Министерство образования и науки Хабаровского края

Краевое государственное бюджетное образовательное учреждение дополнительного образования детей
«ХАБАРОВСКИЙ КРАЕВОЙ ЦЕНТР ВНЕШКОЛЬНОЙ РАБОТЫ «СОЗВЕЗДИЕ»
(КГБОУ ДОД ХКЦВР Созвездие)

ПРИКАЗ

11.02.2013 № 01-04/30
г. Хабаровск

Об утверждении Положения о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных КГБОУ ДОД ХКЦВР Созвездие

В соответствии с действующим законодательством РФ по защите информации
ПРИКАЗЫВАЮ:

1.Утвердить Положение о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных КГБОУ ДОД ХКЦВР Созвездие (Приложение 1).

2.Администратору по обеспечению безопасности персональных данных при их обработке Борчину А.С., системному администратору Маклюку А.Н. в работе руководствоваться настоящим Положением.

3.Контроль за исполнением настоящего приказа возложить на первого заместителя генерального директора - Анисенко И.Н.

Генеральный директор А.Е. Волостникова

Приложение 1 к приказу
от 11.02.2013 № 01-04/30

УТВЕРЖДЕНО
приказом генерального директора
КГБОУ ДОД ХКЦВР Созвездие
от 11.02.2013 № 01-04/30

ПОЛОЖЕНИЕ
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных краевого государственного бюджетного образовательного учреждения дополнительного образования детей «Хабаровский краевой центр внешкольной работы «Созвездие»

1.Общие положения

1.1. Настоящее Положение о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных краевого государственного бюджетного образовательного учреждения дополнительного образования детей «Хабаровский краевой центр внешкольной работы «Созвездие»[1] (далее – Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, Федеральным законом Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Гражданским кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2.Положение определяет порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации, действия, связанные с функционированием информационных систем персональных данных КГБОУ ДОД ХКЦВР Созвездие, меры и средства поддержания непрерывности работы и восстановления работоспособности информационных систем персональных данных.

1.3.Положение призвано определить меры защиты от потери информации, действия по восстановлению в случае потери информации.

---

[1] В целях настоящего Положения считать краевое государственное бюджетное образовательное учреждение дополнительного образования детей «Хабаровский краевой центр внешкольной работы «Созвездие», КГБОУ ДОД ХКЦВР Созвездие и Учреждение равнозначными понятиями.

1.4.Настоящее Положение обязательно для исполнения всеми сотрудниками КГБОУ ДОД ХКЦВР Созвездие. Организационные, распорядительные и локальные нормативные документы Учреждения не должны противоречить настоящему Положению.

1.5.Настоящее Положение вводится в действие приказом генерального директора Учреждения и является локальным нормативным документом постоянного действия.

1.6.Положение признается утратившим силу на основании приказа генерального директора Учреждения.

1.7.Изменения в Положение вносятся приказом генерального директора Учреждения в случаях: изменения законодательства Российской Федерации, изменения организационной структуры или полномочий руководителя, совершенствования системы информационной безопасности и т.п. Инициатором внесения изменений в Положение является Отдел информационных технологий КГБОУ ДОД ХКЦВР Созвездие.

1.8.Ответственность за поддержание настоящего Положения в актуальном состоянии, а также контроль за исполнением требований настоящего Положения возлагается на начальника отдела информационных технологий.

2. Понятия и сокращения, используемые в настоящем Положении

2.1.В целях настоящего Положения используются следующие основные понятия:

Администратор безопасности – сотрудник, ответственный за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации.

Администратор ИСПДн – сотрудник, ответственный за реагирование на инциденты безопасности, приводящие к потере защищаемой информации.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор ИСПДн – сотрудник, осуществляющий обработку персональных данных.

Персональные данные субъекта - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Информация – сведения независимо от формы их представления.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Инцидент - происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

2.2.В целях настоящего Положения используются следующие сокращения:

ИСПДн – информационная система персональных данных.

ПО – программное обеспечение.

ТС – технические средства.

RAID – дисковый массив из нескольких жестких дисков, воспринимаемый операционной системой как единое целое.

RAID-0 - дисковый массив из двух или более жёстких дисков с отсутствием избыточности, не обеспечивающий сохранность данных в случае выхода из строя одного из дисков.

RAID-1 (*mirroring — «зеркалирование»*) — массив из двух дисков, являющихся полными копиями друг друга. То есть данные при этом просто полностью дублируются (зеркалируются), за счет чего достигается очень высокий уровень надежности.

3. Порядок реагирования на инцидент

3.1.Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
-в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

3.2.Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю над соблюдением режима защиты персональных данных».

3.2.В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Учреждения (Администратор безопасности, Администратор и Оператор ИСПДн), предпринимают меры по восстановлению работоспособности ИСПДн. Предпринимаемые меры при необходимости согласуются руководством КГБОУ ДОД ХКЦВР Созвездие.

4. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

4.1. ТЕХНИЧЕСКИЕ МЕРЫ.

4.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

4.1.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

4.1.3.Все критичные помещения Учреждения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

4.1.4.Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

4.1.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

4.1.6. Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

4.1.7. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации.

4.1.8. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

4.1.9. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

4.2. ОРГАНИЗАЦИОННЫЕ МЕРЫ.

4.2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4.2.2.Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета.

4.2.3.Носители, на которые произведено резервное копирование, должны быть промаркированы номером носителя, датой проведения резервного копирования.

4.2.4.Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

4.2.5.Носители должны храниться не менее года для возможности восстановления данных.

Начальник отдела информационных технологий А.С. Борчин