

**ПРОТОКОЛ**  
**заседания Совета по вопросам технической защиты информации**  
**в Ханты-Мансийском автономном округе - Югре**  
**№ 5/17**

г. Ханты-Мансийск

16 ноября 2017 года

**ПРЕДСЕДАТЕЛЬСТВОВАЛ**

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

В заседании Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе - Югре (далее - Совет, автономный округ) приняли участие должностные лица, определенные постановлением Губернатора автономного округа от 29 апреля 2011 года № 59.

Дополнительно на заседание Совета приглашены:

Чувардин Олег Петрович - руководитель Управления ФСТЭК России по Уральскому федеральному округу;

Привалова Елена Игоревна - заместитель начальника 2-го отдела Управления ФСТЭК России по Уральскому федеральному округу;

руководители исполнительных органов государственной власти автономного округа;

должностные лица, ответственные за руководство работами и реализацию мероприятий по защите информации в исполнительных органах государственной власти.

**1. О проведенных мероприятиях по устранению нарушений и недостатков в области обеспечения безопасности персональных данных, выявленных в ходе проверки Аппарата Губернатора и исполнительных органов государственной власти Ханты-Мансийского автономного округа - Югры представителями Управления ФСТЭК России по УрФО в сентябре 2017 года.**

(О.П.Чувардин, О.И.Белоножкина, П.И.Ципорин, А.А.Дренин,  
В.А.Нигматулин, А.А.Радужан, А.Ю.Чиликов)

**РЕШИЛИ:**

1.1. Информацию Управления ФСТЭК России по Уральскому федеральному округу (О.П.Чувардин), Депинформтехнологий Югры (П.И.Ципорин), Депобразования и молодежи Югры (А.А.Дренин), Депздрава Югры (В.А.Нигматулин), Депсоцразвития Югры (А.А.Радужан) и Управления защиты информации и специальной документальной связи Аппарата Губернатора Югры (А.Ю.Чиликов) принять к сведению.

1.2. Управлению защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа - Югры (далее - автономный округ) направить в исполнительные органы государственной власти (далее - ИОГВ) и органы местного самоуправления (далее - ОМСУ) автономного округа «Основные положения по формированию Политики обеспечения информационной безопасности в органах исполнительной власти субъектов Российской Федерации и органах местного самоуправления», разработанные Управлением ФСТЭК России по Уральскому федеральному округу.

Срок: до 21 ноября 2017 года.

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

1.3.1. Руководствоваться «Основными положениями по формированию Политики обеспечения информационной безопасности в органах исполнительной власти субъектов Российской Федерации и органах местного самоуправления» при планировании и осуществлении мероприятий по обеспечению информационной безопасности.

1.3.2. В случае эксплуатации микропрограммного обеспечения Intel Management Engine версий 11.0 и выше учесть уязвимость, позволяющую нарушителю выполнить произвольный код в среде контроллера ввода-вывода (микросхема Platform Controller Hub) на материнских платах, предназначенных для центральных процессоров семейства Skylake и выше, в обход механизмов защиты, функционирующих на уровнях базовой системы ввода-вывода и операционной системы, и тем самым получить полный контроль над средством вычислительной техники.

1.3.3. Принять меры, направленные на нейтрализацию уязвимости, указанную в пункте 1.3.2 настоящего протокола, согласно указаниям, изложенным в Информационном сообщении ФСТЭК России от 25 октября 2017 года № 240/22/4900 (*размещено на сайте <http://fstec.ru>*).

1.3.4. Информацию о выполнении пункта 1.3.3 настоящего протокола направить в Управление защиты информации и специальной документальной связи Аппарата Губернатора автономного округа.

Срок: до 15 декабря 2017 года.

1.4. Руководителям исполнительных органов государственной власти автономного округа, имеющих собственные домены, подготовить и направить в Депинформтехнологий Югры предложения о перенастройке доменной инфраструктуры (переводе домена) на домен Admugra.local.

Срок: до 20 декабря 2017 года.

**2. Направления совершенствования нормативной правовой и методической базы по вопросам технической защиты информации и обеспечения безопасности критической информационной инфраструктуры,**

---

(Е.И.Привалова)

**РЕШИЛИ:**

2.1. Информацию Е.И.Приваловой принять к руководству в работе.

2.2. Руководителям исполнительных органов государственной власти автономного округа:

2.2.1. Обеспечить выполнение «Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем (далее - ГИС) и дальнейшего хранения содержащейся в их базах данных информации», утвержденных постановлением Правительства Российской Федерации от 6 июля 2015 года № 676 (с изменениями на 11 мая 2017 года).

2.2.2. В целях выполнения требований по защите информации при создании ГИС необходимо:

а) определить информацию, подлежащую защите от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации;

б) провести анализ нормативных правовых актов, методических документов и государственных стандартов, которым должна соответствовать государственная информационная система;

в) классифицировать ГИС в соответствии с требованиями по защите информации;

г) определить угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в ГИС, и разработку на их основе модели угроз безопасности информации;

д) определить требования к системе (подсистеме) защиты информации, содержащейся в ГИС.

2.2.3. Создание системы осуществлять в соответствии с техническим заданием с учетом модели угроз безопасности информации, предусмотренной подпунктом "г" пункта 2.2.2 настоящего протокола.

2.2.4. Модель угроз безопасности информации и (или) техническое задание на создание ГИС необходимо согласовать с ФСТЭК России и ФСБ России (*в случае использования криптографических средств защиты информации*), в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации.

2.2.5. При создании ГИС учесть следующие последовательно реализуемые этапы:

а) разработка документации на ГИС и ее части (описание совокупности проектных решений);

- б) разработка рабочей документации на ГИС и ее части;
- в) разработка или адаптация программного обеспечения;
- г) пусконаладочные работы;
- д) проведение предварительных испытаний ГИС;
- е) проведение опытной эксплуатации ГИС;
- ж) проведение приемочных испытаний ГИС.

2.2.6. Ввод системы в эксплуатацию осуществить на основании правового акта исполнительного органа государственной власти автономного округа о вводе системы в эксплуатацию.

Учесть, что с 1 января 2019 года ввод ГИС в эксплуатацию не допускается в случае невыполнения установленных законодательством Российской Федерации требований по защите информации, включая отсутствие действующего аттестата соответствия требованиям безопасности информации.

2.3. Рекомендовать Главам городских округов и муниципальных районов автономного округа реализовать мероприятия по защите муниципальных информационных систем в соответствии с пунктом 2.2 настоящего протокола.

Руководитель Аппарата Губернатора –  
заместитель Губернатора Ханты-Мансийского  
автономного округа - Югры  
председатель Совета



*[Handwritten signature]*  
О.И.Белоножкина

Секретарь Совета

*[Handwritten signature]*

А.Ю.Чиликов