

ПЛАН МЕРОПРИЯТИЙ

по обеспечению безопасности защищаемой информации,
выполнению требований законодательства по защите
информации, а также по контролю уровня защищенности
и выполнения мер по защите информации в
ГИС «Бухгалтерия и кадры»

Разовые мероприятия

№ п/п	Наименование мероприятия	Исполнитель/ Ответственный/ Срок выполнения	Отметка о выполнении	Примечание
1.	Назначение ответственных за защиту информации в МКУК «Центр досуга»(или: Создание подразделения по защите информации в МКУК «Центр досуга»			
2.	Формирование комиссии по классификации ГИС «Бухгалтерия и кадры»			
3.	Анализ актуальных угроз безопасности информации в ГИС «Бухгалтерия и кадры» и разработка документа «Модель угроз», содержащего, в том числе модель, нарушителя			
4.	Оформление и направление в территориальный орган уполномоченного органа по защите прав субъектов персональных данных уведомления об обработке персональных данных			
5.	Классификация ГИС «Бухгалтерия и кадры», разработка акта классификации			
6.	Формирование группы реагирования на инциденты информационной безопасности в МКУК «Центр досуга»			
7.	Разработка и утверждение инструкции по реагированию на инциденты информационной безопасности в МКУК «Центр досуга»			
8.	Разработка и утверждение правил использования средств криптографической защиты			

№ п/п	Наименование мероприятия	Исполнитель/ Ответственный/ Срок выполнения	Отметка о выполнении	Примечание
	информации в МКУК «Центр досуга»			
9.	Разработка, утверждение и публикация для публичного доступа документа «Политика в отношении обработки персональных данных»			
10.	<p>Разработка и утверждение инструкции пользователя ГИС «Бухгалтерия и кадры», содержащей:</p> <ul style="list-style-type: none"> • общие обязанности пользователя по защите информации; • правила управления идентификаторами, учетными записями и паролями; • противодействие методам социальной инженерии и правила работы с электронной почтой; • правила работы со съемными носителями информации 			
11.	<p>Разработка и утверждение политики информационной безопасности в МКУК «Центр досуга», содержащей:</p> <ul style="list-style-type: none"> • перечень сведений конфиденциального характера, обрабатываемых в МКУК «Центр досуга» • описание технологических процессов обработки защищаемой информации в информационных системах МКУК «Центр досуга» • правила и процедуры идентификации и аутентификации пользователей информационных систем МКУК «Центр досуга»}; • правила разграничения доступа к ресурсам информационных систем МКУК «Центр досуга» 			

№ п/п	Наименование мероприятия	Исполнитель/ Ответственный/ Срок выполнения	Отметка о выполнении	Примечание
	<ul style="list-style-type: none"> • правила и процедуры управления информационными потоками; • правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения; • правила защиты машинных носителей информации, контроля интерфейсов ввода-вывода и гарантированного уничтожения информации; • правила взаимодействия информационных систем МКУК «Центр досуга» с внешними информационными системами • правила и процедуры обеспечения доверенной загрузки средств вычислительной техники • правила и процедуры применения удаленного доступа к информационным системам МКУК «Центр досуга» • правила и процедуры обнаружения (предотвращения) вторжений {K2+}; • правила и процедуры выявления, анализа и устранения уязвимостей; • правила и процедуры контроля установки обновлений программного обеспечения; • правила и процедуры контроля состава технических средств, программного обеспечения и средств защиты информации; • правила и процедуры 			

№ п/п	Наименование мероприятия	Исполнитель/ Ответственный/ Срок выполнения	Отметка о выполнении	Примечание
	<p>контроля целостности программного обеспечения {K2+};</p> <ul style="list-style-type: none"> • правила и процедуры резервирования технических средств, программного обеспечения, баз данных, средств защиты информации и их восстановления при возникновении нештатных ситуаций; • правила использования электронной почты и защиты от спама {K2+}; • правила и процедуры контроля использования технологий мобильного кода {K2+}; • ролевую систему доступа к ресурсам информационных систем МКУК «Центр досуга»; • перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами информационных систем МКУК «Центр досуга»; • перечень лиц, допущенных в помещения, в которых производится обработка конфиденциальной информации; • перечень статических сетевых маршрутов; • список разрешающих правил взаимодействия с внешними телекоммуникационными сетями; • список разрешенного программного обеспечения. 			
12.	<p>Формирование требований к системе защиты информации и разработка документа «Техническое задание на создание системы защиты информации в ГИС</p>			

№ п/п	Наименование мероприятия	Исполнитель/ Ответственный/ Срок выполнения	Отметка о выполнении	Примечание
	«Бухгалтерия и кадры»			
13.	Проектирование системы защиты информации и разработка документа «Эскизный проект системы защиты информации в ГИС «Бухгалтерия и кадры»			
14.	Организация контролируемой зоны и утверждение положения «О контролируемой зоне»			
15.	Закупка необходимых сертифицированных средств защиты информации			
16.	Реализация проекта системы защиты информации (установка и настройка средств защиты информации)			
17.	Первичная аттестация ГИС «Бухгалтерия и кадры»			
18.	Ввод ГИС «Бухгалтерия и кадры» в эксплуатацию на основании аттестата соответствия			

Контролирующие и периодические мероприятия

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
Документирование					
1.	Контроль наличия согласий на обработку персональных данных субъектов персональных данных, чьи ПДн обрабатываются в МКУК «Центр досуга»	Ответственный за организацию обработки ПДн	Вручную	Ежеквартально	
2.	Контроль наличия соглашений о неразглашении конфиденциальной информации, подписанных сотрудниками, допущенными к	Ответственный за организацию обработки ПДн	Вручную	Ежеквартально	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	обработке такой информации				
3.	Контроль актуальности внутренней документации по защите информации, в том числе списков лиц, допущенных к обработке конфиденциальной информации	Ответственный за организацию обработки ПДн, Администратор безопасности	Вручную	Ежеквартально либо при существенном изменении законодательства в сфере защиты информации	
4.	Контроль наличия актуальных договоров с организациями, которым передаются персональные данные, а также наличия в этих договорах пунктов, регламентирующих обязанность этих организаций обеспечивать конфиденциальность персональных данных	Ответственный за организацию обработки ПДн	Вручную	Каждые полгода	
5.	Пересмотр актуальных угроз безопасности и актуализация документа «Модель угроз безопасности информации»	Администратор безопасности	Вручную	Ежегодно, либо при изменении нормативной документации в сфере моделирования угроз безопасности информации, либо при поступлении информации о новых угрозах, актуальных для информационных систем МКУК «Центр досуга»	
6.	Повторная аттестация ГИС «Бухгалтерия и кадры»	Организация-лицензиат ФСТЭК России,	Согласовывается в документе «Программа и	1 раз в 5 лет, либо при существенном изменении	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
		привлекаема я для проведения аттестационных испытаний	методики аттестационных испытаний»	структурно-функциональных характеристик ГИС «Бухгалтерия и кадры»	
Информирование и обучение персонала					
7.	Доведение до персонала информации о новых угрозах информационной безопасности	Администратор безопасности	Устные лекции, информирование по каналам электронной почты	Не реже 1 раза в месяц	
8.	{ПДн} Доведение до персонала положений законодательства в сфере защиты персональных данных	Ответственный за организацию обработки ПДн	Устные лекции, информирование по каналам электронной почты	Не реже 1 раза в квартал	
9.	Доведение до персонала положений внутренних нормативных документов по защите информации	Администратор безопасности Ответственный за организацию обработки ПДн	Устно	По мере появления новых внутренних документов или по мере существенного изменения старых	
10.	Повышение квалификации и переподготовка лиц, ответственных за защиту информации в МКУК «Центр досуга» на курсах по направлению «Информационная безопасность» (не менее 72 часов)	Отдел кадров	Планирование учебных курсов	Не реже 1 раза в 5 лет	Учебные курсы должны быть согласованы со ФСТЭК России
11.	Проверка осведомленности персонала в сфере защиты информации	Администратор безопасности Ответственный за организацию обработки ПДн	Устный опрос, письменное тестирование, имитация действий злоумышленника	Ежеквартально	
Физический контроль					

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
12.	Осмотр серверного помещения на предмет несанкционированного доступа, нарушения пломб, физического воздействия и внедрения неучтенных технических средств	Администратор безопасности	Визуальный осмотр	Ежедневно	
13.	Выборочный осмотр рабочих мест пользователей на предмет несанкционированного доступа, нарушения пломб, физического воздействия и внедрения неучтенных технических средств	Администратор безопасности	Визуальный осмотр	Ежедневно	
Тестирование работоспособности средств защиты информации					
14.	Контроль актуальности антивирусных баз	Администратор безопасности	Kaspersky Security Center	Ежедневно	
15.	{K2+} Контроль актуальности баз решающих правил средства обнаружения вторжений	Администратор безопасности	ViPNet IDS 2.0	Ежемесячно	
16.	Контроль актуальности баз уязвимостей	Администратор безопасности	XSpider 7.8.24	Еженедельно	
17.	Контроль корректной работы запрещающих правил межсетевого экрана	Администратор безопасности	Браузер, командная строка	Еженедельно	
18.	Контроль корректности разграничения прав доступа к ресурсам ГИС	Администратор безопасности	ОС Windows, 1С:Предприятие 8, Dallas Lock 8.0-K	Ежемесячно	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	«Бухгалтерия и кадры»				
19.	{K2+} Контроль работоспособности и средств доверенной загрузки путем имитации попыток загрузки технического средства со стороннего носителя	Администратор безопасности	Загрузочный USB-накопитель	Ежемесячно	
20.	Контроль корректной работы подсистемы гарантированного уничтожения информации	Администратор безопасности	Утилиты восстановления удаленной информации (R.Saver и аналоги)	Ежеквартально, либо при передаче учетных съемных носителей между пользователями, либо при утилизации/передаче на ремонт технических средств с машинными носителями информации	
21.	Тестирование на проникновение в ГИС «Бухгалтерия и кадры»	Администратор безопасности, организация-лицензиат ФСТЭК России	Инструменты дистрибутива Kali Linux 2.0	Ежеквартально	
Контроль программного обеспечения и технических средств ИС					
22.	Контроль отсутствия у пользователей на рабочих местах средств разработки и технологий интерпретации мобильного кода (кроме пользователей, которым это необходимо для выполнения своих	Администратор безопасности	XSpider 7.8.24, ручной выборочный контроль	Ежемесячно	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	должностных обязанностей)				
23.	Контроль наличия необходимых обновлений безопасности общесистемного и прикладного программного обеспечения	Администратор безопасности	XSpider 7.8.24, ручной выборочный контроль	Еженедельно	
24.	Контроль отсутствия в ГИС «Бухгалтерия и кадры» посторонних технических средств	Администратор безопасности, пользователи ГИС	Max Patrol, визуальный осмотр	Еженедельно	
25.	Контроль отсутствия в ГИС «Бухгалтерия и кадры» неразрешенного программного обеспечения	Администратор безопасности	Max Patrol	Еженедельно	
Пользователи, учетные записи, парольная политика					
26.	Заведение, удаление учетных записей пользователей. Наделение, лишение, изменение полномочий пользователей по доступу к ресурсам ГИС «Бухгалтерия и кадры»	Администратор безопасности	Active Directory	По мере поступления заявок на заведение/удаление учетных записей и наделение/изменение полномочий в системе	
27.	Мониторинг учетных записей на предмет выявления неблокированных временных учетных записей или учетных записей уволенных сотрудников	Администратор безопасности	Active Directory	Еженедельно	
28.	Мониторинг сессий удаленных	Администратор	Dallas Lock 8.0-K	Ежедневно	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	пользователей	безопасности			
29.	Мониторинг сессий внешних пользователей	Администратор безопасности	Dallas Lock 8.0-K	Ежедневно	
30.	Смена собственного пароля и мониторинг своевременной смены паролей других привилегированных пользователей	Администратор безопасности	Dallas Lock 8.0-K	Каждые 90 суток	
31.	Мониторинг своевременной смены паролей пользователями ГИС «Бухгалтерия и кадры»	Администратор безопасности	Dallas Lock 8.0-K	Ежедневно	
32.	Смена паролей доступа к интерфейсам управления сетевыми устройствами (коммутаторами, маршрутизаторами)	Администратор безопасности	Вручную	Каждые 90 суток	
Беспроводные каналы передачи данных {удалить раздел, если нет таких}					
33.	Мониторинг настроек беспроводных точек доступа на предмет включенных уязвимых функций	Администратор безопасности	Вручную	Ежемесячно	
34.	Мониторинг доступности беспроводного сигнала за пределами контролируемой зоны	Администратор безопасности	Любое мобильное устройство с модулями беспроводной связи	Еженедельно	
35.	Мониторинг отсутствия поддельных точек доступа, маскирующихся под легальные точки доступа МКУК «Центр	Администратор безопасности	Любое мобильное устройство с модулями беспроводной связи	Ежедневно	

№ п/п	Наименование мероприятия	Ответственный	Процедуры / инструменты, применяемые для выполнения мероприятия	Периодичность	Примечание
	досуга»				
Отказоустойчивость					
36.	Резервное копирование информации	Администратор безопасности	Veeam backup & recovery, вручную	В соответствии с утвержденной политикой информационной безопасности	
37.	Контроль целостности резервных копий	Администратор безопасности	Dallas Lock 8.0-K	Ежемесячно	

Директор:  М.В. Холоденко

