АДМИНИСТРАЦИЯ
ПРИСТЕНСКОГО РАЙОНА КУРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 13 мая 2021 № 269-па

О формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определения на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ в информационной системе «Кадры и обращения граждан» в Администрации Пристенского района Курской области

С целью определения класса средств криптографической защиты информации (далее - СКЗИ), позволяющего обеспечить безопасность персональных данных, Администрация Пристенского района Курской области ПОСТАНОВЛЯЕТ:

1. Назначить комиссию в следующем составе:

Председатель комиссии:

– заместитель главы администрации, управляющий делами Администрации Пристенского района Курской области – Миронова Наталья Михайловна;

члены комиссии:

– И.о. начальника отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области – Озеров Иван Сергеевич;

– консультант отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области – Дронова Анна Александровна;

– консультант отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области – Надеина Кристина Александровна;

– консультант отдела организационной, кадровой работы и делопроизводства Администрации Пристенского района Курской области – Гольцова Елена Николаевна.

2. Провести формирование совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак в информационной системе «Кадры и обращения граждан» в Администрации Пристенского района Курской области.

3. Определить на основе сформированной совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и с учетом типа актуальных угроз требуемый класс СКЗИ для использования в информационной системе «Кадры и обращения граждан» в Администрации Пристенского района Курской области в соответствии с Приказом ФСБ России от 10.07.2014 №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».

4. По результатам работ оформить для утверждения Акт формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определения на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ в информационной системе «Кадры и обращения граждан» в Администрации Пристенского района Курской области согласно прилагаемой форме.

5. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации, управляющего делами Администрации Пристенского района Курской области - Миронову Н.М.

6. Постановление вступает в силу со дня его подписания.

Глава Пристенского района
Курской области **В.В. Петров**

УТВЕРЖДЕНО
постановлением Администрации
Пристенского района Курской области
от 13.05.2021 № 269-па

УТВЕРЖДАЮ
Глава Пристенского района
Курской области
_____ В.В. Петров
м.п.
_____г.

АКТ

формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определения на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ в информационной системе «Кадры и обращения граждан» в Администрации Пристенского района Курской области

В соответствии с постановлением Администрации Пристенского района Курской области от _____ № _____ комиссия в составе:

Председатель комиссии:

– заместитель главы администрации, управляющий делами Администрации Пристенского района Курской области – Миронова Наталья Михайловна;

члены комиссии:

– И.о. начальника отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области – Озеров Иван Сергеевич;

– консультант отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области – Дронова Анна Александровна;

– консультант отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области – Надеина Кристина Александровна;

– консультант отдела организационной, кадровой работы и делопроизводства Администрации Пристенского района Курской области – Гольцова Елена Николаевна

руководствуясь Приказом ФСБ России от 10.07.2014 №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» провела формирование совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ в информационной системе «Кадры и обращения граждан» в Администрации Пристенского района Курской области.

На основании экспертной оценки комиссией установлено:

1. При создании способов, подготовке и проведении атак нарушителем могут использоваться следующие возможности:

а) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

б) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ;

в) проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона);

г) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

внесение несанкционированных изменений в СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ;

д) проведение атак на этапе эксплуатации СКЗИ на:

персональные данные;

ключевую, аутентифицирующую и парольную информацию СКЗИ;

программные компоненты СКЗИ;

программные компоненты СФ, включая программное обеспечение BIOS;

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

е) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:

общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);

сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением

сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;

содержание конструкторской документации на СКЗИ;

содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);

все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;

сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;

ж) применение:

находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

специально разработанных АС и ПО;

з) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

и) проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

к) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства).

2. Для информационной системы «Кадры и обращения граждан» в Администрации Пристенского района Курской области актуальны угрозы 3 типа, т.к. для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

3. На основании сформированной совокупности предположений о возможностях, которые могут использоваться при создании способов,

подготовке и проведении атак, с учетом типа актуальных угроз и согласно Приказа ФСБ России от 10.07.2014 №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» **для обеспечения безопасности персональных данных в информационной системе «Кадры и обращения граждан» в Администрации Пристенского района Курской области требуется применять СКЗИ класса КС1.**

Председатель комиссии:

заместитель главы администрации, управляющий делами Администрации Пристенского района Курской области	_____ подпись	Н.М. Миронова

Члены комиссии:

И.о. начальника отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области	_____ подпись	И.С. Озеров
консультант отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области	_____ подпись	А.А. Дронова
консультант отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области	_____ подпись	К.А. Надеина
консультант отдела организационной, кадровой работы и делопроизводства Администрации Пристенского района Курской области	_____ подпись	Е.Н. Гольцова