ПРОТОКОЛ
заседания Совета по вопросам технической защиты информации
в Ханты-Мансийском автономном округе - Югре
№ 3/16

г. Ханты-Мансийск 21 декабря 2016 года

ПРЕДСЕДАТЕЛЬСТВОВАЛ

Заместитель руководителя Аппарата Губернатора
Ханты-Мансийского автономного округа - Югры, заместитель
председателя Совета
Киселев Максим Александрович

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. Об итогах выполнения мероприятий по технической защите информации, реализованных в 2016 году.

(Тумаев М.А.)

РЕШИЛИ:

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

1.2. Управлению защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа - Югры (далее - автономный округ):

1.2.1. Организовать проведение обучающего семинара: «Обеспечение безопасности информации в органах государственной власти и местного самоуправления. Проблемы и решения». Привлечь для участия на данном семинаре ответственных представителей исполнительных органов государственной власти автономного округа, подведомственных им учреждений, а также органов местного самоуправления муниципальных образований автономного округа;

1.2.2. Разработать «Типовой порядок выявления и реагирования на инциденты информационной безопасности, способные привести к сбоям или нарушению функционирования информационных систем и (или) возникновению угроз безопасности конфиденциальной информации».

Отв. Чиликов А.Ю., Тумаев М.А. Срок: до 01.05.2017.

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

1.3.1. Принять к сведению, что в период с 4 по 8 сентября 2017 года Управлением ФСТЭК России по Уральскому федеральному округу будет

проведена проверка исполнительных органов государственной власти (далее - ИОГВ) и органов местного самоуправления автономного округа (далее - ОМСУ, МО) по вопросам организации работ в области технической защиты информации (далее - ТЗИ, проверка).

1.3.2. Обеспечить в вышеуказанный период нахождение на рабочих местах должностных лиц, осуществляющих руководство и организацию работ по ТЗИ.

1.3.3. Учесть при планировании работ по ТЗИ на 2017 год следующий состав вопросов, подлежащих проверке:

- наличие должностных лиц, назначенных ответственными за руководство работами по ТЗИ (из числа заместителей руководителя ИОГВ (Главы МО)), а также за реализацию мероприятий по ТЗИ (из числа штатных работников ИОГВ (ОМСУ)), включение в их должностные регламенты функций и задач по ТЗИ;

- наличие структурного подразделения (штатных специалистов) по ТЗИ (штатная численность, укомплектованность, оснащенность техническими средствами контроля, уровень подготовки специалистов);

- подчинение подразделения (штатного специалиста) по ТЗИ заместителю руководителя ИОГВ (Главы МО), ответственному за руководство работами по ТЗИ, а также наделение данного подразделения (штатного специалиста) полномочиями по контролю состояния ТЗИ во всех структурных подразделениях ИОГВ (ОМСУ);

- наличие постоянно действующей комиссии по защите информации (далее - ПДТК), председателем которой является заместитель руководителя ИОГВ, ответственный за руководство работами по ТЗИ;

- наличие «Плана работы ПДТК», полнота его исполнения, протоколы и решения по вопросам ТЗИ;

- наличие и достаточность в ИОГВ (ОМСУ) руководящих и нормативно-методических документов по ТЗИ;

- наличие «Руководства по ТЗИ в ИОГВ (ОМСУ)»;

- структура системы защиты информации в ИОГВ (ОМСУ);

- наличие «Плана работ по ТЗИ в ИОГВ (ОМСУ)»;

- перечень аттестованных по требованиям безопасности информации объектов информатизации (наименование, категория, класс, номер аттестата соответствия, даты действия аттестата, сведения об органе по аттестации, выполнившего работы, реквизиты приказа о вводе объектов в эксплуатацию);

- перечень используемых средств защиты информации (наименование объекта информатизации, наименование средства защиты информации, серийный номер, даты действия сертификатов соответствия);

- порядок учета, использования и хранения машинных носителей конфиденциальной информации;

- организация работы в международных информационных сетях, в том числе в сети «Интернет»;

- принадлежность информационных систем ИОГВ (ОМСУ) к системам обработки персональных данных (далее - ПДн);

- регистрация ИОГВ (ОМСУ) в Реестре операторов обработки персональных данных, наличие уведомления в Роскомнадзор о начале обработки персональных данных;

- характеристика информационных систем, участвующих в обработке персональных данных (далее - ИСПДн), совокупность используемых баз данных, информационных технологий и технических средств, территориальная распределенность, внешние источники и потребители обрабатываемой информации, особенности физической и логической топологии;

- наличие акта классификации ИСПДн, правильность присвоения соответствующего класса (или наличие документа, устанавливающего уровень защищенности ПДн в ИСПДн);

- наличие модели угроз безопасности ПДн, оценка полноты и правильности определения угроз безопасности;

- размещение ИСПДн с учетом выполнения требований по сохранности носителей ПДн и средств защиты информации, а также исключения возможности проникновения и неконтролируемого пребывания посторонних лиц;

- состав организационно-распорядительных документов, регламентирующих деятельность ИОГВ (ОМСУ) по вопросам ТЗИ;

- наличие документа, определяющего порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в информационных системах;

- наличие электронного журнала обращений пользователей информационной системы к ПДн, выполнение требований по его периодической проверке, порядок рассмотрения нарушений правил доступа;

- содержание мероприятий по защите информации при установке, настройке, отладке, эксплуатации элементов информационной системы;

- организация работ по привлечению сторонних организаций для формирования и сопровождения баз данных и информационного взаимодействия (центров обработки информации), выполняющих функции операторов и администраторов системы централизованной обработки данных;

- порядок представления ПДн органам государственной власти, физическим и юридическим лицам;

- периодичность и порядок резервирования обрабатываемой информации;

- организация учета и использования магнитных, оптических и других машинных носителей информации;

- организация учета применяемых средств защиты информации;

- результаты обучения (инструктажа) лиц, эксплуатирующих средства защиты информации;

- порядок доступа пользователей к информационным ресурсам (наличие утвержденного списка сотрудников, допущенных к обработке ПДн, организация регистрации доступа пользователей);

-мероприятия по защите информации от несанкционированного доступа (далее - НСД), правильность установки и порядок эксплуатации средств защиты от НСД к информации, наличие на них сертификатов соответствия требованиям по безопасности информации, анализ

достаточности мер, исключающих бесконтрольный доступ к защищаемой информации;

- обеспечение безопасности межсетевого взаимодействия (организация защиты ПДн, передаваемых по каналам связи);

- организация антивирусной защиты;

- обнаружение несанкционированных вторжений;

- порядок обеспечения неизменности технических и программных средств (исключение доступа к монтажу, портам, модемам, цорядок внесения изменений в телекоммуникационную схему, технические средства, программное обеспечение и средства защиты информации);

- реализация мероприятий по защите графической, видео- и буквенно-цифровой информации, содержащей ПДн от просмотра посторонними лицами;

- наличие документов, предусмотренных постановлением Правительства Российской Федерации от 21 марта 2012 года №211;

- ведение конфиденциального делопроизводства.

1.3.4. Сформировать и направить в Управление защиты информации и специальной документальной связи Аппарата Губернатора автономного округа Информационную справку о выполнении мероприятий в области ТЗИ по направлениям (вопросам), указанным в пункте 1.3.3 настоящего протокола.

Срок: до 01.07.2016

1.3.5. Обеспечить неукоснительное выполнение требований, следующих нормативных правовых актов:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- 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»;

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

- приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3.6. Организовать внутренний контроль соответствия обработки и защиты информации требованиям, установленным федеральным

законодательством и принятыми в соответствии с ним нормативным актам ИОГВ (ОМСУ).

Срок: постоянно

1.4. Департаменту здравоохранения автономного округа:

1.4.1. Обеспечить в Депздраве Югры, подведомственных ему учреждениях здравоохранения, а также в БУ «Медицинский информационно-аналитический центр» выполнение требований по безопасности информации обрабатываемой в следующих информационных системах:

WEB-портал, «Здравоохранение Югры», РИСТ ХМАО, ПК «Здравоохранение», МИС «ПАЦИЕНТ», МИС «ЮГРА», «МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА» (МИС), ИС «МедВедь», РИР «Медицина», РИС «К врачу.ру», региональный сегмент «Единая государственная информационная система в сфере здравоохранения», «ЕИС ОМС», МИС «ОКБ» (состоящую из следующих подсистем: «Стационар»; «Поликлиника»; «Перинатальный центр»; «Лаборатория»; «Диагностика»; «Аптека»), МИС «СПК», ИСПДн «Здравоохранение», ИСПДн «Бухгалтерия и кадры», мобильное приложение «Электронный кабинет пациента».

1.4.2. Организовать и выполнить мероприятия по аттестации информационных систем персональных данных согласно требованиям по безопасности информации:

ИСПДн «Здравоохранение»;

ИСПДн «Бухгалтерия и кадры» (ИСПДн необходимо разделить на 2 ИСПДн согласно части 3 статьи 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой).

Срок: до 25.08.2017

1.5. Департаменту образования и молодежной политики автономного округа обеспечить выполнение требований по безопасности информации, обрабатываемой в следующих информационных системах:

региональном сегменте федеральной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования ГИС «Государственная итоговая аттестация», ИСПДн «Электронный дневник», ИСПДн «Государственная поддержка студентов», ИСПДн «Бухгалтерский и кадровый учет», ИСПДн «Список детей

выезжающих на летний отдых», ИСПДн «Образование детей с ограниченными возможностями», ИСПДн «Обращение граждан», АИАС «Регион. Контингент», ИС по постановке в очередь и учету контингента образовательных организаций дошкольного образования, ИС по учету участников олимпиад.

Срок: до 25.08.2017

1.6. Департаменту социального развития автономного округа обеспечить выполнение требований по безопасности информации, обрабатываемой в следующих государственных информационных системах:

«Автоматизированная система обработки информации» (ППО АСОИ), автоматизированной информационной системе «Государственный банк данных о детях, оставшихся без попечения родителей» (АИСТ), государственной информационной системе персональных данных «ГИС РППСУ».

Срок: до 25.08.2017

1.7. Департаменту финансов автономного округа обеспечить выполнение требований по безопасности информации, обрабатываемой в следующих информационных системах:

ИСПДн «Управление персоналом», ИСПДн «Парус», АС планирования, бухгалтерского учета и анализа исполнения бюджетов в финансовых органах «Бюджет», ПК «Автоматизированное рабочее место клиента Банка России», СКАД «Сигнатура», ПК «Отчетность субъекта РФ для Министерства финансов и Федерального казначейства РФ и формирование консолидированного бюджета субъекта РФ», защищенная телекоммуникационная система «Контур-Экстерн», ПК серии Аналитик «ИНЭК-Холдинг», «Скиф-Бюджетный процесс», ПК «Муниципальные образования», ПК «Колибри.УФК», ПП «Перечень объектов недвижимого имущества для целей налогообложения», АС «Бюджет поселения», УРМ АС «Бюджет», АС «Финансово-экономический анализ», «СКИФЗ» (программа создания и корректировки информационного фонда), ПП «ПАРУС-Бухгалтерия», 1111 «ПАРУС-Зарплата», «Контур-Экстерн».

Срок: до 25.08.2017

1.8. Службе по контролю и надзору в сфере образования автономного округа:

1.8.1. Организовать и выполнить мероприятия по аттестации информационных систем персональных данных согласно требованиям по безопасности информации:

«Кодекс: Кадры», «1С: Предприятие», «АС УРМ Бюджет», «Казначейство», «Госуслуги».

1.8.2. Обеспечить выполнение требований по безопасности информации в соответствии с требованиями приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не

составляющей государственную тайну, содержащейся в государственных информационных системах» обрабатываемой в:

региональном сегменте Федеральной базы данных об апостилях, проставленных на документах государственного образца об образовании, об ученых степенях и ученых званиях;

государственная информационная система «Реестр организаций, осуществляющих образовательную деятельность по имеющим государственную аккредитацию образовательным программам»;

государственная информационная система «Сводный реестр лицензий на осуществление образовательной деятельности»;

государственная автоматизированная информационная система «Управление»;

региональном сегменте Федеральной информационной системы «Единый реестр проверок».

Срок: до 25.08.2017

1.9. Департаменту информационных технологий автономного округа:

1.9.1. Обеспечить выполнение требований по безопасности информации обрабатываемой в аттестованных согласно требованиям по безопасности информации информационных системах

ИСПДн «Кодекс: Управление персоналом», ИСПДн «Бухгалтерский учет», ГИС «КД Югры»

1.9.2. Завершить мероприятия по внедрению системы защиты информации и аттестации ГИС «ТИС Югры», ГИС «СЭДД «Дело».

1.9.3. Организовать мероприятия по защите информации, обрабатываемых в информационных системах:

видеоконференцсвязи корпоративной сети органов государственной власти Ханты-Мансийского автономного округа - Югры;

IP-телефонии корпоративной сети органов государственной власти Ханты-Мансийского автономного округа - Югры.

Срок: до 25.08.2017

1.10. Департаменту труда и занятости населения автономного округа:

Организовать и выполнить мероприятия по аттестации информационных систем персональных данных согласно требованиям по безопасности информации:

ИСПДн «1С», ИСПДн «Кадры», ИСПДн «ПК Катарсис».

Срок: до 25.08.2017

2. Об утверждении «Плана комплексных мероприятий по технической защите информации в Аппарате Губернатора Ханты-Мансийского автономного округа - Югры на 2017 год»

(Чиликов А.Ю.)

РЕШИЛИ:

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

2.2. Утвердить «План комплексных мероприятий по технической защите информации в Аппарате Губернатора Ханты-Мансийского автономного округа - Югры на 2017 год» (далее - «План ТЗИ-2017»).

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

2.3.1. Организовать проведение комплексных мероприятий по технической защите информации в соответствии с утвержденным «Планом ТЗИ-2017».

Отв.: Тумаев М.А. Срок: до 30.12.2017

2.3.2. Выписки из «Плана ТЗИ-2017» и настоящего протокола направить в исполнительные органы государственной власти и органы местного самоуправления городских округов и муниципальных районов автономного округа (в части, касающейся).

Отв.: Тумаев М.А. Срок: до 30.12.2016

2.4. Руководителям исполнительных органов государственной власти автономного округа:

2.4.1. Разработать план комплексных мероприятий по защите информации в органе власти (по ранее доведенной форме, исх. от 12.02.2014 от ВЕ-2350) и направить в Управление защиты информации и специальной документальной связи Аппарата Губернатора автономного округа копию утвержденного «Плана комплексных мероприятий по защите информации в исполнительном органе государственной власти на 2017 год».

Срок: до 01.02.2017

2.4.2. Информационную справку о реализации мероприятий «Плана комплексных мероприятий по защите информации в исполнительном органе государственной власти на 2017 год» направить в Управление защиты информации и специальной документальной связи Аппарата Губернатора автономного округа.

Срок-до 10.12.2017

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 Тумаева М.А. 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» (далее - «План ОИБ».

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

3.3.1. На основании дополнительно представленных исполнительно-распорядительными органами местного самоуправления городских округов и муниципальных районов автономного округа предложений выполнить корректировку «Плана ОИБ».

Отв.: Тумаев М.А. Срок: до 15.02.2017

3.3.2. Скорректированный «План ОИБ» направить в исполнительно-распорядительные органы местного самоуправления городских округов и муниципальных районов автономного округа для исполнения.

Отв.: Тумаев М.А. Срок: до 28.02.2017

3.4. Руководителям исполнительно-распорядительных органов местного самоуправления городских округов и муниципальных районов автономного округа:

3.4.1.Организовать контроль за практической реализацией мероприятий «Плана ОИБ» (в части касающейся).

3.4.2. Информационную справку о реализации мероприятий «Плана ОИБ» и предложения по его корректировке направлять в Управление защиты информации и специальной документальной связи Аппарата Губернатора автономного округа вместе с ежегодным отчетом о состоянии работ по технической защите информации.

Срок: до 10.12.2017

3.5. Отметить неисполнение пункта 5.2.3.1 протокола заседания Совета по ТЗИ от 24.04.2015 № 1/15 администрациями муниципальных образований: Сургутский район, Ханты-Мансийский район, Октябрьский район, *(не представлена в Аппарат Губернатора автономного округа корректировка «Плана ОИБ» вместе с ежегодным отчетом о состоянии работ по технической защите информации за 2016 год).*

3.6. 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 01.02.2017 исполнение пункта 5.2.3.1 протокола заседания Совета по ТЗИ от 24.04.2015 № 1/15.

3.7. Главам муниципальных образований Сургутский район, Ханты-Мансийский район и Октябрьский район причины неисполнения протокольных решений Совета по ТЗИ рассмотреть на заседании ПДТК муниципального образования.

Предложения по корректировке Плана ОИБ направить в Управление защиты информации и специальной документальной связи Аппарата Губернатора Югры.

Срок: до 01.02.2016.

4. О выполнении решений, принятых на заседаниях Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе - Югре в 2016 году.

(Тумаев М.А.)

РЕШИЛИ:

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

4.2. Работу Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе - Югре в 2016 году признать удовлетворительной.

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

пункт 1.3 вопроса 1 протокола № 1/16 от 27 апреля 2016 года;
пункт 1.4.1 вопроса 1 протокола № 1/16 от 27 апреля 2016 года;
пункт 1.4.8 вопроса 1 протокола № 1/16 от 27 апреля 2016 года;
пункт 1.4.9 вопроса 1 протокола № 1/16 от 27 апреля 2016 года;
пункт 3.4 вопроса 3 протокола № 1/16 от 27 апреля 2016 года;
пункт 1.2.1 вопроса 1 протокола № 2/16 от 29 сентября 2016 года;
пункт 1.2.2 вопроса 1 протокола № 2/16 от 29 сентября 2016 года;
пункт 1.2.3 вопроса 1 протокола № 2/16 от 29 сентября 2016 года;
пункт 2.2.1 вопроса 2 протокола № 2/16 от 29 сентября 2016 года.

5. Об утверждении «Плана работы Совета по вопросам технической защиты информации на 2017 год».

(Чиликов А.Ю.)

РЕШИЛИ:

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

5.2. Утвердить «План работы Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе - Югре на 2017 год».

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

Отв.: Тумаев М.А. Срок: до 30.12.2017

Заместитель руководителя Аппарата Губернатора Ханты-Мансийского автономного округа - Югры, заместитель председателя Совета по ТЗИ М.А.Киселев

Секретарь Совета М.А.Тумаев

Начальник Управления защиты информации и специальной документальной связи Аппарата Губернатора автономного округа А.Ю.Чиликов