Республика Крым
Глава муниципального образования – председатель Евпаторийского городского совета

ПОСТАНОВЛЕНИЕ

«06» сентября 2017 года № 38

Об определении угроз безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Евпаторийском городском совете Республики Крым

С целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента Российской Федерации от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», во исполнение поручения Главы Республики Крым от 13.07.2017г. № 1/01-32/3891,-

ПОСТАНОВЛЯЮ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Евпаторийском городском совете Республики Крым, согласно приложению к настоящему постановлению.
2. Настоящее постановление вступает в силу со дня его официального опубликования (обнародования) и подлежит размещению на официальном сайте Правительства Республики Крым - http://rk.gov.ru в разделе: муниципальные образования, подраздел — Евпатория, а также на официальном сайте муниципального образования городской округ Евпатория Республики Крым - http://myevp.ru в разделе - Документы, подраздел - Постановления Главы муниципального образования.
3. Контроль за исполнением настоящего постановления возложить на заместителя председателя Евпаторийского городского совета Республики Крым Кутнева С.А.

Председатель
Евпаторийского городского совета **О.В. Харитоненко**

Приложение к постановлению
председателя Евпаторийского
городского совета Республики Крым
от «06» 09 2017 г. № 38

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Евпаторийском городском совете Республики Крым

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Евпаторийского городского совета Республики Крым (далее - Актуальные угрозы безопасности ИСПДн) разработаны в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.2. Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) Евпаторийского городского совета Республики Крым (далее – городской совет).

1.3. При разработке Актуальных угроз безопасности ИСПДн использованы методические документы, модели угроз безопасности персональных данных, утвержденные Федеральной службой по техническому и экспортному контролю Российской Федерации (далее - ФСТЭК России) и Федеральной службой безопасности Российской Федерации (далее - ФСБ России).

1.4. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, приведенные в Актуальных угрозах безопасности ИСПДн, подлежат адаптации в ходе разработки частных моделей угроз безопасности персональных данных.

1.5. При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик конкретной ИСПДн и применяемых в ней информационных технологий, особенностей ее функционирования.

1.6. В частной модели угроз безопасности персональных данных указываются:

- описание ИСПДн и ее структурно-функциональных характеристик;
- описание угроз безопасности персональных данных с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;
- описание возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

1.7. Типовая форма частной модели угроз безопасности персональных данных разрабатывается с учетом требований Приказа Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Приказа Федеральной службы безопасности России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (далее - Приказ ФСБ России).

1.8. Актуальные угрозы безопасности персональных данных, обрабатываемых в ИСПДн, содержащиеся в Актуальных угрозах безопасности ИСПДн, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. Указанные изменения согласовываются с ФСТЭК России и ФСБ России в установленном порядке.

1.9. Информационные системы персональных данных в городском совете имеют сходную структуру, однотипны, характеризуются тем, что в качестве объектов информатизации выступают распределенные информационные системы, имеющие подключение к единому центру обработки данных, а также подключение к сетям общего пользования и (или) сетям международного информационного обмена.

1.10. Ввод персональных данных в ИСПДн и вывод данных из ИСПДн осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и компакт-диски.

1.11. Персональные данные субъектов персональных данных обрабатываются:

- в целях обеспечения деятельности Главы муниципального образования и структурных подразделений городского совета;
- в целях обеспечения кадровой работы, в том числе в целях содействия муниципальным служащим в прохождении муниципальной службы, выполнении работы, в обучении и должностном росте, обеспечения личной безопасности служащих и членов их семей, обеспечения сохранности принадлежащего им имущества и имущества городского совета, учета результатов исполнения ими должностных обязанностей, обеспечения

установленных законодательством Российской Федерации условий осуществления служебной деятельности и труда, гарантий и компенсаций;

- в целях формирования кадрового резерва на муниципальной службе, противодействия коррупции;
- в целях реализации процедур по представлению граждан к награждению;
- в целях приема, обработки и распределения поступивших в адрес Главы муниципального образования, руководителей структурных подразделений документов, обращений граждан и организаций, а также регистрации и отправки исходящей корреспонденции;
- в целях ведения внутренней служебной переписки;
-в целях формирования внутренних документов, регламентирующих деятельность городского совета;
- в целях подготовки и проведения мероприятий с участием или по поручению Главы муниципального образования, подготовки пресс-релизов о деятельности городского совета, взаимодействия со сторонними СМИ.

1.12. Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных средств криптографической защиты информации (далее - СКЗИ).

1.13. Контролируемой зоной ИСПДн являются административные здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

1.14. В административных зданиях неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники запрещено. Помещения оборудованы запирающимися дверями.

2. Угрозы безопасности информационных систем персональных данных

2.1. Учитывая особенности обработки персональных данных в городском совете, а также категорию и объем обрабатываемых в ИСПДн персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

2.2. Конфиденциальность - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

2.3. Целостность - состояние защищенности информации,

характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

2.4. Доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

2.5. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

2.6. Для ИСПДн городского совета актуальны угрозы безопасности третьего типа.

2.7. Исходя из состава обрабатываемых персональных данных и типа актуальных угроз, определяется, что для обеспечения безопасности персональных данных в ИСПДн городского совета необходимо обеспечение четвертого уровня защищенности персональных данных (УЗ 4).

2.8. Основной целью применения в ИСПДн городского совета СКЗИ является защита персональных данных, в том числе при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

2.9. Объектами защиты являются:

- персональные данные (ПДн);
- средства криптографической защиты информации (СКЗИ);
- среда функционирования СКЗИ (далее - СФ);
- информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;
- носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
-используемые информационной системой каналы (линии) связи, включая кабельные системы;
- помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

2.10. Основными видами угроз безопасности персональным данным в ИСПДн являются:

- угрозы утечки информации по техническим каналам;
- угрозы утечки акустической информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналам ПЭМИН;
- угрозы несанкционированного доступа к информации;
- угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;
- кража ПЭВМ;
- кража носителей информации;
- кража ключей и атрибутов доступа;
- кража, модификация, уничтожение информации;
- вывод из строя узлов ПЭВМ, каналов связи;
- несанкционированное отключение средств защиты;
- угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (далее - НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- действия вредоносных программ (вирусов);
- использование не декларированных возможностей системного программного обеспечения (далее - ПО) и ПО для обработки персональных данных;
- установка ПО, не связанного с исполнением служебных обязанностей;
- угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты персональных данных (далее - СЗПДн) в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного характера (ударов молний, пожаров, наводнений и т.п.);
- утрата ключей и атрибутов доступа;
- непреднамеренная модификация (уничтожение) информации сотрудниками;
- непреднамеренное отключение средств защиты;
- выход из строя аппаратно-программных средств;
- сбой системы электроснабжения;
- стихийное бедствие;
- угрозы преднамеренных действий внутренних нарушителей;
- доступ к информации, модификация, уничтожение информации лицами, не допущенными к ее обработке;
- разглашение информации, ее модификация или уничтожение сотрудниками, допущенными к ее обработке;
- угрозы несанкционированного доступа по сети и каналам связи;
- угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
- перехват за пределами контролируемой зоны;
- перехват в пределах контролируемой зоны внешними нарушителями;

- перехват в пределах контролируемой зоны внутренними нарушителями;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей по сети;
- угрозы навязывания ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа "Отказ в обслуживании";
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ;
- угрозы несанкционированного доступа при использовании технологий виртуализации;
- угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;
- нарушение работоспособности информационных систем, построенных на основе технологий виртуализации, за счет несанкционированного доступа к средствам виртуализации;
- атака на виртуальные каналы передачи данных;
- несанкционированный доступ к образам виртуальных машин;
- нарушение изоляции пользовательских данных внутри виртуальных машин;
- атака на гипервизор с виртуальной машины;
- атака на гипервизор из физической сети;
- атака на защищаемые виртуальные машины из физической сети;
- неконтролируемый рост числа виртуальных машин;
- атака на сеть репликации виртуальных машин;
- перехват управления в среде виртуализации;
- выход процесса за пределы виртуальной среды.

2.11. При определении актуальных угроз безопасности персональных данных используются следующие положения:
- единый подход к созданию, развитию (модернизации) и эксплуатации информационных систем городского совета, основанный на согласовании технологий обработки информации с Министерством внутренней политики, информации и связи Республики Крым;
- реализация единого порядка согласования технических заданий и технических проектов на создание информационных систем и входящих в их состав систем защиты информации с использованием некриптографических средств защиты информации (далее - СЗИ) и (или) с использованием средств криптографической защиты информации (СКЗИ).

3. Актуальные угрозы безопасности ИСПДн:

- действия вредоносных программ (вирусов);
- утрата ключей и атрибутов доступа;
- перехват передаваемой из ИСПДн и принимаемой из внешних сетей

информации за пределами контролируемой зоны;
- доступ через сети международного обмена;
- несанкционированный доступ через ЛВС организации;
- утечка атрибутов доступа;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей по сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа "Отказ в обслуживании";
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ;
- угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;
- нарушение работоспособности информационных систем, построенных на основе технологий виртуализации, за счет несанкционированного доступа к средствам виртуализации;
- атака на виртуальные каналы передачи данных;
- несанкционированный доступ к образам виртуальных машин;
- нарушение изоляции пользовательских данных внутри виртуальных машин;
- атака на гипервизор с виртуальной машины;
- атака на гипервизор из физической сети;
- атака на защищаемые виртуальные машины из физической сети;
- неконтролируемый рост числа виртуальных машин;
- атака на сеть репликации виртуальных машин;
- перехват управления в среде виртуализации;
- выход процесса за пределы виртуальной среды.