Министерство образования Московской области
Государственное бюджетное профессиональное образовательное учреждение
Московской области «Воскресенский колледж»

УТВЕРЖДАЮ
Директор ГБПОУ МО "Восркесенский колледж"
А.Ю.Лунина

Подписано цифровой подписью:
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ
"ВОСКРЕСЕНСКИЙ КОЛЛЕДЖ"
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760,
ОГРН=1047797019830, STREET="Большой Златоустинский переулок,
д. 6, строение 1", L=г. Москва, C=RU, O=Казначейство России,
CN=Казначейство России
Дата: 3 Май 2024 г. 17:01:06

ПРОГРАММА И МЕТОДИКИ ОЦЕНКИ ЭФФЕКТИВНОСТИ РЕАЛИЗОВАННЫХ В РАМКАХ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ГБПОУ МО «ВОСКРЕСЕНСКИЙ КОЛЛЕДЖ» «БУХГАЛТЕРИЯ», «ОТДЕЛ КАДРОВ», «УЧЕБНОЙ ЧАСТИ СП№1, СП№2, СП№3»

г. Воскресенск
2024

Перечень используемых сокращений

АРМ	–	автоматизированное рабочее место
ИСПДн	–	информационная система персональных данных
НСД	–	несанкционированный доступ
ОС	–	операционная система
ПДн	–	персональные данные
ПО	–	программное обеспечение
СВТ	–	средства вычислительной техники
СЗИ	–	средство защиты информации
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю Российской Федерации

Содержание

1 НОРМАТИВНЫЕ ССЫЛКИ

Программа и методики разработаны с учетом положений и требований нормативных, руководящих и методических документов в области защиты информации, действующих на территории Российской Федерации:

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 6 апреля 2011 г.);

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (в ред. № 261-ФЗ от 25 июля 2011 г. и № 43-ФЗ от 5 апреля 2013 г.);

– Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

– ГОСТ Р 51275-99 «Объект информатизации. Факторы воздействующие на информацию»;

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации»;

– ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»;

– Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности конфиденциальной информации при их обработке в информационных системах персональных данных».

2 ОБЪЕКТ ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Объектом оценки эффективности мер по обеспечению безопасности персональных данных (далее – оценки эффективности), является информационная система персональных данных ГБПОУ МО «Воскресенский колледж» «Бухгалтерия», «Отдел кадров», «Учебной части СП №1, СП №2, СП №3».

В рассматриваемой системе осуществляется обработка персональных данных. Технологический процесс предусматривает многопользовательский режим обработки персональных данных с одинаковыми правами пользователей на доступ к информации.

Актом определения уровня защищенности персональных данных при их обработке в ИСПДн «Бухгалтерия», «Отдел кадров», «Учебной части СП №1, СП №2, СП №3» в ГБПОУ МО «Воскресенский колледж» присвоен 3Б (третий) уровень защищенности персональных данных при их обработке в информационных системах персональных данных в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для оценки эффективности предоставляются:

ИСПДн «Бухгалтерия», «Отдел кадров», «Учебной части СП №1, СП №2, СП №3»;

программа и методики оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных (далее - программа и методики);

комплект организационно-распорядительной документации по защите информации.

Система защиты информации ИСПДн «Бухгалтерия», «Отдел кадров», «Учебной части СП №1, СП №2, СП №3» представляет собой совокупность организационных мер и программных средств защиты информации:

встроенных программных средств обеспечения информационной безопасности операционной системы Microsoft Windows - 7;

средства антивирусной защиты «Kaspersky Endpoint Security для бизнеса».

3 ЦЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Целью оценки эффективности является оценка защищенности персональных данных от несанкционированного доступа и соответствия ИСПДн «Бухгалтерия», «Отдел кадров», «Учебной части СП №1, СП №2, СП №3» нормативным

требованиям по защите информации, обеспечивающим 3Б (третий) уровень защищённости персональных данных при их обработке в информационных системах персональных данных.

4 ОБЪЕМ ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Состав оценки эффективности приведен в таблице (таблица 1)

Таблица 1 - Состав оценки эффективности ИСПДн

№ п/п	Состав и содержание мер по обеспечению безопасности персональных данных	Методики оценки (Раздел 7)
1.	Общие проверки	А.1
2.	Идентификация и аутентификация субъектов доступа и объектов доступа	А.2
3.	Управление доступом субъектов доступа к объектам доступа	А.3
4.	Защита машинных носителей персональных данных	А.4
5.	Регистрация событий безопасности	А.5
6.	Антивирусная защита	А.6
7.	Контроль (анализ) защищенности персональных данных	А.7
8.	Защита технических средств	А.8
9.	Управление конфигурацией информационной системы и системы защиты персональных данных	А.9

5 УСЛОВИЯ И ПОРЯДОК ПРОВЕДЕНИЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оценка эффективности проводится последовательно в соответствии с объемом, определенном в разделе 4, и по методикам, приведенным в разделе 6. Оценка эффективности проводится в полном объеме вне зависимости от результатов каждого отдельного испытания. Система считается эффективной, если она успешно прошла все проверки; в противном случае Система считается не эффективной.

Оценка эффективности проводится в рабочих (эксплуатационных) режимах на реальной конфигурации технических и программных средств, обеспечивающей

функциональную достаточность для проведения проверок в требуемом объеме и достоверность оценки системы.

Оценка эффективности проводится в нормальных климатических условиях (по ГОСТ 21552-84), в помещениях, удовлетворяющих условиям эксплуатации СВТ и требованиям обработки персональных данных.

При проведении оценки эффективности не должны вноситься никакие изменения в состав технических и программных средств, настройки оборудования и программного обеспечения (включая средства защиты информации), а также иные работы, если это явно не предусмотрено методикой.

6 МЕТОДИКИ ПРОВЕДЕНИЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

А.1. Общие проверки

А.1.1 Проверка состава технической, организационно-распорядительной и эксплуатационной документации

Метод: экспертно-документальный.

Методика: 1. Изучить состав представленной документации.

2. Убедиться в наличии:

– приказа о создании комиссии по определению уровня защищенности ИСПДн;

– приказ об утверждении комплекта ОРД;

– акта определения уровня защищенности ИСПДн;

– приказ о вводе в эксплуатацию ИСПДн;

– модели угроз безопасности ПДн;

– приказ о назначении ответственного за организацию обработки ПДн;

– инструкции ответственного и пользователя ИСПДн;

– списка лиц, допущенных к работе в ИСПДн;

– журнал учета МНИ;

– журнал учета паролей;

– технического паспорта.

Критерий: меры по обеспечению безопасности персональных данных считаются эффективными, если представлены все документы, перечисленные в п. 2 методики, либо аналогичные им по содержанию.

А.1.2 Проверка корректности классификации ИСПДн

Метод: экспертно-документальный, экспертно-аналитический.

Методика:

1. Изучить акт определения уровня защищенности персональных данных при их обработке в ИСПДн в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Проанализировать выявленные комиссией по категорированию определяющие признаки и убедиться в их соответствии архитектуре ИСПДн и технологическому процессу обработки информации.

3. Убедиться в соответствии присвоенного уровня защищенности персональных данных при их обработке в ИСПДн и совокупности определяющих признаков категорирования.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если уровень защищенности персональных данных при их обработке в ИСПДн установлен верно, а выявленные определяющие признаки категорирования соответствуют архитектуре ИСПДн и технологическому процессу обработки информации.

А.1.3 Проверка достаточности представленных документов и их соответствия требованиям безопасности информации

Метод: экспертно-документальный, экспертно-аналитический.

Методика:

1. Проанализировать содержание совокупности представленной технической, эксплуатационной и организационно-распорядительной документации.

2. Убедиться, что содержание документов достаточно для обеспечения защиты информации и соответствует требованиям нормативных и руководящих документов в области безопасности информации.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если состав и содержание документов достаточны для обеспечения защиты информации и соответствуют требованиям руководящих документов в области безопасности информации.

А.1.4 Проверка осведомленности пользователей о требованиях организационно-распорядительной документации по защите информации

Метод: экспертно-аналитический.

Методика:

1. Провести опрос:

– ответственного за организацию обработки персональных данных;

– администратора информационной безопасности;

– ответственного за эксплуатацию ИСПДн;

– пользователя ИСПДн.

2. Убедиться, что все лица, перечисленные в п. 1 методики, осведомлены о своих должностных обязанностях, принятом технологическом процессе обработке информации, требованиях организационно-распорядительной документации по защите информации и ответственности за их нарушение.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если содержание организационно-распорядительных документов доведено до всех лиц, перечисленных в п. 1 методики.

А.1.5 Проверка наличия действующих сертификатов соответствия на средства защиты информации

Метод: экспертно-документальный.

Методика:

1. Проанализировать состав средств защиты информации.

2. Проверить наличие копий сертификатов соответствия требованиям безопасности информации на каждое из СЗИ, СКЗИ и убедиться, что сроки действия сертификатов не истекли.

3. Проверить возможность применения (в соответствии с сертификатом) СЗИ в ИСПДн для обеспечения установленного уровня защищенности персональных данных.

4. Проверить маркирование каждого экземпляра СЗИ, сертифицированного в системе сертификации средств защиты информации ФСТЭК России, специальным защитным знаком.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если на каждое СЗИ и СКЗИ имеются в наличии копии сертификатов соответствия, подтверждающие возможность применения в ИСПДн для обеспечения установленного уровня защищенности персональных данных, срок действия сертификатов не истек и все экземпляры СЗИ промаркированы должным образом.

А.1.6 Проверка средств восстановления системы защиты информации

Метод: экспертно-технический.

Методика:

1. Проанализировать состав дистрибутивов программного обеспечения средств защиты информации и эксплуатационную документацию к ним.

2. Убедиться, что комплект дистрибутивов и эксплуатационной документации достаточен для восстановления системы защиты информации.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если комплект дистрибутивов и эксплуатационной документации достаточен для восстановления системы защиты информации.

А.2. Испытание подсистемы идентификации и аутентификации субъектов доступа и объектов доступа

А.2.1 Проверка идентификации и аутентификации пользователей, являющихся работниками оператора

Метод: экспертно-технический.

Методика:

1. Включить (перезагрузить) АРМ (или Сервер).

2. Ввести неверный пароль.

3. Ввести верный пароль.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если в результате выполнения пп. 1 методики пользователю будет отказано в доступе, а в результате выполнения п. 2 методики доступ пользователю будет разрешен.

А.2.2 Проверка управления средствами аутентификации, в том числе хранения, выдачи, инициализации, блокирования средств аутентификации и принятия мер в случае утраты и (или) компрометации средств аутентификации.

Метод: экспертно-документальный, экспертно-технический.

Методика:

1. Проанализировать содержание организационно-распорядительной документации, технической и эксплуатационной документации к СЗИ от НСД.

2. Убедиться в наличии:

- лица, ответственного за учет паролей и управление средствами аутентификации;

- возможности СЗИ от НСД вести учет и производить блокирование.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если назначено лицо, ответственное за учет паролей и управление средствами аутентификации; и все пароли учтены в журнале, возможности СЗИ от НСД позволяют вести учет и производить блокировку системы.

А.2.3 Проверка защиты обратной связи при вводе аутентификационной информации.

Метод: экспертно-технический.

Методика:

1. Включить (перезагрузить) АРМ (или Сервер).

2. Ввести верный пароль.

3. Убедиться в наличии маскирования символов вводимого пароля «звездочками».

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если при вводе пароля символы вводимого пароля маскируются «звездочками».

А.3. Испытание подсистемы управления доступом субъектов доступа к объектам доступа

А.3.1 Проверка управления (заведение, активация, блокирование и уничтожение) учётными записями пользователей

Метод: экспертно-технический.

Методика:

1. Включить (перезагрузить) АРМ.

2. Осуществить вход в операционную систему под учётной записью с правами администратора информационной безопасности.

3. Создать новую учётную запись с правами пользователя.

4. Присвоить созданной учётной записи пароль в соответствии с используемыми в системе правилами (длина, сложность пароля).

5. Выйти из системы или перезагрузить компьютер.

6. Осуществить попытку входа в операционную систему под созданной учетной записью в п.п. 3.

7. Перезагрузить компьютер или выйти из системы.

8. Осуществить блокирование созданной учетной записи в п.п. 3 путем превышения допустимого количества ошибок ввода пароля.

9. Повторить попытку входа, аналогичную п.п. 6.

10.Осуществить вход в операционную систему с правами администратора информационной безопасности.

11.Удалить учётную запись, созданную в п.п. 3.

12.Повторить проверку входа, аналогичную п.п. 6.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если в результате выполнения п. 6 методики доступ пользователю будет разрешен, а выполнения п. 9 и 12 методики доступ пользователю будет запрещён.

А.3.2 Проверка разделения полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

Метод: экспертно-документальный, экспертно-технический.

Методика:

1. Проанализировать содержание эксплуатационной и организационно-распорядительной документации.

2. Убедиться, что в содержании документации описаны разделения полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование системы.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если в документации описаны разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование системы.

А.3.3 Проверка назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

Метод: экспертно-документальный.

Методика:

1. Проанализировать содержание эксплуатационной и организационно-распорядительной документации.

2. Убедиться, что назначены минимально необходимые права и привилегии пользователям, администратору информационной безопасности и лицам, обеспечивающим функционирование информационной системы.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если назначены минимально необходимые права и привилегии пользователям, администратору информационной безопасности и лицам, обеспечивающим функционирование информационной системы.

А.3.4 Проверка ограничения неуспешных попыток входа в систему.

Метод: экспертно-технический.

Методика:

1. Осуществить попытку входа под учетной записью произвольного пользователя с несоответствующим ей паролем.

2. Повторять попытки неудачного входа до тех пор, пока компьютер не будет временно заблокирован.

3. Зафиксировать количество неудачных попыток входа.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если количество неудачных попыток входа до блокировки системы соответствует политике безопасности СЗИ от НСД.

А.3.5 Проверка блокирования сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

Метод: экспертно-технический.

Методика:

1. Осуществить вход в операционную систему под учётной записью произвольного пользователя.

2. Осуществить блокировку компьютера.

3. Разблокировать заблокированный в п. 2 компьютер.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если в ходе выполнения п. 2 компьютер блокируется, а в п. 3 выполняется его разблокирование.

А.3.6 Проверка разрешения (запрета) действий пользователей до идентификации и аутентификации

Метод: экспертно-технический.

Методика:

1. Включить (перезагрузить) АРМ (или Сервер).

2. Осуществить попытку входа в BIOS.

3. Убедиться, что вход в BIOS разрешен только администратору информационной безопасности.

4. Перезагрузить компьютер.

5. Осуществить попытку загрузки системы с оптического привода.

6. Убедиться, что право загрузки с оптического привода имеет только администратор информационной безопасности.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если в ходе выполнения п.п. 2 и 5 методики операции выполняются в соответствии с разрешениями безопасности, установленными для системы.

А.4. Испытание подсистемы защиты машинных носителей персональных данных

А.4.1 Проверка уничтожения (стирания) персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации

Метод: экспертно-документальный.

Методика:

1. Изучить представленную эксплуатационную и организационно-распорядительную документацию.

2. Убедиться в наличии процедуры уничтожения (стирания) персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если имеется задокументированная процедура уничтожения (стирания) персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации.

А.5. Испытание подсистемы регистрации событий безопасности

А.5.1 Проверка регистрации событий безопасности, и сроков их хранения

Метод: экспертно-технический.

Методика:

1. Осуществить вход в операционную систему АРМ (или Сервера) с правами администратора информационной безопасности.

2. Проанализировать систему регистрации событий СЗИ от НСД.

3. Убедиться, что в системе регистрации событий СЗИ от НСД можно просмотреть зарегистрированные события, а также убедиться, что события будут храниться в течении длительного периода времени.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если выполняется п. 3 методики.

А.5.2 Проверка состава и содержания информации о событиях безопасности, подлежащих регистрации

Метод: экспертно-технический.

Методика:

1. Осуществить вход в операционную систему под учетной записью с правами администратора информационной безопасности.

2. Проанализировать систему регистрации событий СЗИ от НСД.

3. Убедиться, что журналы событий безопасности отражают следующую информацию:

события входа в систему (дата и время, код события, тип идентификатора, серийный номер идентификатора, имя пользователя, пароль в случае неправильного ввода)

события запуска программ (дата и время, код события, имя объекта, имя процесса, имя пользователя, гриф объекта, допуск процесса)

события доступа к объектам

события контроля целостности (дата и время, код события, имя файла)

события действий администратора

события управления объектами доступа

события управления пользователями

события управления носителями

события управления устройствами

события системы защиты

события печати.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если выполняется п. 3 методики.

А.5.3 Проверка сбора, записи и хранения информации о событиях безопасности в течении установленного периода времени

Метод: экспертно-технический.

Методика:

1. Осуществить вход в операционную систему под учетной записью с правами администратора информационной безопасности.

2. Проанализировать систему регистрации событий СЗИ от НСД.

3. Убедиться, что сбор, запись и хранение информации о событиях безопасности производятся в течении длительного периода времени.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если выполняется п. 3 методики.

А.5.4 Проверка защиты информации о событиях безопасности

Метод: экспертно-технический, экспертно-документальный.

Методика:

1. Загрузить операционную систему на АРМ (или на Сервере).

2. Осуществить вход в операционную систему под учетной записью с правами администратора информационной безопасности.

3. Проанализировать настройки журнала регистрации событий безопасности операционной системы и матрицу доступа.

4. Убедиться, что установлены права доступа к журналу регистрации событий ОС.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если выполняется п. 4 методики.

А.6. Испытание подсистемы антивирусной защиты

А.6.1 Проверка реализации антивирусной защиты

Метод: экспертно-технический.

Методика:

1. Загрузить операционную систему на АРМ (или на Сервере).

2. Осуществить вход в операционную систему под учетной записью с правами администратора информационной безопасности.

3. Запустить антивирусную программу.

4. Убедиться в соответствии установленного антивирусного ПО Техниче-скому паспорту системы.

5. Убедиться, что запуск и работа антивирусного ПО происходят в соответствии с ТУ на ПО и руководством производителя.

6. Убедиться в том, что установленное антивирусное ПО автоматически запускается при загрузке ОС и выполняет непрерывное и периодическое (по требованию пользователя) сканирование файловой системы и областей оперативной памяти на наличие вредоносных программ.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если п.п. 3, 4, 5 и 6 методики успешно выполнены.

А.6.2 Проверка обновления базы данных признаков вредоносных компьютерных программ (вирусов)

Метод: экспертно-технический.

Методика:

1. Осуществить вход в операционную систему под учетной записью с правами администратора информационной безопасности.

2. Запустить антивирусную программу.

3. Проверить дату последнего обновления антивирусной программы.

4. Убедиться, что антивирусные базы антивирусного ПО находятся в актуальном состоянии и выполнены все необходимые другие обновления антивирусного ПО.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если п. 4. методики успешно выполнен.

А.7. Испытание подсистемы контроля (анализа) защищенности персональных данных

А.7.1 Проверка установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

Метод: экспертно-технический.

Методика:

1. Осуществить вход в операционную систему под учетной записью с правами администратора информационной безопасности.

2. Убедиться, что для операционной системы, программного обеспечения, установлены все необходимые обновления.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если для операционной системы, программного обеспечения, установлены все необходимые обновления.

А.7.2 Проверка работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

Метод: экспертно-документальный, экспертно-технический.

Методика:

1. Изучить требования и ограничения по эксплуатации программного обеспечения и средств защиты информации, приведенные в эксплуатационной документации на ПО и СЗИ.

2. Проверить параметры настройки и правильность функционирования ПО и СЗИ.

3. Убедиться в соответствии реальных условий эксплуатации ПО и СЗИ требованиям эксплуатационной документации.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если ПО и СЗИ корректно настроены и правильно функционируют, а также условия эксплуатации ПО и СЗИ соответствуют требованиям эксплуатационной документации.

А.7.3 Проверка состава технических средств, программного обеспечения и средств защиты информации

Метод: экспертно-документальный, экспертно-технический.

Методика:

1. Изучить состав технических средств, программного обеспечения и средств защиты информации.

2. Убедиться в соответствии состава технических средств, программного обеспечения и средств защиты информации техническому паспорту.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если состав технических средств, программного обеспечения и средств защиты информации соответствует техническому паспорту.

А.8. Испытание защиты технических средств

А.8.1 Проверка контроля и управления физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы

Метод: экспертно-документальный.

Методика:

1. Проанализировать условия размещения технических средств.

2. Проанализировать достаточность мер по контролю физического доступа в помещение, в котором расположены технические средства, средства защиты информации обрабатывающие персональные данные.

3. Проанализировать достаточность принятых мер по физической охране средств вычислительной техники и носителей информации.

4. Проанализировать содержание организационно-распорядительной документации.

5. Убедиться, что указанная документация содержит списки сотрудников оператора, допущенных к обработке конфиденциальной информации, включая персональные данные.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если принятые меры по контролю физического доступа в помещение, в котором расположены технические средства, средства защиты информации и средства криптографической защиты информации, а также меры по физической охране средств вычислительной техники и носителей информации исключают или существенно затрудняют несанкционированный физический доступ, а также если представлены все документы, перечисленные в п. 5 методики, либо аналогичные им по содержанию.

А.8.2 Проверка размещения устройств вывода (отображения) информации, исключающего ее несанкционированный просмотр

Метод: экспертно-документальный.

Методика:

1. Проанализировать условия размещения технических средств.

2. Оценить возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей конфиденциальные сведения.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если размещение технических средств исключает возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей конфиденциальные сведения.

А.9. Испытание подсистемы управления конфигурацией информационной системы и системой защиты персональных данных

А.9.1 Проверка определения лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных

Метод: экспертно-аналитический, экспертно-документальный.

Методика:

1. Проанализировать содержание совокупности представленной технической, эксплуатационной и организационно-распорядительной документации.

2. Убедиться, что в содержании документов определены лица, которым разрешены действия по внесению изменений в конфигурацию строго по инструкциям, разработанным для них, при условии, что эти изменения не снижают уровень защищенности информации.

3. Провести опрос:

- ответственного за обеспечение безопасности персональных данных;
- администратора информационной безопасности;
- ответственного за эксплуатацию ИСПДн;
- пользователя;

4. Убедиться, что все лица, перечисленные в п. 3 методики, осведомлены о своих должностных обязанностях, принятом технологическом процессе об-

работки информации, требованиях организационно-распорядительной документации по защите информации и ответственности за их нарушение.

5. Убедиться, что все лица, перечисленные в п. 3 методики, осведомлены о том, что при эксплуатации системы защиты информации категорически запрещается вносить изменения в комплектность системы защиты информации, в состав, конструкцию, конфигурацию, коммутацию, размещение средств вычислительной техники, в состав и настройки программно-технических средств, в том числе средств защиты информации и средства криптографической защиты информации, которые могут снизить уровень защищенности информации.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если определены лица, которым разрешены действия по внесению изменений в конфигурацию строго по инструкциям, разработанным для них, при условии, что эти изменения не снижают уровень защищенности информации, а также, лица, перечисленные в п. 3 методики, осведомлены о своих должностных обязанностях, требованиях безопасности информации при эксплуатации системы защиты информации.

А.9.2 Проверка управления изменениями конфигурации информационной системы и системы защиты персональных данных

Метод: экспертно-аналитический.

Методика:

1. Убедиться, что ответственный за обеспечение безопасности персональных данных осведомлен о том, что в случае изменений состава, конструкции, конфигурации, коммутации, размещения средств вычислительной техники, состава и настроек программно-технических средств, в том числе средств защиты информации и средства криптографической защиты информации, которые могут снизить уровень защищенности информации, обязан известить об этом орган по аттестации, выдавший «Аттестат соответствия...».

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если ответственный за обеспечение безопасности персональных данных осведомлен о своих должностных обязанностях при управлении изменениями конфигурации системы защиты информации, содержащей персональные данные, и анализе потенциального воздействия планируемых изменений в конфигурацию системы защиты информации.

А.9.3 Проверка осведомленности ответственного за обеспечение безопасности персональных данных при управлении изменениями конфигурации системы защиты информации, содержащей персональные данные, и анализе

потенциального воздействия планируемых изменений в конфигурацию системы защиты информации

Метод: экспертно-аналитический.

Методика:

1. Убедиться, что ответственный за обеспечение безопасности персональных данных осведомлен о том, что в случае изменений состава, конструкции, конфигурации, коммутации, размещения средств вычислительной техники, состава и настроек программно-технических средств, в том числе средств защиты информации и средства криптографической защиты информации, которые могут снизить уровень защищенности информации, обязан известить об этом орган по аттестации, выдавший «Аттестат соответствия...».

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если ответственный за обеспечение безопасности персональных данных осведомлен о своих должностных обязанностях при управлении изменениями конфигурации системы защиты информации, содержащей персональные данные, и анализе потенциального воздействия планируемых изменений в конфигурацию системы защиты информации.

А.9.4 Проверка документирования информации об изменениях в конфигурации информационной системы и системы защиты информации персональных данных

Метод: экспертно-документальный.

Методика:

1. Проанализировать содержание организационно-распорядительной документации.

2. Убедиться в наличии листа регистрации изменений в техническом паспорте.

Критерий:

меры по обеспечению безопасности персональных данных считаются эффективными, если технический пас-порт содержит лист регистрации изменений.

7 ОЦЕНКА РЕЗУЛЬТАТОВ ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Объект информатизации признается успешно прошедшим оценку эффективности, если он успешно прошел все проверки, приведенные в разделе 6 настоящего документа. В противном случае объект информатизации признается не прошедшим оценку эффективности.

8 ОТЧЕТНОСТЬ ПО РЕЗУЛЬТАТАМ ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Результаты оценки эффективности отражаются в заключении по результатам оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных информационной системы персональных данных ГБПОУ МО «Воскресенский колледж» «Бухгалтерия», «Отдел кадров», «Учебной части СП №1, СП №2, СП №3»..

Заместитель директора ГБПОУ МО
«Воскресенский колледж» по безопасности М.И. Милашук