МИНИСТЕРСТВО ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ
СВЕРДЛОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СВЕРДЛОВСКОЙ ОБЛАСТИ «ЕКАТЕРИНБУРГСКАЯ ШКОЛА-ИНТЕРНАТ №10, РЕАЛИЗУЮЩАЯ АДАПТИРОВАННЫЕ ОСНОВНЫЕ ОБЩЕОБРАЗОВАТЕЛЬНЫЕ ПРОГРАММЫ»

ПРИКАЗ

07.11.2024 № 142-д

г. Екатеринбург

Об утверждении планов мероприятий по защите информации

В целях исполнения требований Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и организации работ по защите информации, не составляющей государственную тайну, требование о защите которой установлено законодательством Российской Федерации, нормативными правовыми актами Правительства Российской Федерации, при её обработке в государственном бюджетном общеобразовательном учреждении Свердловской области «Екатеринбургская школа-интернат № 10, реализующая адаптированные основные общеобразовательные программы» (далее - ГБОУ СО «ЕШИ № 10»),

ПРИКАЗЫВАЮ:

1. Утвердить план организационных и технических мероприятий по защите информации в ГБОУ СО «ЕШИ № 10», в соответствии с Приложением № 1.
2. Утвердить план проведения внутреннего контроля по обеспечению уровня защищенности информации в информационных системах ГБОУ СО «ЕШИ № 10» в соответствии с Приложением № 2.
3. Чухниной Е.А. – секретарю директора, довести настоящий приказ под подпись до сотрудников ГБОУ СО «ЕШИ № 10», ответственных за организацию и проведение работ по защите информации.
4. Контроль за выполнением требований настоящего приказа оставляю за собой.

Директор М.Д. Бузань

Отпечатано в ООО «Типография ситипринт», заказ № 230409, тираж 750

Приложение № 1
к приказу «Об утверждении планов
мероприятий по защите информации»
от «07» ноября 2024 г. № 142-д

УТВЕРЖДАЮ
_____ / М.Д. Бузань
приказ от «07» ноября 2024 г. № 142-д

План организационных и технических мероприятий по защите информации в ГБОУ СО «ЕШИ № 10»

№ п/п	Наименование мероприятия	Дата реализации мероприятия по плану	Сотрудники, привлекаемые к реализации	Фактический срок реализации мероприятия	Периодичность проведения мероприятия	Примечание
1	2	3	4	5	6	7
1	ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ					
1.1	Проведение инструктажа: – пользователей информационных систем (далее – ИС); – пользователей средств криптографической защиты информации (далее – СКЗИ).				При ротации сотрудников.	С отметкой в журналах: – учета пользователей, имеющих право доступа к ИС; – учета пользователей СКЗИ. С внесением изменений в Матрицу доступа пользователей к защищаемым информационным ресурсам ИС.
1.2	Утвердить перечень внутренних документов по защите информации.					—

1	2	3	4	5	6	7
1.3	Учет: – пользователей ИС; – пользователей СКЗИ.				При ротации сотрудников.	С отметкой в журналах: – учета пользователей, имеющих право доступа к ИС; – учета пользователей СКЗИ. С внесением изменений в Матрицу доступа пользователей к защищаемым информационным ресурсам ИС.
1.4	Ввести в рабочий процесс перечень внутренних документов по защите информации.					—
1.5	Внести в должностные инструкции пользователей ИС сведения: – об обработке информации ограниченного распространения в ходе исполнения функциональных обязанностей (при необходимости доступа к такой информации); – об ответственности за обеспечение защиты информации, предусмотренной законодательством Российской Федерации в сфере защиты информации.					—
1.6	Направление в Управление Федеральной службы по надзору в сфере связи, информационных технологий					—

1	2	3	4	5	6	7
	и массовых коммуникаций по Уральскому федеральному округу информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных.					
1.7	При изменении перечня программного обеспечения, в котором осуществляется обработка персональных данных и которое представляет собой базы данных, направление в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Уральскому федеральному округу информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных.					—
1.8	Организация учета и порядка сдачи ключей от: – помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой,					—

1	2	3	4	5	6	7
	аутентифицирующей и парольной информации СКЗИ; – хранилищ (предназначенных для хранения съемных машинных носителей информации, для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей).					
1.9	Для Помещений, в которых нет технических средств охраны, но которые оборудованы средствами опечатывания завести журналы опечатывания (вскрытия) помещений.					—
1.10	Для сейфов (предназначенных для хранения съемных машинных носителей информации, для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями					—

1	2	3	4	5	6	7
	для опечатывания замочных скважин ГБОУ СО «ЕШИ № 10», завести журналы опечатывания (вскрытия) хранилищ.					
1.11	Контроль содержания текстов договоров, предполагающих передачу персональных данных.					Такие договоры должны содержать пункты о соблюдении требований законодательства в части защиты персональных данных.
1.12	Контроль содержания текстов договоров, предполагающих передачу информации ограниченного распространения.					Такие договоры должны содержать пункты о соблюдении требований по защите информации (в том числе соблюдение конфиденциальности) при оказании услуг исполнителем по договору.
1.13	Контроль содержания текстов договоров, предполагающих техническое сопровождение программных продуктов и (или) технических средств, являющихся элементами ИС, а равно и доступ к программным и техническим элементам ИС.					—
1.14	Систематизация учетных записей для доступа к информационным ресурсам ИС.				При ротации сотрудников.	С внесением изменений в Матрицу доступа пользователей к защищаемым информационным ресурсам ИС.
1.15	Учет машинных носителей информации.				– при поступлении новых машинных носителей информации;	С отметкой в журнале учета машинных носителей информации.

1	2	3	4	5	6	7
					– при замене машинных носителей информации.	
1.16	Анализ необходимости оформления актов установки /актов деинсталляции средств защиты информации (далее – СЗИ), СКЗИ					—
1.17	Поэкземплярный учет СЗИ, эксплуатационной и технической документации к ним.				При приобретении/ установке новых СЗИ.	С отметкой в журнале поэкземплярного учета СЗИ ИС, эксплуатационной и технической документации к ним.
1.18	Поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.				При приобретении/ установке новых СКЗИ.	С отметкой в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.
1.19	Учет хранилищ и ключей от них.					С отметкой в журнале учета хранилищ и ключей от них.
1.20	Учет личных печатей, предназначенных для опечатывания помещений (хранилищ).					С отметкой в журнале учета личных печатей, предназначенных для опечатывания помещений (хранилищ).
1.21	Оформление актов установки и ввода в эксплуатацию СКЗИ.				При установке новых СКЗИ.	—
1.22	Оформление актов установки СЗИ.				При установке новых СЗИ.	—
1.23	Оформление заявок на предоставление сотруднику прав доступа к				При необходимости предоставления сотруднику прав доступа к	—

1	2	3	4	5	6	7
	информационным массивам ИС.				информационным массивам ИС.	
1.24	Учет выдачи паролей для доступа к ИС.				– при смене паролей; – при ротации сотрудников.	С отметкой в журнале учета выдачи паролей для доступа к ИС. С внесением изменений в Матрицу доступа пользователей к защищаемым информационным ресурсам ИС.
1.25	Учет инцидентов безопасности и нештатных ситуаций в ИС.				При возникновении нештатной ситуации в ИС. Если нештатные ситуации в течение одного квартала отсутствуют, производить запись в журнале об их отсутствии.	С отметкой в журнале учета нештатных ситуаций в ИС.
1.26	Обезличивание персональных данных.				при наступлении условий обезличивания персональных данных.	—
1.27	Уничтожение персональных данных.				При наступлении условий уничтожения персональных данных.	С составлением акта об уничтожении персональных данных.
1.28	Уничтожение машинных носителей информации.				При наступлении условий уничтожения машинных носителей информации.	С составлением акта об уничтожении машинных носителей информации.
1.29	Уничтожение материальных носителей информации ограниченного				При наступлении условий:	С составлением акта: – об уничтожении информации ограниченного распространения;

1	2	3	4	5	6	7
	распространения в т.ч. документов на бумажных носителях.				– уничтожения информации ограниченного распространения; – уничтожения материальных носителей.	– об уничтожении материальных носителей информации ограниченного распространения.
1.30	Информирование и обучение персонала по вопросам информационной безопасности.				С учетом сроков планового/внепланового/индивидуального обучения.	С отметкой в журнале проведения обучения и проверки знаний по вопросам информационной безопасности.
1.31	Актуализация плана мероприятий по защите информации.				– по представлению предложений от лиц, ответственных за защиту информации; – по результатам внутреннего контроля по обеспечению уровня защищенности информации в ИС.	—
2	ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ					
2.1	Контроль технического состояния и работоспособности технических средств охранной и пожарной сигнализации.				Один раз в неделю.	С отметкой в журнале проверки работы средств охранной сигнализации, размещенных в помещениях.
2.2	Проведение антивирусных проверок.				Один раз в неделю.	С отметкой в журнале учета антивирусных проверок ИС.
2.3	Проведение антивирусных проверок электронных архивов.				Один раз в месяц.	С отметкой в журнале учета антивирусных проверок ИС.

1	2	3	4	5	6	7
2.4	Резервное копирование информационных массивов ИС.				Один раз в месяц.	С отметкой в журнале резервного копирования информационных массивов ИС.
2.5	Проверка электронных журналов ИС.				Один раз в неделю.	С отметкой в журнале проверок электронных журналов ИС.
2.6	Смена паролей.				– плановая смена паролей: один раз в квартал; – внеплановая смена паролей: при наступлении условий, изложенных в Положения по организации и проведению работ по обеспечению безопасности защищаемой информации.	С отметкой в журнале учета выдачи паролей для доступа к ИС.
2.7	Управление конфигурацией ИС.				При изменении конфигурации ИС.	С отметкой в журнале регистрации действий по сопровождению ИС и изменению их конфигурации.
2.8	Периодическое тестирование функционирования СЗИ.				Один раз в месяц.	С отметкой в журнале учета периодического тестирования СЗИ ИС.
2.9	В случае изменений следующих сведений: – наименование, адрес юридического лица; – цели обработки персональных данных;					—

1	2	3	4	5	6	7
	– описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств; – фамилии, имени, отчества физического лица, ответственного за организацию обработки персональных данных, и номеров их контактных телефонов, почтовых адресов и адресов электронной почты; – даты начала обработки персональных данных; – срока или условия прекращения обработки персональных данных; – сведений о наличии или об отсутствии трансграничной передачи персональных данных в процессе обработки; – сведений об обеспечении безопасности персональных данных в соответствии с требованиями к защите					

1	2	3	4	5	6	7
	персональных данных, установленными Правительством Российской Федерации. Ответственные лица _____ _____ обязаны уведомлять об этом Управление Федеральной службы по надзору в сфере связи и массовых коммуникаций по Уральскому федеральному округу не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения (часть 7 ст. 22 Федерального закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ)					
2.10	Мероприятия по внутреннему контролю по обеспечению уровня защищенности информации в ИС в ГБОУ СО «ЕШИ № 10».				Один раз в полгода.	– с оформлением протокола/отчета о результатах внутреннего контроля за обеспечением уровня защищенности информации; – с отметкой в журнале учета проведения внутреннего контроля за обеспечением уровня защищенности информации.

Приложение № 2
к приказу «Об утверждении планов
мероприятий по защите информации»
от «07» ноября 2024 г. № 142-д

УТВЕРЖДАЮ
_____ / М.Д. Бузань
приказ от «07» ноября 2024 г. № 142-д

План проведения внутреннего контроля по обеспечению уровня защищенности информации в информационных системах ГБОУ СО «ЕШИ № 10»

№ п/п	Наименование мероприятия	Примечание
1	Проверка целей, правового основания обработки персональных данных.	—
2	Проверка наличия не выявленных ранее: - информационных систем (далее – ИС), предназначенных для обработки информации ограниченного распространения; - государственных (муниципальных) ИС.	—
3	Проверка актуальности содержания локальных документов ГБОУ СО «ЕШИ № 10» по защите информации.	—
4	Проверка актуальности для каждой ИС: – локальных документов ГБОУ СО «ЕШИ № 10»; – актов классификации ИС/определения уровня защищенности/определения класса защищенности ГИС; – модели угроз ИС; – требований по защите информации при её обработке в ИС; – матрицы доступа пользователей к защищаемым информационным ресурсам ИС; – технического паспорта ИС; – прочих документов, разработанных для каждой ИС.	—
5	Проверка актуальности перечня материальных носителей информации ограниченного распространения (документы на бумажном носителе), их мест хранения и перечня сотрудников, имеющих прав доступа к таким носителям.	—

№ п/п	Наименование мероприятия	Примечание
6	Проверка достаточности перечня локальных документов ГБОУ СО «ЕШИ № 10» по защите информации по требованиям законодательства Российской Федерации.	—
7	Проверка знаний сотрудниками ГБОУ СО «ЕШИ № 10» требований законодательства Российской Федерации в сфере защиты информации, локальных документов ГБОУ СО «ЕШИ № 10» по защите информации.	—
8	Проверка уровня овладения сотрудниками ГБОУ СО «ЕШИ № 10»технологией безопасной обработки информации ограниченного распространения.	—
9	Проверка проведения планового/внепланового/индивидуального обучения и проверки знаний по вопросам информационной безопасности.	—
10	Проверка наличия запланированных сроков последующего планового/индивидуального обучения и проверки знаний.	—
11	Контроль проведения уничтожения информации ограниченного распространения в самой ИС, на машинных носителях информации и на бумажных носителях.	—
12	Контроль возникновения условий для обезличивания персональных данных.	—
13	Контроль возникновения условий для уничтожения информации ограниченного распространения.	—
14	Контроль возникновения условий для уничтожения машинных носителей информации.	—
15	Контроль возникновения условий для уничтожения материальных носителей информации ограниченного распространения (в т.ч. бумажных документов).	—
16	Проверка соблюдения регламента доступа в помещения, где размещены средства ИС.	—
17	Проверка выполнения требований к условиям размещения автоматизированных рабочих мест в помещениях, в которых размещены технические и средства ИС.	—
18	Проверка целостности пломб на системных блоках и других технических средствах ИС, подлежащих опечатыванию/опломбированию.	—
19	Проверка соответствия фактического состава и структуры программно-технических средств ИС документированному составу и структуре средств ИС (проверка изменения конфигурации ИС).	—
20	Проверка соответствия разграничения прав доступа для каждой ИС субъектов доступа к объектам доступа.	—
21	Проверка ведения журналов: – учета пользователей, имеющих право доступа к ИС; – учета пользователей средств криптографической защиты информации (далее – СКЗИ).	—
22	Проверка ведения журнала учета выдачи паролей для доступа к ИС.	—
23	Проверка ведения журнала учета антивирусных проверок ИС.	—

№ п/п	Наименование мероприятия	Примечание
24	Проверка ведения журнала проверок электронных журналов ИС.	—
25	Проверка ведения журнала нештатных ситуаций в ИС.	—
26	Проверка ведения журнала регистрации действий по сопровождению ИС и изменению их конфигураций.	—
27	Проверка исполнения требований по реагированию на инциденты безопасности.	—
28	Проверка ведения журнала проведения внутреннего контроля за обеспечением уровня защищенности информации.	—
29	Проверка работоспособности установленных средств защиты информации (далее – СЗИ) и СКЗИ.	—
30	Проверка соответствия реальных настроек СЗИ, СКЗИ с настройками, приведенными в соответствующих документах.	—
31	Проверка наличия СЗИ, СКЗИ, в соответствии с указанными в: – журнале поэкземплярного учета СЗИ ИС, эксплуатационной и технической документации к ним; – актами установки сертифицированных СЗИ; – журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов; – актами установки и ввода в эксплуатацию СКЗИ.	—
32	Проверка наличия бухгалтерских документов, подтверждающих правовое основание использования операционных систем, программного обеспечения, технических средств из состава ИС, СЗИ, СКЗИ.	—
33	Проверка неизменности настроенных параметров антивирусной защиты на автоматизированных рабочих местах.	—
34	Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИС.	—
35	Проверка соблюдения правил парольной политики.	—
36	Проверка работоспособности систем резервного копирования.	—
37	Проверка ведения журнала резервного копирования информационных массивов ИС.	—
38	Проверка учета и условий хранения машинных носителей информации.	—
39	Проверка соблюдения требований по обеспечению безопасности при использовании ресурсов сети «Интернет», локальной вычислительной сети.	—
40	Проверка организации порядка учета и сдачи ключей от: – помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ; – хранилищ (предназначенных для хранения съемных машинных носителей информации, для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей).	—
41	Проверка ведения журналов опечатывания (вскрытия) помещений.	—

№ п/п	Наименование мероприятия	Примечание
42	Проверка ведения для хранилищ, оборудованных средствами опечатывания, журналов опечатывания (вскрытия) хранилищ.	—
43	Контроль содержания текстов договоров, предполагающих передачу персональных данных субъектов персональных данных.	—
44	Контроль содержания текстов договоров, предполагающих техническое сопровождение программных продуктов и (или) технических средств, являющихся элементами ИС, а равно и доступ к программным и техническим элементам ИС.	—
45	Проверка оборудования входных дверей помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, опечатывающими устройствами или наличия в таких помещениях технических средств охранной сигнализации.	—
46	Проверка учета хранилищ и ключей от них, в т.ч. проверка ведения журнала учета хранилищ и ключей от них.	—
47	Проверка учета личных печатей, предназначенных для опечатывания помещений (хранилищ), в т.ч. проверка ведения журнала учета личных печатей, предназначенных для опечатывания помещений (хранилищ).	—
48	Проверка актуальности содержания плана мероприятий по защите информации.	—
49	Проверка наличия изменений, предусмотренных частью 7 ст. 22 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и влекущих необходимость уведомления о них Управление Федеральной службы по надзору в сфере связи и массовых коммуникаций по Уральскому федеральному округу.	—
50	Оформление протокола/отчета о результатах внутреннего контроля за обеспечением уровня защищенности информации.	—