Мэру города Омска
О.Н. Фадиной

Информационный материал
по вопросу: «Об организационных и технических мерах по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Перед планированием заседания комиссии по информатизации при Мэре города Омска Казенным учреждением города Омска «Управление информационно-коммуникационных технологий» проведен опрос структурных подразделений Администрации города Омска с целью выявления наиболее актуальных проблем в ИТ-сфере для рассмотрения в комиссии. Наиболее частым было предложение рассмотреть вопросы в области информационной безопасности.

Ежегодно Федеральная служба по техническому и экспортному контролю (далее – ФСТЭК) проводит проверки организаций – операторов персональных данных. Для подготовки к проверке необходимо обратить внимания всем руководителям структурных подразделений Администрации города Омска и подведомственных организаций на перечень проверяемых сведений и документов при контроле по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

1. Принадлежность информационной системы к системам обработки персональных данных (регистрация в Реестре операторов обработки персональных данных, наличие уведомления о начале обработки персональных данных).

2. Характеристика информационной системы, участвующей в обработке персональных данных (совокупность используемых баз данных, информационных технологий и технических средств, территориальная распределённость, внешние источники и потребители циркулирующей информации, особенности физической и логической топологии).

3. Акт оператора по классификации информационной системы персональных данных.

4. Модель угроз безопасности персональных данных (в том числе защита от утечки за счет ПЭМИН и акустической (речевой) информации).

5. Структура системы защиты персональных данных на объекте.

6. Задачи, функции и полномочия подразделения и (или) должностных лиц в части обеспечения безопасности персональных данных, организационно−распорядительные документы, регламентирующие их деятельность.

7. Документ, определяющий порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в

информационных системах.

8. Список сотрудников организации − оператора, допущенных к соответствующим персональным данным.

9. Электронный журнал обращений пользователей информационной системы к персональным данным.

10. Порядок взаимодействия с вышестоящими службами и федеральными органами исполнительной власти по вопросам безопасности персональных данных. Документы, регламентирующие вышеуказанные мероприятия.

11. Организация работ по привлечению сторонних организации для формирования и сопровождения баз данных и информационного взаимодействия (центров обработки информации), выполняющих функции операторов и администраторов системы централизованной обработки данных. Документы, регламентирующие вышеуказанные мероприятия.

12. Порядок предоставления информации органам власти, физическим и юридическим лицам. Документы, регламентирующие вышеуказанные мероприятия.

13. Периодичность и порядок резервирования - обрабатываемой информации. Документы, регламентирующие вышеуказанные мероприятия.

14. Организация учета и использования магнитных, оптических и других машинных носителей информации. Документы, регламентирующие вышеуказанные мероприятия.

15. Обучение лиц, применяющих средства защиты информации.

16. Состав технических средств (ТС) с указанием наличия сертификатов (предписаний на эксплуатацию), мест (помещений) их установки и программно-математического обеспечения (ПМО), производители ТС и ПМО.

17. Разработка системы защиты персональных данных на основе утвержденной модели угроз безопасности персональных данных.

18. Порядок доступа пользователей к информационным ресурсам (наличие утвержденного списка сотрудников, допущенных к обработке персональных данных, организация регистрации доступа пользователей).

19. Мероприятия по защите информации от НСД (правильность установки и порядок эксплуатации средств защиты от НСД к информации, наличие на них сертификатов соответствия требованиям по безопасности информации).

20. Порядок обеспечения неизменности технических и программных средств (исключение доступа к монтажу, портам, модемам, порядок внесения изменений в телекоммуникационную схему, технические средства, программное обеспечение и СЗИ). Документы, регламентирующие вышеуказанные мероприятия.

21. Документы, определяющие соответствие выполнения требований НМД ФСТЭК России с учетом присвоенного класса ИСПДн и Модели угроз безопасности ПДн при их обработке в ИСПДн:

- по управлению доступом;
- по регистрации и учету;
- по обеспечению целостности;
- по обеспечению безопасного межсетевого взаимодействия;
- по контролю отсутствия недекларированных возможностей;
- по антивирусной защите;
- к системе анализа защищенности;
- к системе обнаружения вторжений.

Федеральным законодательством РФ предусмотрена ответственность за нарушение требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». В зависимости от конкретных обстоятельств и серьезности нарушений может последовать административная, гражданско-правовая, дисциплинарная ответственность (Приложение 1). Административная ответственность с 1 июля 2017 года ужесточилась – вместо одного состава правонарушения ст. 13.11 КоАП РФ теперь предусматривает семь.

Приложение 1

Виды ответственности за нарушение Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»

Вид ответственности	Нарушение	Санкция	Норма
Административная	Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено законом, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации	Административный штраф на должностных лиц в размере от 5 тыс. до 10 тыс. руб.	Статья 5.39 КоАП РФ
	Обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных	Предупреждение или административный штраф: на граждан – от 1 тыс. до 3 тыс. руб.; на должностных лиц – от 5 тыс. до 10 тыс. руб.; на юридических лиц – от 30 тыс. до 50 тыс. руб.	Часть 1 ст. 13.11 КоАП РФ
	Обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие	Административный штраф: на граждан – от 3 тыс. до 5 тыс. руб.; на должностных лиц – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 15 тыс. до 75 тыс. руб.	Часть 2 ст. 13.11 КоАП РФ

	Невыполнение оператором обязанности по опубликованию или обеспечению иным образом неограниченного доступа к политике обработки персональных данных	Предупреждение или административный штраф: на граждан – от 700 до 1 тыс. руб.; на должностных лиц – от 3 тыс. до 6 тыс. руб.; на индивидуальных предпринимателей – от 5 тыс. до 10 тыс. руб.; на юридических лиц – от 15 тыс. до 30 тыс. руб.	Часть 3 ст. 13.11 КоАП РФ
	Невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	Предупреждение или административный штраф: на граждан – от 1 тыс. до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 6 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 15 тыс. руб.; на юридических лиц – от 20 тыс. до 40 тыс. руб.	Часть 4 ст. 13.11 КоАП РФ
	Невыполнение оператором в установленные сроки требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении (если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели	Предупреждение или административный штраф: на граждан – от 1 тыс. до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 10 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 25 тыс. до 45 тыс. руб.	Часть 5 ст. 13.11 КоАП РФ

	обработки)		
	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих их сохранность и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении них	Административный штраф: на граждан – от 700 до 2 тыс. руб.; на должностных лиц – от 4 тыс. до 10 тыс. руб.; на индивидуальных предпринимателей – от 10 тыс. до 20 тыс. руб.; на юридических лиц – от 25 тыс. до 50 тыс. руб.	Часть 6 ст. 13.11 КоАП РФ
	Невыполнение оператором, являющимся государственным или муниципальным органом, обязанности по обезличиванию персональных данных либо несоблюдение установленных для этого требований или методов	Предупреждение или наложение административного штрафа на должностных лиц в размере от 3 тыс. до 6 тыс. руб.	Часть 7 ст. 13.11 КоАП РФ
	Непредставление или несвоевременное представление в государственный или иной уполномоченный орган сведений, представление которых предусмотрено законом либо предоставление таких сведений в неполном объеме или в искаженном виде	Административный штраф: на граждан – от 100 до 300 руб.; на должностных лиц – от 300 до 500 руб.; на юридических лиц – от 3 тыс. до 5 тыс. руб.	Статья 19.7 КоАП РФ

Уголовная	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ	Штраф до 200 тыс. руб., либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо принудительные работы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет или без такового), либо арест на срок до четырех месяцев, либо лишение свободы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет)	Статья 137 Уголовного кодекса
	То же деяние, совершенное с использованием служебного положения	Штраф от 100 тыс. до 300 тыс. руб., либо лишение права занимать определенные должности на срок от двух до пяти лет, либо принудительные работы на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет или без такового), либо арест на срок до шести месяцев, либо лишение свободы на срок до четырех лет (с лишением права занимать определенные должности на срок до пяти лет)	
	Незаконное публичное распространение информации, указывающей на личность лица, не достигшего 16 лет, по уголовному делу, либо информации, содержащей описание	Штраф от 100 тыс. до 300 тыс. руб., либо лишение права занимать определенные должности на срок от трех до пяти лет, либо принудительные работы на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет или без такового), либо арест на срок до	

	полученных им в связи с преступлением физических или нравственных страданий	шести месяцев, либо лишение свободы на срок до пяти лет (с лишением права занимать определенные должности на срок до шести лет)	
	Неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление ему неполной или заведомо ложной информации, если это причинило вред правам и законным интересам граждан	Штраф до 200 тыс. руб., либо лишение права занимать определенные должности на срок от двух до пяти лет	Статья 140 УК РФ
	Неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование	Штраф до 200 тыс. руб., либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо лишение свободы на тот же срок	Статья 272 УК РФ
Гражданско-правовая	Причинение лицу убытков в результате нарушения правил обработки его персональных данных. Под убытками при этом понимаются: расходы, которые лицо произвело или должно будет произвести для восстановления нарушенного права; утрата или повреждение его имущества; неполученные доходы, которые лицо получило бы, не будь его право нарушено.	Возмещение убытков	Статья 15 Гражданского кодекса

	Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных	Компенсация морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков)	Статья 24 закона о персональных данных, ст. 151 ГК РФ
Дисциплинарная	Разглашение одним работником персональных данных другого, если они стали известны ему в связи с исполнением трудовых обязанностей	Увольнение	Подпункт "в" п. 6 ч. 1 ст. 81 Трудового кодекса
	Иные нарушения в области персональных данных при их обработке	Замечание или выговор	Статья 90, ст. 192 ТК РФ

Приложение 2

КУ г. Омска УИКТ (далее – УИКТ) готово оказывать методическую и консультационную помощь всем структурным подразделениям Администрации города Омска по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. При необходимости аттестовать объект информатизации.

УИКТ имеет лицензии

1) Управления федеральной службы безопасности Российской федерации по Омской области № 0001509 от 11 декабря 2012 года на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств;

2) Федеральной службы по техническому и эскпортному контролю № 1419 от 31 марта 2011 года на осуществление деятельности по контролю защищенности конфиденциальной информации от утечки по техническим каналам, по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации, по проектированию в защищенном исполнении, по установке и монтажу средств защиты информации.

Сотрудники сектора информационной УИКТ в полным составе прошли обучение в Омском государственном техническом университете по программе «Обеспечение комплексной защиты информации ограниченного доступа, не составляющую государственную тайну, в государственных информационных системах» в объеме 100 часов.

Двое сотрудников прошли профессиональную переподготовку в Частном учреждении дополнительного профессионального образования «Центр информационных технологий и безопасности информационных систем» по программе «Комплексное обеспечение информационной безопасности автоматизированных систем. Криптографические средства и методы защиты информации» в объеме 560 часов.

УИКТ имеет в собственности оборудование для осуществления деятельности по технической защите информации: а) для Оценки защищенности технических средств от утечки по каналу ПЭМИН (Измерительный комплекс «СИГУРД»); б) для Оценки защищенности выделенных помещений по виброакустическому каналу (Измерительный комплекс «ШЕПОТ»); в) для Измерения действующих высот случайных антенн и реального затухания электромагнитных сигналов (измерительный комплекс «СТЕНТОР»); г) специальное программное обеспечение для оценки защищенности информационных систем от несанкционированного доступа.

Для обеспечения защиты информации по каналам связи создан Удостоверяющий центр VipNet с разветвленной сетью координаторов в округах и департаментах.

Для проведения поисковых мероприятий в рамках Администрации города Омска в УИКТ имеется необходимая аппаратура поиска и обнаружения устройств негласного съема информации.

В Администрации города Омска и ее структурных подразделениях в настоящее время имеются четырнадцать Муниципальных информационных систем. Сектор информационной безопасности в составе УИКТ ведет работы, связанные с аттестованными объектами информатизации (единый реестр избирателей, база детей оставшихся без попечительства, реестр муниципальных служащих и др.).