Утверждено приказом директора Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей» № 01-06/ 191 от 17.02.2015.

РЕГЛАМЕНТ
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ГОСМУДАРСТВЕННОГО АВТОНОМНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ЧУКОТСКОГО АВТОНОМНОГО ОКРУГА «ЧУКОТСКИЙ ОКРУЖНОЙ ПРОФИЛЬНЫЙ ЛИЦЕЙ»

г. Анадырь, 2015 год

СОДЕРЖАНИЕ

1	Общие положения	3
2	Обеспечение безопасности персональных данных в ИСПДн Чукотский окружной профильный лицей	3-4
3	Основные направления и методы защиты информации в ИСПДн в Чукотском окружной профильном лицее	4-6
3.1.	Защита информации от вредоносного программного обеспечения	7
3.2.	Защита персональных данных от несанкционированного доступа	8
3.3.	Защита персональных данных от несанкционированного и непреднамеренного воздействия	9
3.4.	Защита персональных данных от распространения неограниченному кругу лиц	9-10
4	Порядок резервирования и восстановления работоспособности ИСПДн Чукотского окружного профильного лицея	10
4.1.	Порядок реагирования на инцидент	10
4.2.	Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов	10
4.2.1.	Технические меры	10-11
4.2.2.	Организационные меры	11
5	Порядок обращения со средствами криптографической защиты информации	11-12
5.1.	Состав СКЗИ	12
5.2.	Учёт используемых СКЗИ	12
5.3.	Допуск работников к СКЗИ	12
5.3.1.	Порядок оформления допуска к СКЗИ	12
5.3.2.	Порядок выдачи СКЗИ	12
5.3.3.	Порядок пересмотра прав доступа к СКЗИ	13
5.3.4.	Порядок прекращения прав доступа и изъятия СКЗИ из обращения	13
6	Порядок обращения с материальными носителями персональных данных	13
6.1.	Порядок использования машинных носителей персональных данных	13
6.1.1.	Порядок хранения машинных носителей, содержащих персональные данные	13-14
6.1.2.	Хранение носителей резервного копирования	14
6.1.3.	Порядок уничтожения машинных носителей, содержащих персональные данные	14
6.1.4.	Порядок уничтожения (стирания) персональных данных с машинного носителя	14
6.2.	Порядок уничтожения (стирания) персональных данных с машинного носителя	15

Приложение № 1. Журнал учёта применяемых в ИСПДн Чукотского окружного профильного лицея средств защиты информации.

Приложение № 2. Журнал поэкземплярного учёта применяемых в ИСПДн Чукотский окружной профильный лицей криптографических (шифровальных) средств, эксплуатационной и технической документации к ним.

Приложение № 3. Журнал учёта машинных носителей персональных данных, обрабатываемых в ИСПДн Чукотский окружной профильный лицей.

Приложение № 4. Акт уничтожения машинных носителей персональных данных.

Приложение № 5. Порядок обеспечения антивирусной защиты ИСПДн Чукотского окружного профильного лицея.

Приложение № 6. Порядок обеспечения парольной защиты ИСПДн Чукотский окружной профильный лицей.

1. Общие положения

Настоящий Регламент обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей» (далее – Регламент) устанавливает и определяет основные организационные и технические меры по защите персональных данных, основные обязанности пользователей и должностных лиц, обрабатывающих персональные данные автоматизированным способом в информационной системе персональных данных Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей» (далее – ИСПДн Чукотский окружной профильный лицей) и телекоммуникационных сетях Чукотского окружного профильного лицея.

Требования Регламента являются обязательными для работников Чукотского окружного профильного лицея и третьих лиц, которые допущены к работе с персональными данными (далее – ПДн).

При приёме на работу работники Чукотского окружного профильного лицея, допущенные к персональным данным, должны быть под расписку ознакомлены с требованиями настоящего Регламента, в части, касающейся их деятельности, информированы об ответственности за их нарушение.

Настоящий Регламент утверждается директором Чукотского окружного профильного лицея и носит обязательный характер для всех работников.

2. Обеспечение безопасности персональных данных в ИСПДн Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей»

Обеспечение безопасности ПДн в Чукотском окружном профильном лицее достигается за счёт выполнения требований нормативных актов РФ в сфере защиты персональных данных и выполнения требований, установленных во внутренних нормативных документах Чукотского окружного профильного лицея, всеми пользователями персональных данных.

Персональные данные субъектов ПДн, обрабатывающиеся в ИСПДн Чукотского окружного профильного лицея подлежат защите от несанкционированного доступа и копирования. Безопасность персональных данных при их обработке в ИСПДн Чукотского окружного профильного лицея, обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Технические и программные средства обработки и защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации, относящейся к персональным данным.

Реализация требований по обеспечению безопасности персональных данных в информационных системах возлагается на структурное подразделение или лицо, ответственное за обеспечение безопасности ПДн в ИСПДн Чукотского окружного профильного лицея совместно со структурными подразделениями, обрабатывающими персональные данные согласно Перечню должностей служащих, замещение которых предусматривает осуществление обработки ПДн.

При обработке персональных данных в информационных системах ответственными лицами должно быть обеспечено:

Лицо, ответственное за обеспечение безопасности ПДн, контролирует, в пределах своей компетенции, состояние защиты персональных данных с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки её защищенности.

Повседневный и периодический (не реже одного раза в год) контроль за состоянием защиты персональных данных выполняется силами подразделений (штатных работников), обрабатывающих персональные данные согласно должностным обязанностям, и специалистов структурного подразделения Чукотского окружного профильного лицея, ответственного за обеспечение безопасности ПДн, в соответствии с «Регламентом осуществления внутреннего контроля за обеспечением уровня защищенности ПДн и соблюдением условий использования средств защиты информации, а также соблюдением требований законодательства РФ по обработке ПДн в ИСПДн Чукотского окружного профильного лицея.

Ежегодно о состоянии защиты персональных данных в Чукотском окружном профильном лицее, а также об инцидентах в связи с невыполнением сотрудниками или третьими лицами требований и норм по защите персональных данных, в результате которых имелись или имеются возможности их утечки, лицо, ответственное за обеспечение безопасности ПДн, сообщает лицу, ответственному за организацию обработки ПДн, а тот, соответственно руководству Чукотского окружного профильного лицея.

В целях предотвращения несанкционированного доступа к техническим средствам обработки, хранения и передачи информации (далее – ТСПИ), их хищения и нарушения работоспособности ИСПДн Чукотского окружного профильного лицея, самостоятельно, или с привлечением аутсорсинговых организаций, обеспечивается охрана и физическая защита помещений объектов информатизации, в которых располагаются технические средства ИСПДн Чукотского окружного профильного лицея.

Структурное подразделение Чукотского окружного профильного лицея, ответственное за обеспечение безопасности ПДн, обязано обеспечивать защиту всех компонент информационной структуры ИСПДн Чукотского окружного профильного лицея, поддерживать в актуальном состоянии организационно - распорядительную, проектную и эксплуатационную документацию на систему защиты ПДн ИСПДн Чукотского окружного профильного лицея, телекоммуникационные линии связи, ТСПИ, средства криптографической защиты информации (далее – СКЗИ).

Защита персональных данных в Чукотском окружном профильном лицее от актуальных угроз безопасности осуществляется по следующим направлениям:

- ✓ от внедрённых специальных электрических устройств;
- ✓ от вредоносного кода;
- ✓ от несанкционированного доступа;
- ✓ от несанкционированного воздействия;
- ✓ от непреднамеренного воздействия;
- ✓ от разглашения;
- ✓ от технических средств разведки (далее – ТСР).

В качестве основных мер защиты персональных данных Чукотского окружного профильного лицея должностными лицами, обрабатывающими или защищающими персональные данные, а также подразделениями, осуществляющими или защищающими персональные данные, а также подразделениями, осуществляющими эксплуатацию

3.1. Защита информации от вредоносного программного обеспечения

Организация антивирусной защиты информации в ИСПДн Чукотского окружного профильного лицея достигается путём:

- ✓ внедрения и применения средств антивирусной защиты информации;
- ✓ обновления сигнатурных баз данных средств антивирусной защиты информации;
- ✓ спланированных действий должностных лиц при обнаружении заражения информационных ресурсов ИСПДн Чукотского окружного профильного лицея вирусным программным обеспечением.

Система антивирусной защиты ИСПДн включает в себя:

- ✓ антивирусную защиту рабочих станций ИСПДн;
- ✓ антивирусную защиту серверов и баз персональных данных ИСПДн;
- ✓ возможность автоматического обновления сигнатурных антивирусных баз и версий.

Организация работ по антивирусной защите информации возлагается на структурное подразделение или назначенное лицо «НО», ответственное за обеспечение безопасности ПДн, и должностных лиц, осуществляющих эксплуатацию объектов информатизации ИСПДн Чукотского окружного профильного лицея, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации – на лицо, ответственное за обеспечение безопасности ПДн.

Порядок применения средств антивирусной защиты устанавливается с учётом необходимости выполнения следующих требований:

пользователями ИСПДн:

- ✓ периодическая проверка носителей информации (не реже одного раза в неделю) и обязательная проверка используемых в работе съёмных носителей информации перед началом работы с ними на отсутствие программных вирусов;
- ✓ внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса.

работниками подразделения, осуществляющего эксплуатацию ИСПДн:

- ✓ обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации съёмных и встроенных носителей информации, информационных массивов и баз данных, программных средств общего и специального назначения;
- ✓ восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

К использованию в Чукотском окружном профильном лицее допускается только санкционированные структурным подразделением или назначенным работником Чукотского окружного профильного лицея, ответственным за обеспечение безопасности ПДн, антивирусные средства. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

При обнаружении программных вирусов пользователь ИСПДн обязан прекратить все работы на рабочем месте, поставить в известность структурное подразделение Чукотского окружного профильного лицея ответственное за обеспечение безопасности ПДн, и совместно с его специалистами принять меры к локализации и удалению вирусов с помощью имеющихся антивирусных средств защиты.

При функционировании автоматизированного рабочего места в качестве локальной рабочей станции вычислительной сети производится её отключение от локальной сети, локализация и удаление программных вирусов в вычислительной технике.

3.3. Защита персональных данных от несанкционированного и непреднамеренного воздействия

Защита персональных данных от несанкционированного и непреднамеренного воздействия осуществляется по следующим направлениям:

- ✓ соблюдение порядка разработки, ввода в действие и эксплуатации объектов информатизации;
- ✓ определение условий размещения информационных ресурсов ИСПДн относительно границ контролируемой зоны;
- ✓ определение технических средств и систем, предполагаемых к использованию в ИСПДн и системах связи, условий их расположения;
- ✓ определение режимов обработки персональных данных в ИСПДн Чукотского окружного профильного лицея в целом и в отдельных компонентах;
- ✓ установление правил разграничения доступа для пользователей с целью минимизации их воздействия на программные и аппаратные средства автоматизации обработки персональных данных;
- ✓ повышение уровня квалификации пользователей и обслуживающего персонала, периодическое и выборочное тестирование знаний и квалификации в области информационной безопасности;
- ✓ контроль, техническое обслуживание и обеспечение установленных режимов работы ТСПИ в целях предупреждения их сбоев, аварий, неисправностей (Приложение 1);
- ✓ применение постоянно обновляемого антивирусного программного обеспечения;
- ✓ защита от природных и техногенных явлений и стихийных бедствий (пожары, наводнения и т.п.);
- ✓ предупреждение передачи конфиденциальных персональных данных по открытым линиям связи и их обработки незащищёнными техническими средствами;
- ✓ строгое выполнение работниками установленных в организации требований по защите персональных данных;
- ✓ организация эффективного контроля выполнения предусмотренных мер защиты персональных данных;
- ✓ использование ИСПДн в защищённом исполнении.

3.4. Защита персональных данных от распространения неограниченному кругу лиц

Правовой основой работы с работниками Чукотского окружного профильного лицея, допущенными к обработке персональных данных, является:

- ✓ наличие в трудовом договоре пункта о правилах работы со сведениями, относящимися к персональным данным;
- ✓ наличие в должностной инструкции работника пунктов о мерах безопасности при обработке персональных данных и ответственности за её несанкционированное разглашение;
- ✓ наличие Перечня персональных данных, обрабатываемых в Чукотском окружном профильном лицее, инструкций и регламентов по защите персональных данных, ознакомление с которыми должно проводиться работником в первый день заступления на должность и под обязательную роспись в ознакомлении;
- ✓ создание работникам достаточных условий для обеспечения эффективной защиты персональных данных.

В целях предупреждения разглашения персональных данных структурное подразделение или назначенное Чукотским окружным профильным лицеем лицо, ответственное за обеспечение безопасности ПДн, организует мероприятия по аудиту защищённости персональных данных, тестированию уровня осведомленности

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн Чукотского окружного профильного лицея, сетевое и коммуникативное оборудование, а также наиболее критичные рабочие станции подключаются 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 и т.д.);
- ✓ резервные линии электропитания в пределах комплекса зданий;
- ✓ аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- ✓ кластеризация;
- ✓ технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн Чукотского окружного профильного лицея при сбое в работе оборудования и их автоматической замены без простоев используют методы кластеризации.

Для наиболее критичных компонентов ИСПДн Чукотского окружного профильного лицея должны использоваться территориально удалённые системы кластеров.

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.

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

4.2.2. Организационные меры

Резервное копирование и хранение данных должно осуществляться на периодической основе:

- ✓ для обрабатываемых персональных данных – не реже одного раза в неделю;
- ✓ для технологической информации – не реже одного 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 Чукотского окружного профильного лицея – не реже одного раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учёта.

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

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

Носители должны храниться не менее одного года, для возможности восстановления данных.

5. Порядок обращения со средствами криптографической защиты информации

Использование СКЗИ в Чукотском окружном профильном лицее необходимо для достижения следующих целей:

- ✓ обеспечение целостности ПДн, обрабатываемых в ИСПДн;

5.3.3. Порядок пересмотра прав доступа к СКЗИ

Лицо, ответственное за обеспечение безопасности ПДн, обязано производить ежемесячный пересмотр допуска ПДн к СКЗИ путём анализа Перечня лиц, допущенных к работе с СКЗИ.

В случае обнаружения Пользователей ПДн с истекающим сроком использования СКЗИ, лицо, ответственное за обеспечение безопасности ПДн, не менее чем за 5 рабочих дней, обязано оповестить Пользователя о прекращении использования СКЗИ.

5.3.4. Порядок прекращения прав допуска и изъятия СКЗИ из обращения

Прекращение прав доступа Пользователя ПДн к СКЗИ осуществляется лицом, ответственным за обеспечение безопасности ПДн, в следующих случаях:

- ✓ достигнуты цели использования СКЗИ;
- ✓ истёк период времени, указанный в заявке;
- ✓ увольнение Пользователя ПДн или его перевод на другую должность, не связанную с необходимостью использования СКЗИ.

При наступлении вышеуказанных случаев, лицо ответственное за обеспечение безопасности ПДн, осуществляет исключение Пользователя ПДн из Перечня лиц, допущенных к работе с СКЗИ и изымает СКЗИ из обращения. Перед повторным использованием с основного и резервного ключевых носителей СКЗИ при помощи средств гарантированного уничтожения должна быть удалена вся информация.

6. Порядок обращения с материальными носителями персональных данных

Учёту подлежат следующие типы машинных носителей ПДн:

- ✓ Отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD. DVD. Blu-ray и прочие)4
- ✓ Неотчуждаемые носители информации (жёсткие магнитные диски).

6.1. Порядок организации учёта машинных носителей, содержащих персональные данные

Все машинные носители данных, используемые при работе со средствами вычислительной техники (далее СВТ) для обработки и хранения персональных данных, обязательно регистрируются и учитываются в Журнале учёта машинных носителей ПДн, обрабатываемых в ИСПДн Чукотского окружного профильного лицея (далее – Журнал учёта носителей) с присвоением индивидуального учётного номера (Приложение № 3).

Ответственность за хранение машинных носителей ПДн и ведение Журнала учёта носителей в Чукотском окружном профильном лицее несёт лицо, ответственное за обеспечение безопасности ПДн.

Учётный номер и гриф «Конфиденциально» наносятся на носитель информации или его корпус. Если не возможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель.

Несъёмные жёсткие магнитные диски закрепляются за работником, ответственным за СВТ, в котором они установлены.

6.1.1. Порядок использования машинных носителей персональных данных

Машинные носители данных выдаются Пользователям или другим лицам, участвующим в обработке персональных данных, для работы под расписку в Журнале учёта носителей. После завершения работы машинные носители данных сдаются лицу, ответственному за обеспечение безопасности ПДн.

Уничтожение персональных данных с материального носителя происходит путём очистки информации, с использованием сертифицированных по требованиям

Уничтожение производится один раз в год путём их физического разрушения с предварительным затиранием (уничтожением) содержащейся на них ПДн, если это позволяют физические принципы работы носителя.

Уничтожение машинных носителей производится Комиссией в составе не менее трёх человек, в состав Комиссии должно обязательно входить лицо, ответственное за обеспечение безопасности ПДн, и лицо, ответственное за организацию обработки ПДн. После уничтожения всех машинных носителей составляется акт об уничтожении (Приложение № 4).

При уничтожении машинные носители данных снимаются с учёта. Отметка, об уничтожении носителей, проставляется в Журнале учёта носителей.

6.2. Порядок уничтожения (стирания) персональных данных с машинного носителя

Основанием для уничтожения (стирания) записей или части записей с машинного носителя являются следующие случаи:

- ✓ возврат носителя работником;
- ✓ передача носителя в ремонт;
- ✓ списание носителя.

Хранящиеся на машинных носителях и потерявшие актуальность персональные данные, своевременно стираются (уничтожаются). Лицо, ответственное за обеспечение безопасности ПДн принимает окончательное решение о необходимости их уничтожения.

Ответственный за процесс обработки ПДн передаёт машинный носитель лицу, ответственному за обеспечение безопасности ПДн. Совместно с машинным носителем передаётся служебная записка, в которой указываются причины возврата и состав ПДн, которые подлежат уничтожению.

Лицо, ответственное за обеспечение безопасности ПДн, при получении носителя должно обеспечить уничтожение (стирание) записей или части записей с носителя и подготовить акт об уничтожении (стирании) записей с носителя (Приложение № 4) с внесением данных в Журнал учёта носителей.

В акт уничтожения заносится дата, учётный номер носителя и способ уничтожения (стирания) записей ПДн, также в акте отображается наименование программного обеспечения, которым производилось стирание.

Приложение № 2.

ЖУРНАЛ

поэкземплярного учёта применяемых в ИСПДн Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей» криптографических (шифровальных) средств, эксплуатационной и технической документации к ним

Журнал начат: _____ Журнал завершён: _____

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Примечание
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя СКЗИ	Дата и расписка в получении	ФИО сотрудника, проводившего установку	Дата установки и подписи лиц, производивших установку	Номера аппаратных средств, в которые установлены СКЗИ	
1	2	3	4	5	6	7	8	9	10	11	12

Приложение № 4.

АКТ №
уничтожения машинных носителей персональных данных
Государственного автономного общеобразовательного учреждения
Чукотского автономного округа
«Чукотский окружной профильный лицей»

г. Анадырь «____» _____ 201___года

Мы, нижеподписавшиеся, комиссия в составе:
председателя _____
(должность, ФИО)
членов комиссии: _____
(должность, ФИО)

_____
(должность, ФИО)

_____
(должность, ФИО)

_____
(должность, ФИО)

составила настоящий акт о том, что произведено уничтожение машинных носителей/ПДн, содержащихся на машинных носителях, предназначенных для обработки конфиденциальной информации в составе:
«тип носителя, учётный номер носителя, тип конфиденциальной информации»
«тип носителя, учётный номер носителя, тип конфиденциальной информации»
«тип носителя, учётный номер носителя, тип конфиденциальной информации»
Носители уничтожены путём: _____
(сжигания, размагничивания, физического уничтожения)

Председатель _____
(должность, ФИО)
Члены комиссии: _____
(должность, ФИО)

_____
(должность, ФИО)

_____
(должность, ФИО)

_____
(должность, ФИО)

Приложение № 5.

ПОРЯДОК
Обеспечения антивирусной защиты ИСПДн Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей»

1. Порядок использования антивирусных средств

1.2. Применение средств антивирусного контроля

Средства антивирусной защиты установлены и настроены на всех допускающих такую установку программно-технических средствах до начала их использования для обработки ПДн.

Модуль средств антивирусной защиты, отвечающий за мониторинг вирусной активности в реальном времени (антивирусный монитор), запускается при загрузке операционной системы в автоматическом режиме с основным модулем средства антивирусной защиты.

Антивирусный контроль рабочих станций проводится ежедневно в автоматическом режиме. В тех случаях, когда проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, проводится выборочная проверка загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и файлов, загружаемых по сети или с внешних носителей. В этом случае полная проверка осуществляется не реже одного раза в неделю в период неактивности пользователя.

Антивирусный контроль серверов проводится ежедневно, а также при перезапуске сервера.

Проводится антивирусная проверка на рабочих станциях и серверах, вернувшихся с технического обслуживания или ремонта (в том числе гарантийного), производимого сторонними организациями.

Любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съёмных носителях (магнитных дисках, лентах CD/DVD-R/RW, USB Flash drive и т.п.) подлежит обязательному антивирусному контролю.

Контроль исходящей информации проводится непосредственно перед архивированием и отправкой (записью на съёмный носитель).

Файлы, помещаемые в электронный архив, в обязательном порядке проходят антивирусный контроль. Периодические проверки электронных архивов проводятся не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вредоносных программ. Непосредственно после установки (изменения) программного обеспечения компьютера системным администратором ИСПДн «НО» выполняется антивирусная проверка.

Обновления антивирусных баз проводятся не реже одного раза в сутки в автоматическом режиме, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления, обновление баз производится вручную с той же периодичностью.

Установка, настройка и использование стандартного антивирусного пакета для серверов и рабочих станций производятся в соответствии с инструкциями производителя конкретного антивирусного продукта.

2. Действия при обнаружении вредоносных программ

В случае обращений Пользователей ИСПДн Чукотского окружного профильного лицея, связанных с подозрением на наличие вредоносных программ, проводится внеочередной антивирусный контроль рабочих станций обратившихся Пользователей. В случае подтверждения наличия вредоносных программ в результате проведения контроля делается вывод либо об их уничтожении, либо о необходимости дальнейшего восстановления работоспособности компьютера.

Приложение № 6.

Порядок обеспечения парольной защиты

1. Общие требования к использованию паролей

При создании новой учётной записи для неё устанавливается первичный пароль. При его создании используется опция, требующая смены пароля при первом входе в систему, и производится соответствующее уведомление владельца учётной записи о необходимости смены пароля.

Пользователи ИСПДн Чукотского окружного профильного лицея всегда положительно идентифицируются до изменения пароля и предоставления нового пароля.

Реинициализованные пароли принудительно меняются при первом входе в систему. Система автоматически блокирует учётную запись после 3 неудачных попыток ввода пароля. Блокировка учётной записи автоматически снимается по прошествии одной минуты, после чего пользователь вновь получает возможность авторизоваться в системе. Неудачные попытки авторизации регистрируются в системном журнале.

Если система предоставляет автоматизированные инструменты для конфигурирования требуемых опций, то они соответствующим образом настроены.

Хранение, работником, значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале.

2. Правила формирования пароля

Персональные пароли генерируются специальными программными средствами администраторами ИСПДн Чукотского окружного профильного лицея с учётом следующих требований:

- ✓ длина пароля составляет не менее 7-ми символов;
- ✓ длина пароля для привилегированных пользователей составляет не менее 10-ти символов;
- ✓ в составе символов пароля обязательно присутствуют буквы в верхнем и нижнем регистрах, цифры и специальные символы (“~!@#$%^&*()-+_=\|/?,);
- ✓ при смене пароля новое значение отличается от предыдущего не менее чем в 4-ёх позициях;
- ✓ пароль может повторяться не менее чем после использования 5-ти различных паролей;
- ✓ личный пароль пользователь не имеет права сообщать никому;
- ✓ пароль не включает в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе.

3. Срок действия пароля

Пароли на серверы, рабочие станции, сетевые устройства, базы данных и приложения изменяются согласно требованиям, изложенным в Таблице 1. Блокирование учётной записи с истекшим паролем автоматизировано. Если это не возможно, пользователь изменяет свои пароли, основываясь на приведённом в таблице 1 расписании.

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ЧУКОТСКОГО АВТОНОМНОГО ОКРУГА «ЧУКОТСКИЙ ОКРУЖНОЙ ПРОФИЛЬНЫЙ ЛИЦЕЙ»

П Р И К А З

17 февраля 2015 года **г. Анадырь** **№ 01-06/191**

Об утверждении документов, регламентирующих обработку персональных данных.

В соответствии с требованиями Федерального закона № 152-ФЗ от 27 июля 2006 года «О защите персональных данных», в целях определения порядка обработки и защиты персональных данных Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей», обеспечения защиты прав и свобод граждан при обработке персональных данных, а также установления ответственности должностных лиц, имеющих доступ к персональным данным,

ПРИКАЗЫВАЮ:

1. Положение о персональных данных работников Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей».
2. Регламент обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей».
3. Порядок доступа сотрудников Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей», в помещениях, в которых ведётся обработка персональных данных.
4. Инструкция о порядке обеспечения конфиденциальности при обработке, хранении и движении документов, содержащих персональные данные.
5. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.
6. Перечень сведений конфиденциального характера в Государственном автономном общеобразовательном учреждении Чукотского автономного округа «Чукотский окружной профильный лицей».
7. Перечень информационных систем персональных данных Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей».
8. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных Государственного автономного общеобразовательного учреждения Чукотского автономного округа «Чукотский окружной профильный лицей».