02.2017
выполнение работ по гос.контракту – до 31.12.2017

3.2.2. Техническое обслуживание систем безопасности и защиты информации Аппарата Губернатора автономного округа.

Сроки: разработка и согласование ТЗ – до 20.02.2017
выполнение работ по гос.контракту – до 31.12.2017

3.2.3. Выполнение работ по защите информации ограниченного доступа с поставкой защищенных абонентских пунктов.

Сроки: разработка и согласование ТЗ – до 15.03.2017
выполнение работ по гос.контракту – до 10.08.2017

3.2.4. Выполнение работ по защите объектов информатизации Аппарата Губернатора автономного округа в соответствии с требованиями по безопасности конфиденциальной информации.

Сроки: разработка и согласование ТЗ – до 20.03.2017
выполнение работ по гос.контракту – до 10.08.2017

3.2.5. Выполнение работ по оборудованию и аттестации зала конфиденциальных совещаний и КВС.

Сроки: разработка технического задания – до 15.04.2017
выполнение работ по гос.контракту – до 31.12.2017

3.2.6. Выполнение работ по специальной проверке технических средств, установленных в выделенных помещениях здания Дома Правительства автономного округа.

Сроки: разработка технического задания – до 1.05.2017
выполнение работ по гос.контракту – до 10.08.2017

Руководитель Аппарата Губернатора –
заместитель Губернатора Ханты-Мансийского
автономного округа – Югры,
председатель Совета О.И.Белоножкина

Секретарь Совета М.А.Тумаев