АДМИНИСТРАЦИЯ ПРИВОЛЖСКОГО МУНИЦИПАЛЬНОГО РАЙОНА

ПОСТАНОВЛЕНИЕ

от 30.11.2017 № 890 - п

О внесении изменений в постановление администрации Приволжского муниципального района от 28.01.2014 № 38-п «Об утверждении мер, направленных на обработку персональных данных в администрации Приволжского муниципального района»

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 года N 152-ФЗ «О персональных данных» и во исполнение Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», администрация Приволжского муниципального района **п о с т а н о в л я е т:**

1. Внести в постановление администрации Приволжского муниципального района от 28.01.2014 № 38-п «Об утверждении мер, направленных на обработку персональных данных в администрации Приволжского муниципального района» следующие изменения:

1.1. Изложить перечень информационный систем персональных данных в новой редакции (приложение №3).

1.2. Утвердить Типовые обязанности пользователей при обработке персональных данных в автоматизированных информационных системах, используемых в администрации Приволжского муниципального района. (Приложение №13).

1.3. Утвердить инструкцию по организации антивирусной защиты в администрации Приволжского муниципального района (Приложение №14)

1.4. Утвердить перечень угроз безопасности персональных данных в информационных системах, эксплуатируемых в администрации Приволжского муниципального района (Приложение №15).

2. Руководителям структурных подразделений администрации Приволжского муниципального района при работе с персональными данными руководствоваться настоящим постановлением.

3. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации - руководителя аппарата администрации

Приволжского муниципального района С.Е. Сизову

4. Опубликовать настоящее постановление в информационном бюллетене «Вестник Совета и администрации Приволжского муниципального района» и разместить на официальном сайте Приволжского муниципального района.

5. Настоящее постановление вступает в силу с момента подписания.

ВРИП Главы Приволжского
муниципального района **Е.Б.Носкова**

Приложение №3
к Постановлению
администрации Приволжского
муниципального района
от 28.01.2014 г. №38-п

Реестр информационных систем
администрации Приволжского муниципального района

№	Наимено-вание ИС	Дата и № регист рации в реестре	Область использования и назначения	Содержание и особенности	Сведени я о разрабо тчике	Пользователи ИС	Дата измен ения записи в реестр е	Основ ания измене ния записи в реестр е	Дата исключе ния из реестра	Основ ание исклю чения из реестр а
1	2	3	4	5	6	7	8	9	10	11
1	Консуль тант Плюс		Настоящий стандарт распространяется на организационно-распорядительные документы, относящиеся к Унифицированной системе организационно-распорядительной документации (УСОРД), - постановления, распоряжения, приказы, решения, протоколы, акты, письма и др. (далее - документы), включенные в ОК 011-93	"Общероссийский классификатор управленческой документации	Консуль тант Плюс	Отделы и комитеты администрации Приволжского муниципальног о района				

			"Общероссийский классификатор управленческой документации" (ОКУД) (класс 0200000)							
2	1С		Ведение бухгалтерского учета		1С	Финансовое управление администрации Приволжского района, МКУ «ОКМСиТ», МКУ "МФЦ. Управление делами"				
3	Контур Экстерн		Системы защищённого электронного документооборота, позволяющей сдавать отчётность в ФНС, ПФР, ФСС и др. контролирующие органы	Системы защищённого электронного документооборота, позволяющей сдавать отчётность в ФНС, ПФР, ФСС и др. контролирующие органы	СКБ Контур	Финансовое управление администрации Приволжского района; МКУ «ОКМСиТ», МКУ "МФЦ. Управление делами"				
4	Spu_orb		Подготовка отчетных документов для сдачи в Пенсионный фонд России	Подготовка отчетных документов для сдачи в Пенсионный фонд России	ОПФР по Оренбургской области	Финансовое управление администрации Приволжского района				

5	Налогоплательщик ЮЛ		Подготовка отчетных документов для сдачи в налоговую службу.	Пограмма предназначена для автоматизации процесса подготовки юридическими и физическими лицами документов налоговой и бухгалтерской отчётности, расчета страховых взносов, справок о доходах физических лиц (форма №2-НДФЛ), специальных деклараций (декларирование активов и счетов), документов по регистрации ККТ и других.	Филиал ФГУП ГНИВЦ ФНС России в Чувашской Республике	Отделы и комитеты администрации Приволжского муниципального района				
6	Свод-смарт		Комплексное Интернет-решение, обеспечивающее формирование консолидированной отчетности всеми участниками бюджетного процесса в масштабе субъекта Российской Федерации, главного распорядителя,	WEB-подключение по интернет-каналу; СМАРТ-подключение по интернет-каналу;	КОМПАНИЯ «КЕЙС ИСТЕМС»	Финансовое управление администрации Приволжского района				

			муниципального образования.	СМАРТ-подключение по локальной сети. Поддержка сбора отчетности в единой базе данных от всех участников бюджетного процесса, создание и поддержка иерархии бюджетов бюджетной системы Российской Федерации и организаций любого уровня вложенности (ГРБС, РБС, ПБС.						
7	Бюджет-смарт		Программный комплекс «Бюджет-СМАРТ» предназначен для автоматизации процессов составления, анализа и исполнения бюджета субъекта и бюджетов муниципальных образований.	Программный комплекс «Бюджет-СМАРТ» обеспечивает возможность работы в режиме отсутствия связи с финансовым органом и построен по трехуровневой архитектуре (клиентское приложение – сервер приложений – сервер баз данных) на базе объектного ядра	КОМПАНИЯ «КЕЙС ИСТЕМС»	Финансовое управление администрации Приволжского района				

				прикладного программного комплекса «Бюджет-КС», эксплуатируемого в территориальных и муниципальных финансовых органах. Наследует мощную справочную систему и удобную систему администрирования, имеет полную совместимость по форматам передаваемых данных.						
8	ГИС ГМП		ГИС ГМП является информационной системой, предназначенной для размещения и получения информации об уплате физическими и юридическими лицами платежей за оказание государственных и муниципальных услуг, услуг, указанных в части 3 статьи 1 и части 1 статьи 9 настоящего Федерального закона, платежей, являющихся источниками формирования доходов	Размещение и получение информации об уплате физическими и юридическими лицами платежей за оказание государственных и муниципальных услуг, услуг	ЗАО «КСК технологии»	Финансовое управление администрации Приволжского района, МКУ "МФЦ. Управление делами"				

			бюджетов бюджетной системы Российской Федерации, а также иных платежей, в случаях, предусмотренных федеральными законами.							
9	СУФД		Предназначен для автоматизации производственных процессов Федерального казначейства по кассовому обслуживанию исполнения федерального бюджета, бюджетов субъектов РФ и бюджетов муниципальных образований, в части обеспечения информационного взаимодействия органов ФК с другими участниками бюджетного процесса	Обеспечение возможности удаленного online взаимодействия ДУБП, обслуживаемых в данных Органах ФК, с серверным ППО Портала, доступном через сети общего пользования. Кроме того, в Портале, развернутом в УФК, будет осуществляться обслуживание ДУБП подчиненных ОФК.	ОТР Центр Технического Обслуживания	Финансовое управление администрации Приволжского района; МКУ «ОКМСиТ», МКУ "МФЦ. Управление делами"				

10	Электронный бюджет		Электронный бюджет" предназначен для обеспечения прозрачности, открытости и подотчетности деятельности государственных органов и органов управления государственными внебюджетными фондами, органов местного самоуправления, государственных и муниципальных учреждений, а также для повышения качества их финансового менеджмента за счет формирования единого информационного пространства и применения информационных и телекоммуникационных технологий в сфере управления государственными и муниципальными (общественными) финансами.	повышение доступности информации о финансовой деятельности и финансовом состоянии публично-правовых образований, государственных и муниципальных учреждений, об их активах и обязательствах;	Группа IBS	Финансовое управление администрации Приволжского района; МКУ «ОКМСиТ» Тихомирова Марина Владимировна Локтева Наталия Георгиевна				

11	ЕДИНОЙ ИНФОРМАЦИОННОЙ ИСТЕМЫ В СФЕРЕ ЗАКУПОК		Обеспечение свободного и безвозмездного доступа к полной и достоверной информации о контрактной системе в сфере закупок и закупках товаров, работ, услуг, отдельными видами юридических лиц, а также для формирования, обработки и хранения такой информации.		«Ланит»	Финансовое управление администрации Приволжского района				
12	ГАИС "Управление"		ГАИС «Управление» представляет собой единую государственную информационную систему, обеспечивающую сбор, учет, обработку и анализ данных, содержащихся в государственных и муниципальных информационных ресурсах, аналитических данных, данных официальной государственной статистики, а также иных сведений, необходимых для обеспечения поддержки принятия управленческих решений в сфере государственного управления. ГАС			Рысакова Надежда Витальевна Куликов Геннадий Валерьевич Говяжова Елена Николаевна Бучина Татьяна Анатольевна				

			«Управление» предназначена для устранения дублирующих потоков и запросов аналитической информации между органами государственной власти.							
13	Единая информационная система в сфере закупок		Предназначена для обеспечения свободного и безвозмездного доступа к полной и достоверной информации о контрактной системе в сфере закупок и закупках товаров, работ, услуг, отдельными видами юридических лиц, а также для формирования, обработки и хранения такой информации.			Отдел экономики и закупок, МКУ "МФЦ. Управление делами"				
14	Федеральная государственная информационная система		Единый реестр проверок содержит информацию о плановых и внеплановых проверках юридических лиц и индивидуальных предпринимателей, проводимых в			Бучина Татьяна Анатольевна				

	«Единый реестр проверок»		соответствии с Федеральным законом «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», иными федеральными законами, устанавливающими особенности организации и проведения проверок, и их результатах.							
15	Система удаленного финансового документооборота		СУФД-online представляет собой WEB-приложение, доступное через Интернет, которое позволяет клиентам Федерального казначейства управлять своими платежами, финансовыми документами и иметь доступ к актуальной отчетности, сформированной в автоматизированной системе Федерального казначейства (АСФК).			Тихомирова Марина Владимировна Локтева Наталия Георгиевна				
16	Система электронного		Организация хранения электронных документов, а также работы с ними.			Дремова Наталья Ивановна				

	документооборота									
17	Официальный сайт Российской Федерации для размещения информации о проведении торгов					Отдел Экономики и закупок, МКУ "МФЦ. Управление делами", КУМИ				
18	Региональная государственная информационная система «Региональный реестр государственных и муниципальных услуг (функци		Предназначена для информирования физических и юридических лиц: о государственных и муниципальных услугах; государственных функциях по контролю и надзору; об органах государственной власти об органах местного самоуправления			Рысакова Надежда Витальевна				

	й)»									
19	Сетевой справочный телефонный узел (ССТУ.РФ)		Портал по работе с обращениями граждан.			Ткачева Алена Вадимовна				
20	Государственная информационная система жилищно-коммунального хозяйства		ГИС ЖКХ – это единая федеральная централизованная информационная система, функционирующая на основе программных, технических средств и информационных технологий, обеспечивающих сбор, обработку, хранение, предоставление, размещение и использование информации о жилищном фонде, стоимости и перечне услуг по управлению общим			Румянцева Елена Валерьевна				

			имуществом в многоквартирных домах, работ по содержанию и ремонту общего имущества в многоквартирных домах, предоставлении коммунальных услуг и поставке ресурсов, необходимых для предоставления коммунальных услуг, размере платы за жилое помещение и коммунальные услуги, задолженности по указанной плате, объектах коммунальной и инженерной инфраструктур, а также иной информации, связанной с жилищно-коммунальным хозяйством.							
21	Интернет-портал «ГИС Энергоэффективность»		Официальный информационный портал по энергосбережению, часть государственной информационной системы (ГИС) «Энергоэффективность», площадка для раскрытия информации в рамках федерального			Галочкина Любовь Брониславовна				

			законодательства.							
22	Система межведомственного электронного взаимодействия		Информационная система, которая позволяет федеральным, региональным и местным органам власти, кредитным организациям (банкам), негосударственным пенсионным фондам, и прочим участникам СМЭВ обмениваться данными, необходимыми для оказания государственных услуг гражданам и организациям, в электронном виде.			Сабирова Екатерина Александровна Макаров Юрий Геннадьевич Сухарева Лариса Александровна				
23	Федеральная информационная адресная система		Федеральная информационная адресная система (ФИАС) содержит достоверную единообразную и структурированную адресную информацию по территории Российской Федерации, доступную для использования органами			Кудряшов Сергей Михайлович				

			государственной власти, органами местного самоуправления, физическими и юридическими лицами.							
24	Система удаленного финансового документооборота		Организация хранения электронных документов, а также работы с ними.			Соколова Ирина Николаевна Белова Александра Владимировна				
25	Региональная государственная информационная система «Региональный реестр государственных и муниципальных услуг (функций)»		Предназначена для информирования физических и юридических лиц: о государственных и муниципальных услугах; государственных функциях по контролю и надзору; об органах государственной власти об органах местного самоуправления			Стрижова Марина Вадимовна Кудряшова Ирина Николаевна				

26	Единая информационная система в сфере закупок		Предназначена для обеспечения свободного и безвозмездного доступа к полной и достоверной информации о контрактной системе в сфере закупок и закупках товаров, работ, услуг, отдельными видами юридических лиц, а также для формирования, обработки и хранения такой информации.			МКУ "МФЦ. Управление делами"; МКУ «ОКМСиТ»				

27	СКУД Biosmart studio		Предназначено для управления, контроля и конфигурирования СКУД BioSmart, системы учета рабочего времени, мониторинга и хранения событий системы.	- регистрация пользователей в СКУД BioSmart, ввод персональной информации, регистрация кодов карт, отпечатков пальцев, вен ладоней; - назначение пользователям сценариев доступа, временных режимов доступа; - просмотр событий идентификации пользователей в реальном времени, мнемосхема помещений (Модуль Мониторинг); - просмотр и формирование отчетов по архивным событиям, поиск событий, составление отчетов; - создание отчетов по рабочему времени (более 30 различных видов отчетов), конструктор отчетов (Модуль Work Time); - создание и		Электронная проходная администрации Приволжского муниципального района				

				просмотр дизайна пропусков RFID карт (Модуль Дизайнер пропусков); - конфигурирование системы, настройка оборудования; - планировщик задач (рассылка SMS сообщений, уведомлений, сценарий работы устройств СКУД, автоматическое создание отчетов и отправка их по e-mail); - интеграция с системами видеонаблюдения (Модуль Мониторинг); - экспорт журналов, отчетов в форматах Excel, pdf, html;						
28	bus.gov.ru		Официальный сайтдля размещения информации о государственных (муниципальных) учреждениях			Отделы и комитеты администрации Приволжского муниципального района				

29	Единая система идентификации и аутентификации		Единая система идентификации и аутентификации (ЕСИА) — информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах.			Отдел экономики и закупок, МКУ "МФЦ.Управление делами"				

Приложение №13
к Постановлению
администрации Приволжского
муниципального района
от 28.01.2014 г. №38-п

Типовые обязанности пользователей при обработке персональных данных в автоматизированных информационных системах, используемых в администрации Приволжского муниципального района

1. При обработке персональных данных в автоматизированных информационных системах (далее – АИС) администрации Приволжского муниципального района обязаны:

- знать и соблюдать ограничения, связанные с обработкой персональных данных;
- знать и соблюдать правила работы с персональными компьютерами (далее – ПК) и другими средствами вычислительной техники, правила работы в локальной и корпоративной вычислительных сетях;
- знать и соблюдать меры по защите персональных данных в АИС;
- знать и исполнять требования эксплуатационной документации на АИС;
- при работе с АИС выполнять только служебные задания, только в рабочее время;
- при работе использовать только учтенные в установленном порядке внешние носители (дискеты, флэш-карты и т.п.);
- перед началом работы на ПК проверить свои рабочие папки на жестком магнитном диске, рабочие внешние носители информации на отсутствие вирусов с помощью штатных средств антивирусной защиты, убедиться в исправности ПК. При необходимости использования внешних носителей, поступивших из других структурных подразделений, сторонних организаций, прежде всего, провести проверку этих носителей на отсутствие вирусов. При сообщениях тестовых программ о появлении вирусов немедленно прекратить работу, доложить непосредственному руководителю;
- при невозможности самостоятельно устранить возникшие трудности, руководитель докладывает руководителю МКУ «МФЦ.Управление делами», обеспечивающего техническую поддержку ПК;
- представлять для контроля за выполнением правил по защите персональных данных свой ПК технику-программисту МКУ «МФЦ.Управление делами», обеспечивающему техническую поддержку ПК;
- сохранять в тайне свой индивидуальный пароль, периодически изменять его и не сообщать другим лицам. Вводить пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;
- располагать дисплей таким образом, чтобы исключить несанкционированное ознакомление лиц, не допущенных к обработке персональных данных, с отображаемыми сведениями;

- при обнаружении различных неисправностей в работе компьютерной техники или локальной вычислительной сети, недокументированных свойств в программном обеспечении, нарушений целостности пломб (наклеек, печатей), несоответствия номеров на аппаратных средствах сообщить непосредственному руководителю.

2. Пользователю при работе запрещается:

- предоставлять свой ПК в пользование другим работникам, посторонним лицам, кроме случаев, связанных с техническим обслуживанием техническими специалистами, осуществляющими эксплуатацию средств информатизации;
- передавать другим лицам персональные пароли;
- самостоятельно устанавливать компьютерные программы на свой ПК;
- перенастраивать программное обеспечение ПК;
- самостоятельно вскрывать ПК и другие средства вычислительной техники;
- запускать на своем ПК любые системные или прикладные программы, кроме установленных техническими специалистами, осуществляющими эксплуатацию средств информатизации;
- изменять или копировать файл, принадлежащий другому пользователю, не получив предварительно разрешения владельца файла;
- оставлять включенным без присмотра свой ПК, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было в доступном для других лиц месте свое персональное устройство идентификации (при наличии), машинные носители и распечатки, содержащие персональные данные;
- производить копирование защищаемой информации на неучтенные носители;
- отсылать по электронной почте информацию, не связанную с исполнением служебных обязанностей, а также информацию по просьбе третьих лиц без согласования с руководителем структурного подразделения;
- запрашивать и получать из сети «Интернет» материалы развлекательного характера (игры, клипы и т.д.), кроме случаев их использования в служебных целях (только по согласованию с руководителем структурного подразделения);
- запрашивать и получать из сети «Интернет» программные продукты, базы данных, обновления программных продуктов и баз данных, кроме случаев, связанных с исполнением служебных обязанностей;
- входить в другие компьютерные системы через локальную сеть без разрешения операторов этих систем и предоставления допуска в установленном порядке;
- использовать в личных целях сведения конфиденциального характера, ставшие известными вследствие выполнения служебных обязанностей.

Приложение №14
к Постановлению
администрации Приволжского
муниципального района
от 28.01.2014 г. №38-п

ИНСТРУКЦИЯ
по организации антивирусной защиты в администрации Приволжского муниципального района

1. Общие положения

1.1. Компьютерный вирус является разрушающей программной закладкой и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на компьютерах и магнитных носителях. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать хранящуюся в компьютере и магнитных носителях информацию, при этом также могут пострадать аппаратные средства.

1.2. Основными путями вирусного вторжения являются неквалифицированное обращение пользователей с компьютерной техникой при использовании ими зараженных дискет, съемных носителей (карт памяти) и сети «Интернет», либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов.

2. Порядок, обеспечивающий безопасную работу на компьютере и с магнитными носителями

2.1. Установка и техническая поддержка персональных компьютеров (далее – ПК) производится МКУ «МФЦ. Управление делами», обеспечивающим техническую поддержку ПК.

2.2. Каждый компьютер решением руководителя персонально закрепляется за ответственным за его эксплуатацию подготовленным работником.

2.3. Допуск работников к самостоятельной работе на компьютерах и с внешними носителями осуществляется только после овладения ими навыками работы с компьютером, антивирусными пакетами программ.

2.4. На компьютерах может использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности. Запрещается использовать на компьютерах программные и аппаратные средства, не предназначенные для выполнения служебной деятельности.

2.5. На любом работающем компьютере в обязательном порядке должен быть установлен и активирован пакет антивирусных программ. Ответственность за это несет конкретный, отвечающий за его работоспособность работник, а также МКУ «МФЦ. Управление делами», обеспечивающее техническую поддержку ПК.

2.6. Периодически, не реже 1 раза в неделю, работник, ответственный за компьютер, проверяет его дисковое пространство с использованием антивирусного пакета программ на возможное наличие компьютерного вируса.

2.7. Пользователь обязан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируемые/разархивируемые файлы и т.д.), получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях (магнитных дисках, оптических носителях, Flash — память и т.п.).

2.8. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- провести лечение или уничтожение зараженных файлов (при невозможности выполнения требований данного пункта самостоятельно, привлечь техника-программиста МКУ «МФЦ. Управление делами»).

3. Ответственность

3.1. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на пользователя ПК.

3.2. Пользователь несет ответственность за качество и своевременность выполнения задач и функций, возложенных на него в соответствии с настоящей Инструкции.

Приложение №15
к Постановлению
администрации Приволжского
муниципального района
от 28.01.2014 г. №38-п

Перечень
угроз безопасности персональных данных в информационных системах, эксплуатируемых в администрации Приволжского муниципального района

Настоящее приложение определяет перечень угроз безопасности персональных данных (далее – УБ ПДн), актуальных при обработке персональных данных (далее ПДн) в информационных системах персональных данных (далее ИСПДн), эксплуатируемых в администрации Приволжского муниципального района при осуществлении ими соответствующих видов деятельности, с учетом содержания ПДн, характера и способов их обработки.

1. Основные УБ ПДн в ИСПДн.

Основными группами УБ ПДн в ИСПДн являются:

- угрозы утечки информации по техническим каналам;
- угрозы использования штатных средств ИСПДн с целью совершения несанкционированного доступа (далее-НСД) к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы недекларированных возможностей (далее-НДВ) в системном программном обеспечении (далее – СПО) и прикладном программном обеспечении (далее – ППО);
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;
- угрозы, связанные с использованием облачных услуг;
- угрозы, связанные с использованием суперкомпьютерных технологий;
- угрозы, связанные с использованием технологий виртуализации;
- угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- угрозы, связанные с нарушением процедур установки/обновления

программного обеспечения и оборудования;

- угрозы физического доступа к компонентам ИСПДн;
- угрозы эксплуатации уязвимостей в СПО, ППО, средств защиты информации (далее- СЗИ), средств криптографической защиты (далее – СКЗИ), аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- угрозы, связанные с использованием сетевых технологий;
- угрозы инженерной инфраструктуры;
- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- угрозы, связанные с контролем защищенности ИСПДн;
- угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

2. Актуальные УБ ПДн в ИСПДн

1. Информационно-справочные ИСПДн.

На официальном сайте администрации Приволжского муниципального района:

- угрозы утечки информации по техническим каналам;
- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы НДВ в СПО и ППО;
- угрозы, не являющиеся атаками;
-угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;
- угрозы, связанные с использованием облачных услуг;
- угрозы, связанные с использованием технологий виртуализации;
- угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- угрозы физического доступа к компонентам ИСПДн;
- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- угрозы, связанные с использованием сетевых технологий;
- угрозы инженерной инфраструктуры;

- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- угрозы, связанные с контролем защищенности ИСПДн;
- угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

На закрытых порталах для нескольких групп участников:
- угрозы утечки информации по техническим каналам;
- Угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы НДВ в СПО и ППО;
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;
- угрозы, связанные с использованием облачных услуг;
- угрозы, связанные с использованием технологий виртуализации;
- угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- угрозы физического доступа к компонентам ИСПДн;
- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- угрозы, связанные с использованием сетевых технологий;
- угрозы инженерной инфраструктуры;
- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- угрозы, связанные с контролем защищенности ИСПДн;
- угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

На служебных ИСПДн:

ИСПДн бухгалтерского учета и управления финансами.
- угрозы утечки информации по техническим каналам;
- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;

- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы НДВ в СПО и ППО;
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;
- угрозы, связанные с использованием технологий виртуализации;
- угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- угрозы физического доступа к компонентам ИСПДн;
- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- угрозы, связанные с использованием сетевых технологий;
- угрозы инженерной инфраструктуры;
- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- угрозы, связанные с контролем защищенности ИСПДн;
- угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

ИСПДн кадрового учета и управления персоналом.
- угрозы утечки информации по техническим каналам;
- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы НДВ в СПО и ППО;
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;

- угрозы программно-математических воздействий;
- угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- угрозы физического доступа к компонентам ИСПДн;
- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- угрозы, связанные с использованием сетевых технологий;
- угрозы инженерной инфраструктуры;
- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- угрозы, связанные с контролем защищенности ИСПДн;
- угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

ИСПДн документооборота и делопроизводства.
- угрозы утечки информации по техническим каналам;
- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы НДВ в СПО и ППО;
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;
- угрозы, связанные с использованием технологий виртуализации;
- угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- угрозы физического доступа к компонентам ИСПДн;
- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- угрозы, связанные с использованием сетевых технологий;
- угрозы инженерной инфраструктуры;
- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

- угрозы, связанные с контролем защищенности ИСПДн;
- угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

ИСПДн поддерживающие:
- угрозы утечки информации по техническим каналам;
- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы НДВ в СПО и ППО;
- угрозы, не являющиеся атаками;
-угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;
- угрозы, связанные с использованием технологий виртуализации;
- угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- угрозы физического доступа к компонентам ИСПДн;
- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- угрозы, связанные с использованием сетевых технологий;
- угрозы инженерной инфраструктуры;
- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- угрозы, связанные с контролем защищенности ИСПДн;
- угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

ИСПДн интеграционные:
- угрозы утечки информации по техническим каналам;
- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы НДВ в СПО и ППО;
- угрозы, не являющиеся атаками;

- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;
- угрозы, связанные с использованием технологий виртуализации;
- угрозы, связанные с нарушением правил эксплуатации машинных носителей;
- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;
- угрозы физического доступа к компонентам ИСПДн;
- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;
- угрозы, связанные с использованием сетевых технологий;
- угрозы инженерной инфраструктуры;
-угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;
- угрозы, связанные с контролем защищенности ИСПДн;
- угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.

ИСПДн многопрофильные:

- угрозы утечки информации по техническим каналам;
- угрозы использования штатных средств ИСПДн с целью совершения НСД к информации;
- угрозы нарушения доступности информации;
- угрозы нарушения целостности информации;
- угрозы НДВ в СПО и ППО;
- угрозы, не являющиеся атаками;
- угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации;
- угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом;
- угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИСПДн/системы защиты ИСПДн;
- угрозы ошибочных/деструктивных действий лиц;
- угрозы нарушения конфиденциальности;
- угрозы программно-математических воздействий;
- угрозы, связанные с использованием технологий виртуализации;
- угрозы, связанные с нарушением правил эксплуатации машинных носителей;

- угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования;

- угрозы физического доступа к компонентам ИСПДн;

- угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении;

- угрозы, связанные с использованием сетевых технологий;

- угрозы инженерной инфраструктуры;

- угрозы, связанные с отсутствием системы регистрации событий информационной безопасности;

- угрозы, связанные с контролем защищенности ИСПДн;

- угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи.