ПРАВИТЕЛЬСТВО ПРИМОРСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

25.12.2020 г. Владивосток № 1070-пп

О внесении изменений в постановление Администрации Приморского края от 26 августа 2019 года № 553-па «О перечне угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Приморского края, аппарате Администрации Приморского края, аппарате Губернатора Приморского края, органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях»

На основании Устава Приморского края Правительство Приморского края постановляет:

1. Внести в постановление Администрации Приморского края от 26 августа 2019 года № 553-па «О перечне угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Приморского края, аппарате Администрации Приморского края, аппарате Губернатора Приморского края, органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях» (далее - постановление) следующие изменения:

1.1. Изложить наименование постановления в следующей редакции:

«Об утверждении Перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Правительстве Приморского края, в

аппарате Губернатора Приморского края и Правительства Приморского края, в органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях.»;

1.2. Изложить пункт 1 постановления в следующей редакции:

«1. Утвердить прилагаемый Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Правительстве Приморского края, в аппарате Губернатора Приморского края и Правительства Приморского края, в органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях.»;

1.3. Изложить пункт 4 постановления в следующей редакции:

«4. Контроль за исполнением настоящего постановления возложить на заместителя председателя Правительства Приморского края, курирующего вопросы государственно-правового управления, гражданской обороны, защиты от чрезвычайных ситуаций и ликвидации последствий стихийных бедствий Приморского края, записи актов гражданского состояния, защиты государственной тайны, мобилизационной подготовки, общественной безопасности и координации правоохранительной деятельности, исполнения административного законодательства, обеспечения деятельности мировых судей.»;

1.4. Изложить Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Администрации Приморского края, аппарате Администрации Приморского края, аппарате Губернатора Приморского края, органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях, утвержденный постановлением, в новой редакции согласно приложению к настоящему постановлению.

2. Департаменту информационной политики Приморского края обеспечить официальное опубликование настоящего постановления.

И.о. первого вице-губернатора Приморского края –
председателя Правительства
Приморского края А.А. Волошко

Приложение

к постановлению
Правительства Приморского края
от 25.12.2020 № 1070-пп

ПЕРЕЧЕНЬ
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в Правительстве Приморского края, в аппарате Губернатора края и Правительства Приморского края, в органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях

I. Основные угрозы безопасности персональных данных	
№ п/п	Наименование угрозы
1	**2**
1.1.	Угроза деструктивного использования декларированного функционала BIOS
1.2.	Угроза загрузки нештатной операционной системы
1.3.	Угроза изменения режимов работы аппаратных элементов компьютера
1.4.	Угроза неправомерного ознакомления с защищаемой информацией
1.5.	Угроза неправомерных действий в каналах связи
1.6.	Угроза несанкционированного копирования защищаемой информации
1.7.	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
1.8.	Угроза несанкционированного использования привилегированных функций BIOS
1.9.	Угроза несанкционированного удаления защищаемой информации
1.10.	Угроза повреждения системного реестра
1.11.	Угроза подмены действия пользователя путём обмана

1	2
1.12.	Угроза подмены субъекта сетевого доступа
1.13.	Угроза приведения системы в состояние «отказ в обслуживании»
1.14.	Угроза заражения компьютера при посещении неблагонадёжных сайтов
1.15.	Угроза неправомерного шифрования информации
1.16.	Угроза распространения «почтовых червей»
1.17.	Угроза «фишинга»
1.18.	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты
1.19.	Угроза отказа подсистемы обеспечения температурного режима
1.20.	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
1.21.	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере
1.22.	Угроза некорректного использования функционала программного обеспечения
1.23.	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
1.24.	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
1.25.	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
1.26.	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
1.27.	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
1.28.	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети
1.29.	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
1.30.	Угроза несанкционированного доступа к виртуальным каналам передачи
1.31.	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети

1	2
1.32.	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения
1.33.	Угроза несанкционированного доступа к системе при помощи сторонних легитимных сервисов (социальных сетей, мессенджеров, репозиториев кода и т.п.), используемых в качестве посредника.
1.34.	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации.
1.35.	Угроза перехвата управления информационной системой в результате подмены средств централизованного управления информационной системой или её компонентами.
II. Актуальные возможности источников атак, направленных на нарушение безопасности информации, защищаемой с помощью СКЗИ	
№ п/п	**Описание возможности источников атак (соответствующие актуальные угрозы)**
2.1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны
2.2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и СФК
2.3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и СФК
III. Возможные действия нарушителей, направленные на нарушение безопасности информации.	
№ п/п	**Уточненные возможности нарушителей и направления атак**
3.1.	Проведение атаки при нахождении в пределах контролируемой зоны
3.2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФК; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФК
3.3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

1	2
	- сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФК
3.4.	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий
3.5.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФК
3.6.	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий