ПРОТОКОЛ
заседания Совета по вопросам технической защиты информации
в Ханты-Мансийском автономном округе – Югре
№ 3/17

г. Ханты-Мансийск 29 мая 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.

Дополнительно на заседание Совета приглашены:

Ципорин Павел Игоревич, директор Департамента информационных технологий автономного округа;

Торгашин Юрий Ильич, первый заместитель директора Департамента информационных технологий автономного округа;

Максимова Лилия Владимировна, первый заместитель директора Департамента образования и молодежной политики автономного округа;

Кукарская Марина Геннадьевна, заместитель директора Департамента финансов автономного округа;

Спиридонова Татьяна Сергеевна, заместитель руководителя Службы по контролю и надзору в сфере образования автономного круга;

Шадрин Александр Николаевич, начальник Управление телекоммуникаций, связи и телерадиовещания Департамента информационных технологий автономного округа;

Русова Маргарита Степановна, начальник отдела организационной работы и защиты информации Департамента образования и молодежной политики автономного округа;

Гудков Иван Валерьевич, и.о. начальника управления автоматизации и информационных технологий Департамента социального развития автономного округа;

Малкин Алексей Викторович, консультант отдела программно-технического обеспечения управления автоматизации и информационных технологий Департамента социального развития автономного округа;

Чистяков Сергей Николаевич, заместитель директора по организационным вопросам БУ автономного округа «Медицинский информационно аналитический центр»;

Шафета Денис Александрович, заместитель директора по вопросам информатизации и развития БУ автономного округа «Медицинский информационно аналитический центр».

1. О рассмотрении проектов нормативно-методических документов по вопросам информационной безопасности.

(Тумаев М.А.)

РЕШИЛИ:

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

1.2. Одобрить разработанные методические документы:

«Типовые функции и задачи должностного лица, ответственного за руководство работами по защите информации в исполнительном органе государственной власти (органе местного самоуправления) Ханты-Мансийского автономного округа – Югры»;

«Типовые функции и задачи должностного лица, ответственного за организацию обработки персональных данных в исполнительном органе государственной власти (органе местного самоуправления) Ханты-Мансийского автономного округа – Югры»;

«Типовые функции и задачи структурного подразделения (штатного специалиста, ответственного за реализацию мероприятий) по защите информации в исполнительном органе государственной власти (органе местного самоуправления) Ханты-Мансийского автономного округа – Югры»;

«Типовые функции и задачи администратора безопасности информации в исполнительном органе государственной власти (органе местного самоуправления) Ханты-Мансийского автономного округа – Югры;

«Типовые функции и задачи работников, эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные в исполнительном органе государственной власти (органе местного самоуправления) Ханты-Мансийского автономного округа – Югры»;

«Типовое положение о постоянно действующей технической комиссии по защите информации в исполнительном органе государственной власти Ханты-Мансийского автономного округа – Югры».

1.3. Управлению защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югры (далее – автономный округ) направить вышеуказанные методические документы в исполнительные органы государственной власти и органы местного самоуправления автономного округа.

Срок: до 05.06.2017

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

- провести анализ собственных организационно-распорядительных документов, разработанных в области обеспечения безопасности информации;

- организовать внесение изменений в должностные регламенты должностных лиц, ответственных за руководство и реализацию мероприятий по защите информации с учетом разработанных методических документов.

Срок: до 01.08.2017

2. О мероприятиях по защите информации, выполненных в исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры.

РЕШИЛИ:

2.1. Информацию Депинформтехнологий Югры (Ципорин П.И.), Депобразования и молодежной политики Югры (Максимова Л.В.), Депсоцразвития Югры (Гудков И.В.), Депздрава Югры (Шафета Д.А.), Депфина Югры (Кукарская М.Г.) и Обрнадзора Югры (Спиридовнова Т.С.) принять к сведению.

2.2. Руководителям исполнительных органов государственной власти автономного округа:

2.2.1. Продолжить реализацию мероприятий по обеспечению требуемого уровня защиты информации в соответствии с требованиями законодательства Российской Федерации и Ханты-Мансийского автономного округа – Югры;

2.2.2. Обеспечить нахождение на рабочих местах в период с 11 по 15 сентября 2017 года должностных лиц, ответственных за руководство и реализацию мероприятий по защите информации;

2.2.3. Доработать состав Обходного листа увольняемого работника, внеся в него дополнительные позиции, связанные с обеспечением информационной безопасности (согласование с АУ автономного округа «Югорский НИИ информационных технологий» (по прекращению действия электронной цифровой подписи) и согласование с БУ автономного округа «Окружной Центр ИКТ» (по исключению учетных записей в СЭДД «Дело» и служебной электронной почте).

2.2.4. Принять меры, направленные на исключение несанкционированного доступа в серверные (коммутационные) помещения, а также в технологические ниши (люки, шахты) и телекоммуникационные шкафы, в которых проложены линии связи и электропитания (далее – технологические объекты), для чего выполнить комплекс организационно-технических работ (при необходимости, во взаимодействии с БУ автономного округа «Дирекция по эксплуатации служебных зданий»):

- оснастить технологические объекты оконечными устройствами охранной сигнализации и (или) организовать опечатывание дверей данных объектов на постоянной основе;

- разработать и утвердить порядок вскрытия вышеуказанных технологических объектов, списки уполномоченных на вскрытие должностных лиц органов власти и обслуживающих организаций, порядок комиссионного вскрытия в нерабочее время (выходные и праздничные дни).

Срок: до 01.09.2017

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

- организовать проведение дополнительного мониторинга состояния готовности исполнительных органов государственной власти автономного округа к предстоящей проверке состояния системы и организации работ в области защиты информации, запланированной ФСТЭК России в сентябре 2017 года;

- результаты мониторинга довести до курирующих заместителей Губернатора автономного округа.

Срок: до 01.08.2017

2.4. Департаменту информационных технологий автономного округа:

- разработать план мероприятий по аттестации автоматизированных рабочих мест работников исполнительных органов государственной власти автономного округа с учетом завершения данных работ до 01.08.2017;

- направить информацию о реализации вышеуказанного плана в Управление защиты информации и специальной документальной связи Аппарата Губернатора автономного округа.

Срок: еженедельно, до момента завершения аттестационных работ.

3. О дополнительных мерах по защите государственных (муниципальных) информационных систем.

РЕШИЛИ:

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

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

3.2.1 Учесть при организации работ по обеспечению защиты информации в государственных (муниципальных) информационных системах следующие нарушения и недостатки[1]:

- не назначено должностное лицо, ответственное за защиту информации (пункты 14, 15 и 16 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (далее – ППРФ № 1119), а также п. 9 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17 (далее – приказ ФСТЭК № 17));

- управление доступом и регистрация событий безопасности реализуются программным обеспечением, не прошедшим необходимую оценку соответствия (п. 11 приказа ФСТЭК № 17);

[1] По результатам контрольных мероприятий, проведенных Управлением ФСТЭК России по УрФО

- используются средства защиты информации с истекшим сроком действия сертификата соответствия (п. 11 приказа ФСТЭК № 17);

- не определяется класс защищенности информационной системы, либо результаты классификации не оформлены актом классификации (п. 14.2 приказа ФСТЭК № 17);

- не определяется уровень защищенности персональных данных (п. 8 ППРФ № 1119);

- не определялись угрозы безопасности информации, модели угроз на их основе не разрабатываются, либо в модели угроз учтены не все актуальные угрозы безопасности информации (п. 1 части 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ), а также п.14.3 приказа ФСТЭК № 17));

- не проводится анализ уязвимостей информационной системы, в целях оценки возможности преодоления нарушителем системы защиты информации (п. 16.6 приказа ФСТЭК № 17);

- не осуществляется оценка эффективности принимаемых мер по обеспечению безопасности информации до ввода в эксплуатацию информационной системы, в том числе не принимается решение о повторной аттестации или проведении дополнительных аттестационных испытаниях при модернизации аттестованной информационной системы (п. 17.1, 17.4, 18.3 приказа ФСТЭК № 17);

- не осуществляется контроль за событиями безопасности и действиями пользователей в информационной системе (п.18.4 приказа ФСТЭК № 17);

- не осуществляется учет машинных носителей информации (п. 5 ч. 2 ст. 19 Закона № 152-ФЗ, п. 20, 20.4 Приказа № 17);

- не определены границы контролируемой зоны, а также меры по исключению несанкционированного доступа к средствам, обеспечивающим функционирование информационных систем (п. 20.12 приказа ФСТЭК № 17);

- меры по защите среды виртуализации не учитывались при аттестационных испытаниях (п. 20.11, 21 приказа ФСТЭК № 17);

- не реализованы меры по ограничению программной среды (п. 20.3 приказа ФСТЭК № 17);

- не реализованы в полном объеме меры по антивирусной защите (п. 20.6 приказа ФСТЭК № 17);

- не используются средства обнаружения (предотвращения) вторжений (п. 20.7 приказа ФСТЭК № 17);

- отсутствуют сертифицированные средства межсетевого экранирования, (п. 20.13, 26 приказа ФСТЭК № 17);

- не проводится анализ защищенности информационных систем, предполагающий применение сертифицированных программных средств (сканеров безопасности) (п. 6 и 9 части 2 статьи 19 Закона № 152-ФЗ, п. 20.8 приказа ФСТЭК № 17);

- не проводится периодический (ежегодный) контроль за выполнением требований к защите информации ограниченного доступа (п. 3.24 Специальных требований и рекомендаций по защите конфиденциальной

информации, утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282, п. 8.3 ГОСТ РО 0043-003-2012, п. 18.4 и 20.8 приказа ФСТЭК № 17);

- не установлены ограничения на срок действия пароля пользователя в средствах защиты информации от несанкционированного доступа (ИАФ.4 методический документ от 11.02.2014 «Меры защиты информации в государственных информационных системах»);

- состав программной среды не соответствует перечню программных средств, указанному в техническом паспорте (п. 18 приказа ФСТЭК № 17, п. 7.2-7.3 ГОСТ РО 0043-003-2012 «Аттестация объектов информатизации. Общие положения» от 17.04.2012);

- подключаются сотовые телефоны и USB-накопители информации на автоматизированные рабочие места, обрабатывающие государственные информационные ресурсы (п. 20.13 приказа ФСТЭК № 17);

- настройки средств защиты информации от несанкционированного доступа не соответствуют Матрице доступа (УПД.2 методический документ от 11.02.2014 «Меры защиты информации в государственных информационных системах»);

- на автоматизированных рабочих местах, предназначенных для работы с государственной (муниципальной) информационной системой, используются средства защиты информации от несанкционированного доступа устаревшей версии, имеющие в своем составе уязвимости (Информационное сообщение ФСТЭК России от 19.07.2016 № 240/24/3246, Информационное сообщение ФСТЭК от 12.04.2016 № 240/24/1649, размещены на сайте fstec.ru).

3.2.2. Провести анализ вышеуказанных нарушений (недостатков), организовать работу по их устранению.

Срок: до 01.09.2017

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

- учесть вышеуказанный состав недостатков и нарушений при проведении дополнительного мониторинга состояния готовности исполнительных органов государственной власти автономного округа к предстоящим контрольным мероприятиям;

- оказывать соответствующую методическую помощь должностным лицам исполнительных органов государственной власти автономного округа.

Срок: до 01.09.2017

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

Секретарь Совета М.А.Тумаев