ПРОТОКОЛ
заседания Совета по вопросам технической защиты информации
в Ханты-Мансийском автономном округе – Югре
№ 3/15

г. Ханты-Мансийск 16 декабря 2015 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.

Дополнительно на заседание приглашен исполняющий обязанности заместителя начальника Управления ФСТЭК России по Уральскому федеральному округу Клюкин Андрей Анатольевич.

1. О состоянии системы технической защиты информации Уральского федерального округа, способах и методах её совершенствования, в том числе обеспечении защиты информации в государственных информационных системах.

(Клюкин А.А.)

РЕШИЛИ:

1.1. Информацию Клюкина А.А. принять к сведению.

1.2. Руководителям исполнительных органов государственной власти автономного округа (далее – ИОГВ) и исполнительно-распорядительных органов местного самоуправления городских округов и муниципальных районов автономного округа (далее – ОМСУ):

1.2.1. Обеспечить выполнение требований следующих нормативных правовых актов:

- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – ФЗ-152);

- постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление № 1119);

- приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Приказ № 17);

- постановления Губернатора Ханты-Мансийского автономного округа – Югры от 11 декабря 2015 года № 162 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в

исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры» (далее – Постановление № 162).

1.2.2. Определить уровень защищенности персональных данных при их обработке в информационных системах персональных данных *(согласно п. 8 Постановления № 1119)*;

1.2.3. Провести классификацию государственных информационных систем по требованиям защиты информации *(согласно п. 14.2. Приказа № 17)*;

1.2.4. Определить актуальные угрозы безопасности персональных данных (далее – ПДн), на их основе разработать модель угроз безопасности ПДн (*согласно Постановлению № 162, а также «Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн)», утвержденных заместителем директора ФСТЭК России 14 февраля 2008 года*);

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

1.2.6. Разработать систему защиты ИСПДн, предусматривающую применение организационных и технических мер по обеспечению безопасности персональных данных в ИСПДн *(создание системы защиты ИСПДн регламентировано п. 2 части 2 ст. 19 ФЗ-152 и п. 2 Постановления № 1119, согласно которым безопасность ПДн обеспечивается с помощью системы защиты ПДн, нейтрализующей актуальные угрозы. При этом система защиты ПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн)*;

1.2.7. Организовать периодический контроль за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных *(согласно требованиям 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)*;

1.2.8. 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)*;

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

1.2.10. Организовать контроль (анализ) защищенности государственных информационных систем (далее – ГИС), в т.ч. тестирование их системы защиты информации;

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

1.2.12. Исключить подключение к ГИС внешних 3G/4G usb-модемов с целью организации доступа к сети «Интернет»;

1.2.13. Разработать организационно-распорядительные документы, предусмотренные постановлением Правительства Российской Федерации от 21 марта 2012 года № 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»;

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

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

Сроки: пункт 1.2.1 – постоянно;

пункты 1.2.2-1.2.15 – до 1 ноября 2016 года.

1.3. Депинформтехнологий Югры, Управлению специальных мероприятий Аппарата Губернатора Ханты-Мансийского автономного округа – Югры оказать ответственным специалистам ИОГВ и ОМСУ необходимое содействие по реализации мероприятий, предусмотренных пунктом 1.2 настоящего протокола.

2. Об итогах выполнения мероприятий по технической защите информации, реализованных в 2015 году.

(Чиликов А.Ю.)

РЕШИЛИ:

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

2.2. Признать удовлетворительным выполнение мероприятий по технической защите информации, реализованных в 2015 году.

2.3. Руководителям исполнительных органов государственной власти автономного округа:

2.3.1. Организовать мероприятия по контролю состояния конфиденциального делопроизводства в Департаменте (Службе) в соответствии с п. 11.15 «Инструкции по делопроизводству в государственных органах Ханты-Мансийского автономного округа – Югры и исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры», утвержденной постановлением Губернатора Ханты-Мансийского автономного округа – Югры от 30 декабря 2012 года № 176;

2.3.2. Направить в Управление специальных мероприятий Аппарата Губернатора автономного округа копию акта проверки наличия и состояния конфиденциальных документов.

Срок – до 1.04.2016.

2.4. Руководителям исполнительно-распорядительных органов местного самоуправления городских округов и муниципальных районов автономного округа провести анализ эффективности функционирования системы технической защиты информации в администрациях муниципальных образований и организовать (при необходимости) выполнение следующих обязательных мероприятий:

2.4.1. Разработать положение о Системе технической защиты информации в администрации городского округа (муниципального района) на основе постановления Губернатора Ханты-Мансийского автономного округа – Югры от 17 июля 2003 года № 151 «О системе технической защиты информации в Ханты-Мансийском автономном округе – Югре»;

2.4.2. Назначить из числа заместителей главы администрации должностное лицо, ответственное за руководство работами по защите информации. Включить данную функцию в его должностной регламент. Подчинить вышеуказанному заместителю напрямую подразделение по технической защите информации (далее – ТЗИ) и постоянно действующую техническую комиссию по защите государственной тайны (далее – ПДТК);

2.4.3. Создать из числа муниципальных служащих (работников подведомственного муниципального учреждения), имеющих допуск к сведениям, составляющим государственную тайну, структурное подразделение (штатных специалистов) по технической защите информации;

Разработать положение о подразделении по ТЗИ в соответствии с требованиями «Типового положения о подразделении по защите информации…», одобренного решением Гостехкомиссии России от 14 марта 1995 года № 32;

Назначить из числа работников подразделения по ТЗИ двух администраторов безопасности для обеспечения требуемого технологического процесса обработки информации ограниченного доступа;

2.4.4. Организовать обучение (повышение квалификации) должностных лиц, указанных в пункте 2.4.1. и 2.4.2. настоящего протокола, по учебным программам, согласованным со ФСТЭК России;

2.4.5. Подразделению (штатным специалистам) по ТЗИ оказывать методическую помощь структурным подразделениям администрации и подведомственным учреждениям (в муниципальных районах – администрациям городских и сельских поселений, расположенных на территории районов) по вопросам обеспечения информационной безопасности;

2.4.6. 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 августа 2002 года № 282;

2.4.7. Провести дополнительный анализ и рассмотреть на заседании ПДТК вопрос об объектах ключевых систем информационной инфраструктуры (далее – КСИИ). При необходимости организовать работу по обеспечению безопасности информации в данных системах в соответствии с «Общими требованиями по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утвержденными заместителем директора ФСТЭК России 18 мая 2007 года;

2.4.8. Разработать постановление администрации «О порядке обращения с конфиденциальной информацией» на основе раздела 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 Ханты-Мансийского автономного округа – Югры от 30 декабря 2012 года № 176;

2.4.9. Разработать «План комплексных мероприятий по технической защите информации в органе местного самоуправления на 2016 год»;

2.4.10. Выполнить расчет бюджетных ассигнований, необходимых для выполнения работ по защите информации. Включить данные расходы отдельным разделом (подразделом) в состав муниципальной программы по развитию информатизации.

2.4.11. Информационную справку по результатам реализации пункта 2.4. настоящего протокола направить в Аппарат Губернатора Ханты-Мансийского автономного округа – Югры.

Срок – до 01.07.2016

2.5. Депинформтехнологий Югры совместно с Управлением специальных мероприятий Аппарата Губернатора автономного округа продолжить работу по созданию Центра защиты информации Ханты-Мансийского автономного округа – Югры на базе автономного учреждения Ханты-Мансийского автономного округа – Югры «Югорский научно-исследовательский институт информационных технологий».

Отв.: Торгашин Ю.И., Киселев М.А., срок – до 30.12.2016

3. О корректировке «Комплексного плана мероприятий по обеспечению информационной безопасности в органах государственной власти и органах местного самоуправления Ханты-Мансийского автономного округа – Югры на 2015-2020 годы».

(Чиликов А.Ю.)

РЕШИЛИ:

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

3.2. Утвердить предложения по корректировке «Комплексного плана мероприятий по обеспечению информационной безопасности в органах государственной власти и органах местного самоуправления Ханты-Мансийского автономного округа – Югры на 2015-2020 годы».

3.3. Депинформтехнологий Югры в целях безусловного выполнения решения Совета Безопасности Российской Федерации *(пункт 10.2 протокола от 1.10.2014)* внести в установленном порядке изменения в государственную программу «Информационное общество Ханты-Мансийского автономного округа – Югры на 2016 - 2020 годы», сформировав отдельное мероприятие по обеспечению информационной безопасности (защите информации) в исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры».

Отв.: Торгашин Ю.И., срок – до 1.07.2016

3.4. Управлению специальных мероприятий Аппарата Губернатора автономного округа на основании дополнительно представленных исполнительно-распорядительными органами местного самоуправления городских округов и муниципальных районов автономного округа предложений подготовить и внести на рассмотрение Совета по ТЗИ предложения по корректировке «Плана ОИБ».

Отв.: Чиликов А.Ю., срок – до 30.12.2016

4. Об утверждении «Плана комплексных мероприятий по технической защите информации в Аппарате Губернатора Ханты-Мансийского автономного округа – Югры на 2016 год».

(Киселев М.А.)

РЕШИЛИ:

4.1. Информацию Киселева М.А.принять к сведению.

4.2. Утвердить «План комплексных мероприятий по технической защите информации в Аппарате Губернатора Ханты-Мансийского автономного округа – Югры на 2016 год» (далее - «План ТЗИ-2016»).

4.3. Управлению специальных мероприятий Аппарата Губернатора автономного округа:

4.3.1. Организовать проведение комплексных мероприятий по технической защите информации в соответствии с утвержденным «Планом ТЗИ-2016».

Отв.: Чиликов А.Ю., срок – до 30.12.2016

4.3.2. Выписки из «Плана ТЗИ-2016» и настоящего протокола направить в исполнительные органы государственной власти и исполнительно-распорядительные органы местного самоуправления городских округов и муниципальных районов автономного округа (в части, касающейся).

Отв.: Чиликов А.Ю., срок – до 30.12.2015

4.4. Руководителям исполнительных органов государственной власти автономного округа в соответствии с требованиями утвержденного Управлением ФСТЭК России по УрФО «Типового Руководства по защите

информации от иностранных технических разведок и от ее утечки по техническим каналам» разработать *(по ранее доведенной форме, исх. от 12.02.2014 от ВЕ-2350)* и направить в Аппарат Губернатора автономного округа (через Управление специальных мероприятий) копию утвержденного «Плана комплексных мероприятий по защите информации в исполнительном органе государственной власти на 2016 год».

Срок – до 15.02.2016

5. О выполнении решений, принятых на заседаниях Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе – Югре в 2015 году.

(Чиликов А.Ю.)

РЕШИЛИ:

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

Работу Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе – Югре в 2015 году признать удовлетворительной.

5.2. Считать исполненными поручения, предусмотренные решениями заседаний Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе – Югре:

- пункт 1.5 вопроса № 1 протокола от 30.04.2015 № 1/15;
- пункт 2.3 вопроса № 2 протокола от 30.04.2015 № 1/15;
- пункт 3.3 вопроса № 3 протокола от 30.04.2015 № 1/15;
- пункт 1.3 вопроса № 1 протокола от 17.07.2015 № 2/15;
- пункт 3.2 вопроса № 3 протокола от 17.07.2015 № 2/15.

5.3. Отметить не исполненным в полном объеме исполнительно-распорядительными органами местного самоуправления:

- гг. Нягань, Урай и Октябрьского района - пункт 5.3.1 протокола от 30 апреля 2015 года № 1/15 *(не представлены сведения о внесении раздела по информационной безопасности в муниципальную программу развития информатизации)*;

- г. Когалым и Березовского района - пункт 5.3.2 протокола от 30 апреля 2015 года № 1/15 (*не предусмотрено финансовое обеспечение планируемых мероприятий по защите муниципальных информационных систем на период 2015-2020 годов)*;

- г. Нефтеюганск, Белоярского района и Нижневартовского района - пункт 5.3.3 протокола от 30 апреля 2015 года № 1/15 *(не разработан комплекс дополнительных мер по совершенствованию информационной безопасности в администрации муниципального образования на период 2016-2020 годов).*

5.4. В целях безусловной реализации решений Совета Безопасности Российской Федерации *(пункта 10.2 протокола от 1.10.2014)* и Совета при полномочном представителе Президента Российской Федерации в УрФО *(п.п. 1.1 п. 1 протокола от 6.10.2014 №2):*

продлить до 01.07.2016 сроки исполнения вышеуказанными исполнительно-распорядительными органами местного самоуправления пунктов 5.3.1, 5.3.2., 5.3.3. протокола от 30 апреля 2015 года № 1/15.

5.5. Рекомендовать руководителям исполнительно-распорядительных органов местного самоуправления гг. Нягань, Урай, Когалым, Нефтеюганск, Октябрьского района, Березовского района, Белоярского района и Нижневартовского района причины неисполнения протокольных решений Совета по ТЗИ рассмотреть на заседании ПДТК муниципального образования.

6. Об утверждении «Плана работы Совета по вопросам технической защиты информации на 2016 год».

(Киселев М.А.)

РЕШИЛИ:

6.1. Информацию Киселева М.А. принять к сведению.

6.2. Утвердить «План работы Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе – Югре на 2016 год».

6.3. Организовать подготовку и проведение заседаний Совета в соответствии с утвержденным Планом.

Отв.: Чиликов А.Ю., срок – до 30.12.2016

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

Секретарь Совета А.Ю.Чиликов

Начальник Управления специальных мероприятий
Аппарата Губернатора автономного округа,
заместитель председателя Совета М.А.Киселев