УТВЕРЖДАЮ
Зам. директора по УПР
ГПОУ «УМК»
_____ Е.Д. Канева
25.09.2016

ПЛАН МЕРОПРИЯТИЙ

по обеспечению безопасности персональных данных
в ГПОУ «УМК» на 2016 год

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	– автоматизированное рабочее место;
БД	– база данных;
ИСПДн	– информационная система персональных данных;
Комиссия	– постоянно действующая комиссия по защите персональных данных;
ЛВС	– локальная вычислительная сеть;
ЛНА	– локальные нормативные акты;
МНИ	– машинные носители информации;
НСД	– несанкционированный доступ;
ОС	– операционная система;
ПДн	– персональные данные;
ПО	– программное обеспечение;
САВЗ	– средства антивирусной защиты;
СВТ	– средства вычислительной техники;
СЗИ	– средства защиты информации;
СЗПДн	– система защиты персональных данных;
ТС	– технические средства;
УБПДн	– угрозы безопасности персональных данных;
Учреждение	– ГПОУ «УМК».

ВВЕДЕНИЕ

План мероприятий по обеспечению безопасности ПДн разработан для обеспечения выполнения Учреждением обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О ПДн» и принятыми в соответствии с ним нормативными правовыми актами, в качестве оператора ПДн**.**

План разработан на основании результатов проведения внутренней проверки обработки ПДн, с учетом актуальных УБПДн, информационных технологий, используемых в ИСПДн Учреждения, а также принимаемых мер защиты и рекомендаций Комиссии.

Обеспечение выполнения Учреждением обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О ПДн» и принятыми в соответствии с ним нормативными правовыми актами осуществляется поэтапно:

I. Подготовительный этап.
II. Первоочередной этап.
III. Основной этап:
    1) базовые мероприятия;
    2) дополнительные мероприятия.
IV. Заключительный этап.

В план включены следующие категории мероприятий:

- организационные;
- физические и инженерные;
- технические (аппаратные и программные);
- контрольные.

В план включена следующая информация:

- название мероприятия;
- срок выполнения / периодичность;
- ответственное лицо;
- отметка о выполнении;
- примечание.

ПЛАН МЕРОПРИЯТИЙ

№ п/п	Мероприятие	Срок выполнения	Ответственный	Отметка о выполнении	Примечание
Этап I: Подготовительные организационные мероприятия					
1	Оформление и направление в территориальный орган уполномоченного органа по защите прав субъектов ПДн уведомления об обработке (о намерении осуществлять обработку) ПДн		Директор, Комиссия		Если не было отправлено ранее
2	Проведение инвентаризации СВТ, МНИ, мест хранения ПДн		Главный бухгалтер		
3	Проведение экспертизы лицензионности ПО		Техник-программист		С привлечением экспертной организации
4	Планирование мероприятий по обеспечению безопасности ПДн		Директор, Комиссия		Настоящий план
Этап II: Первоочередные организационные мероприятия					
5	Разработка или актуализация годового плана работы Комиссии		Комиссия		
6	Организация СЗПДн, включающей в себя организационные и (или) технические меры, определенные с учетом актуальных УБПДн и информационных технологи, используемых в ИСПДн		Директор, Комиссия		
7	Определение целей сбора, сроков хранения, состава и способов уничтожения обрабатываемых ПДн, принятие решения об отказе от сбора избыточных ПДн для заявленных целей обработки		Комиссия, руководители структурных подразделений		
8	Разработка или актуализация положения об обработке и защите ПДн		Комиссия		
9	Разработка, размещение на информационном стенде и публикация на официальном сайте политики в отношении обработки ПДн		Директор, Комиссия		
10	Проведение оценки возможного вреда, который может быть причинен субъектам ПДн в случае реализации актуальных УБПДн и (или) нарушения Учреждением Федерального закона от 27.07.2006 № 152-ФЗ «О ПДн»		Комиссия		
11	Определение необходимости обеспечения установленных Правительством РФ уровней защищенности ПДн при их обработке в ИСПДн Учреждения		Комиссия		

12	Проведение оценки достаточности принимаемых мер по обеспечению безопасности ПДн		Комиссия		
13	Определение состава и содержания мер по обеспечению безопасности ПДн, необходимых для обеспечения установленных Правительством РФ уровней защищенности ПДн при их обработке в ИСПДн Учреждения		Комиссия		
14	Разработка или актуализация перечня ИСПДн		Комиссия		
15	Сбор обязательств о неразглашении ПДн с работников Учреждения		Директор, Комиссия		
16	Организация получения согласий на обработку ПДн от субъектов ПДн		Комиссия		При необходимости
17	Определение порядка ведения журнальных форм СЗПДн		Комиссия		
Этап II: Первоочередные контрольные мероприятия					
18	Создание журнала учета ознакомлений с ЛНА и назначение ответственного за его ведение		Директор		При необходимости
19	Создание журнала учета мероприятий по контролю обеспечения безопасности ПДн и назначение ответственного за его ведение		Директор		
Этап II: Первоочередные физические и инженерные мероприятия					
20	Оснащение оконных проемов помещений, в которых осуществляется обработка ПДн, жалюзи или плотными шторами		Директор		
21	Оборудование входных дверей помещений, в которых осуществляется обработка ПДн, запираемыми замками		Директор		
22	Оборудование помещений, в которых осуществляется обработка ПДн, металлическими входными дверями		Директор, Комиссия		При необходимости
Этап III: Базовые организационные мероприятия					
23	Назначение ответственного за обеспечение работоспособности и функционирования ИСПДн		Директор		
24	Определение функций, обязанностей, полномочий и ответственности лица, ответственного за обеспечение работоспособности и функционирования ИСПДн		Директор		
25	Определение перечня должностей работников Учреждения, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн		Комиссия, руководители структурных подразделений		

26	Определение перечня лиц, участвующих в обработке ПДн с соответствующими полномочиями и правами		Комиссия		
27	Категорирование субъектов и объектов доступа в ИСПДн Учреждения. Разработка или актуализация положения о разграничении прав доступа к ресурсам ИСПДн		Комиссия		
28	Определение функций, обязанностей и ответственности пользователей ИСПДн		Комиссия		
29	Определение перечней прав доступа к ресурсам ИСПДн		Комиссия		
30	Актуализация используемых типовых форм		Комиссия		
31	Определение перечня помещений, в которых осуществляется обработка ПДн		Комиссия		
32	Организация и обеспечение контролируемой зоны вокруг ИСПДн и (или) помещений, в которых осуществляется обработка ПДн		Директор, Комиссия		
33	Организация порядка доступа в помещения, в которых осуществляется обработка ПДн		Комиссия		
34	Организация порядка учета, хранения и выдачи ключей от помещений, сейфов, шкафов		Комиссия		
35	Определение мест хранения ПДн и их материальных носителей		Директор, Комиссия		
36	Введение политики «чистого стола»		Комиссия		
37	Организация порядка резервного копирования ПДн		Комиссия		
38	Актуализация сведений об УБПДн		Комиссия		
39	Актуализация должностных инструкций работников Учреждения, обрабатывающих ПДн		Директор, Комиссия		
40	Утверждение типовых форм журналов учета и назначение ответственных за их ведение		Директор		
Этап III: Базовые контрольные мероприятия					
41	Контроль над соблюдением порядка обработки и защиты ПДн	Ежедневно	Комиссия		
42	Контроль над уничтожением ПДн и их материальных носителей	Ежеквартально	Комиссия		
43	Контроль над исполнением плана резервного копирования	Еженедельно	Комиссия		
44	Контроль над корректностью (целостностью) создаваемых резервных копий	Раз в 2 месяца	Ответственный за обеспечение работоспособнос		

			ти и функционирования ИСПДн		
45	Контроль исполнения обращений (запросов) субъектов ПДн	Ежемесячно	Комиссия		
Этап III: Базовые физические и инженерные мероприятия					
46	Расположение АРМ ИСПДн согласно требованиям безопасности (исключение возможности просмотра информации с мониторов АРМ посторонними лицами и техническими средствами)		Комиссия		
47	Установка входных перегородок (стоек), препятствующих проходу в помещения, в которых осуществляется обработка ПДн		Директор		При необходимости
48	Оснащение помещений, в которых осуществляется обработка ПДн, запираемыми шкафами, столами и сейфами для хранения материальных носителей ПДн		Директор		
49	Установка источников бесперебойного питания на ключевые элементы ИСПДн		Комиссия		
Этап III: Базовые технические мероприятия					
50	Анализ действующих настроек ОС АРМ и серверов ИСПДн. Настройка групповых (локальных) политик ОС АРМ и серверов ИСПДн в соответствии с установленными уровнями защищенности		Комиссия		Microsoft Windows
51	Анализ существующей маршрутизации в ЛВС Учреждения. Настройка активного сетевого оборудования ЛВС в соответствии с требованиями безопасности		Комиссия		
52	Аудит информационных ресурсов		Комиссия		TNI Audit
53	Настройка серверных служб и сервисов в соответствии с требованиями безопасности		Комиссия		
54	Организация замкнутой программной среды на АРМ ИСПДн		Комиссия		AppLocker
55	Настройка АРМ ИСПДн для работы только с учтенными МНИ		Комиссия		Групповые (локальные) политики ОС
56	Настройка средств удаленного администрирования (доступа) в соответствии с требованиями безопасности		Комиссия		
57	Анализ действующей системы резервного копирования. Повышение отказоустойчивости		Комиссия		Cobian backup 11, RAID
58	Введение политики «чистого экрана»		Комиссия		

59	Смена паролей пользователей ИСПДн	Ежеквартально			
Этап III: Дополнительные организационные мероприятия					
60	Анализ используемых СЗИ, соотнесение их возможностей с потребностями		Комиссия		
61	Оценка скоростных характеристик каналов связи (внутренних и внешних), составление карты скоростей		Комиссия		При необходимости
62	Разработка частного технического задания на создание СЗПДн (технические меры), с учетом выбранных мер по обеспечению безопасности ПДн, необходимых для обеспечения установленных Правительством РФ уровней защищенности ПДн при их обработке в ИСПДн Учреждения		Комиссия		С привлечением лицензиата ФСТЭК в области технической защиты конфиденциальной информации
63	Проектирование СЗПДн. Разработка эскизного проекта СЗПДн (технические меры)		Комиссия		С привлечением лицензиата ФСТЭК в области технической защиты конфиденциальной информации
64	Организация порядка антивирусной защиты		Комиссия		
65	Организация порядка парольной защиты		Комиссия		
66	Организация порядка обеспечения информационной безопасности в сфере информационного обмена		Комиссия		
67	Организация порядка резервирования и восстановления ТС и ПО, БД и СЗИ		Комиссия		
68	Организация порядка учета, хранения и уничтожения МНИ		Комиссия		
69	Организация порядка обеспечения безопасности ПДн в случае нештатных ситуаций		Комиссия		
70	Организация порядка предоставления ПДн и их материальных носителей		Комиссия		

71	Организация порядка реагирования на обращения (запросы) субъектов ПДн		Комиссия		
72	Заключение дополнительных соглашений о конфиденциальности к договорам, поручающим обработку ПДн контрагентам или к договорам, в соответствии с которыми Учреждение берет на себя обязательства по обработке ПДн		Директор, Комиссия		
73	Организация обучения работников Учреждения вопросам защиты ПДн		Комиссия		
74	Планирование финансирования внедрения СЗПДн (технические меры) и выполнения работ по защите ПДн		Директор, Комиссия, главный бухгалтер		
75	Оформление и направление в территориальный орган уполномоченного органа по защите прав субъектов ПДн уведомления об изменении сведений об операторе ПДн		Директор, Комиссия		
76	Оформление и направление в территориальный орган уполномоченного органа по защите прав субъектов ПДн запроса на получение выписки из реестра операторов, осуществляющих обработку ПДн		Директор, Комиссия		Если не было отправлено ранее
77	Разработка и подача заявки на закупку сертифицированных СЗИ		Директор, Комиссия, главный бухгалтер		
78	Разработка и согласование программы и методики испытаний СЗПДн (технические меры)		Комиссия		С привлечением лицензиата ФСТЭК в области технической защиты конфиденциальной информации
Этап III: Дополнительные контрольные мероприятия					
79	Проведение полной внутренней проверки условий обработки и защиты ПДн и выполнения требований законодательства РФ	Не реже 1 раза в 3 года	Комиссия		

80	Проведение внутренней проверки на предмет выявления изменений в порядке защиты и условиях обработки ПДн	Ежегодно	Комиссия		В случае изменения законодательства РФ в области ПДн
81	Проверка наличия материальных носителей ПДн (документов на бумажных носителях и МНИ)	Не реже 1 раза в год	Комиссия		
82	Контроль над обеспечением антивирусной защиты	Еженедельно	Комиссия		
83	Контроль над ведением журнальных форм СЗПДн	Раз в 6 месяцев	Комиссия		
84	Контроль установки ПО, не связанного с исполнением служебных (трудовых) обязанностей	Ежеквартально	Комиссия		
85	Создание журнала учета проверок знаний работников по вопросам защиты ПДн и назначение ответственного за его ведение		Директор		
86	Анализ и пересмотр актуальных УБПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	Комиссия		
87	Контроль актуальности состояния ЛНА, регламентирующих обработку и защиту ПДн	Раз в 6 месяцев	Комиссия		
88	Контроль над разработкой и внесением изменений в ПО собственной (заказной) разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями	Ежеквартально	Комиссия		
Этап III: Дополнительные физические и инженерные мероприятия					
89	Организация и обеспечение пропускного режима		Директор, Комиссия		При необходимости
90	Организация и обеспечение внутриобъектового режима		Директор, Комиссия		При необходимости
91	Внедрение технической системы контроля доступа в контролируемую зону и (или) помещения, в которых осуществляется обработка ПДн (по электронным пропускам, токену)		Директор, Комиссия		При необходимости
92	Внедрение системы видеонаблюдения. Обеспечение ее функционирования		Директор, Комиссия		При необходимости
93	Установка систем кондиционирования и (или) вентиляции воздуха в помещениях, в которых расположены ключевые элементы ИСПДн		Директор, Комиссия		При необходимости
Этап III: Дополнительные технические мероприятия					

94	Внедрение единого хранилища зарегистрированных действий пользователей ИСПДн с ПДн		Комиссия		
95	Внедрение подсистемы управления доступом, регистрации и учета. Установка и настройка сертифицированных СЗИ от НСД		Комиссия		
96	Внедрение подсистемы централизованной антивирусной защиты. Установка и настройка сертифицированных САВЗ, центра администрирования		Комиссия		
97	Внедрение подсистемы межсетевого экранирования. Установка и настройка сертифицированных межсетевых экранов		Комиссия		
98	Внедрение подсистемы обеспечения целостности ПО, файлов и программной среды. Установка сертифицированных средств контроля целостности		Комиссия		
99	Проведение приемо-сдаточных испытаний СЗПДн (технические меры) в соответствии с программой и методикой испытаний		Комиссия		С привлечением лицензиата ФСТЭК в области технической защиты конфиденциальной информации
Этап IV: Заключительные организационные мероприятия					
100	Ввод ИСПДн Учреждения в эксплуатацию		Директор, Комиссия		
101	Организация учета СЗИ, эксплуатационной и технической документации к ним		Комиссия		
102	Установка защитных пломб на системные блоки АРМ и серверов ИСПДн		Комиссия		
103	Разработка технических паспортов ИСПДн		Комиссия		
104	Декларирование (аттестация) соответствия защиты ПДн требованиям законодательства РФ в области ПДн		Комиссия		При необходимости
105	Обучение работников Учреждения порядку обработки ПДн в ИСПДн и работы с СЗИ		Комиссия		
106	Подготовка отчета о проделанной работе за текущий календарный год	До 1 февраля 2017 г.	Комиссия		

107	Разработка плана мероприятий на следующий календарный год	До 15 декабря 2016г.	Комиссия		
Этап IV: Заключительные контрольные мероприятия					
108	Контроль над системными журналами СЗПДн	Еженедельно	Комиссия		
109	Контроль над соблюдением порядка защиты ПДн при работе в ИСПДн (соблюдения политик безопасности)	Ежедневно	Комиссия		
110	Контроль состояния пломб на системных блоках АРМ и серверов ИСПДн	Ежеквартально	Комиссия		
111	Проведение внутренней проверки состояния СЗПДн	Не реже 1 раза в год	Комиссия		
112	Контроль над обновлением и единообразием используемого ПО, а также соответствием технического и программного состава АРМ техническим паспортам ИСПДн	Раз в 2 месяца	Ответственный за обеспечение работоспособности и функционирования ИСПДн		
Этап IV: Заключительные физические и инженерные мероприятия					
113	Установка металлических решеток на оконные проемы помещений, в которых осуществляется обработка ПДн, находящихся на первом и последнем этажах здания		Комиссия		При необходимости
Этап IV: Заключительные технические мероприятия					
114	Внедрение подсистемы аудита и категорирования посещаемых ресурсов		Комиссия		При необходимости
115	Внедрение подсистемы анализа защищенности. Установка и настройка сертифицированных средств анализа защищенности		Комиссия		При необходимости
116	Внедрение подсистемы обнаружения вторжений. Установка и настройка сертифицированных систем обнаружения вторжений		Комиссия		При необходимости
117	Внедрение подсистемы централизованного распространения обновлений		Комиссия		При необходимости