ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2020 год

Содержание

1. Термины и сокращения

ИСПДн	– информационная система персональных данных
СЗПДн	– система (подсистема) защиты персональных данных
СКЗИ	– средства криптографической защиты информации
НСД	– несанкционированный доступ

2. Общие положения

2.1. Администратор безопасности информационной системы персональных данных (Администратор безопасности) отвечает за обеспечение необходимого уровня состояния защиты ИСПДн, правильность настройки средств защиты, организацию выдачи, хранения и уничтожения материальных носителей персональных данных.

2.2. Администратор безопасности назначается и освобождается от исполнения своих обязанностей распоряжением главы Администрации городского округа Электросталь Московской области, в приделах полномочий подчиняется ответственному лицу за организацию обработки персональных данных.

2.3. Администратор безопасности утверждает изменения состава и конфигурации технических и программных средств после их анализа на соответствие политике безопасности.

2.4. Все добавляемые компоненты должны быть проверены на работоспособность и отсутствие вирусов.

3. Обязанности Администратора безопасности информационной системы персональных данных

3.1. Администратор безопасности обязан:

а. разработать и исполнять утверждённый план проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного распространения и доступа, искажения и утраты информации;

б. вести разъяснительную работу с сотрудниками по вопросам информационной безопасности;

в. обеспечить полное стирание персональных данных с электронных носителей в случаях их передачи для обслуживания или ремонта;

г. обеспечить уничтожение со съёмных носителей персональных данных, не предназначенных для дальнейшего использования, методом многократной перезаписи без возможности восстановления;

д. проверять электронный журнал обращений к ИСПДн;

е. контролировать надлежащее функционирование программных и технических средств защиты информации, входящих в состав ИСПДн, во всех режимах работы, а именно:

1) использование только лицензионного (сертифицированного) программного обеспечения;
2) использование только сертифицированных средств защиты информации;
3) соблюдение условий использования и правильность конфигурирования (настройки) средств защиты информации.

3.2. В обязанности Администратора безопасности входит:

а. проведение разбирательств и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации.

б. уничтожение пришедших в негодность съемных носителей персональных данных. Форма акта об уничтожении приведена в Приложении А.

4. Мониторинг

4.1. Мониторинг парольной защиты и контроль надёжности пользовательских паролей предусматривают:

а. установление сроков действия паролей – минимального и максимального;

б. периодическую проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей.

4.2. Мониторинг целостности программного обеспечения включает следующие действия:

а. проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств защиты при загрузке операционной системы;

б. обнаружение дубликатов идентификаторов пользователей;

в. восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

4.3. Антивирусный контроль: Администратор безопасности контролирует регулярность обновления антивирусных баз на рабочих станциях и серверах.

5. Системный аудит

5.1. Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесенных изменений в системное программное обеспечение.

5.2. Обзоры безопасности проводятся с целью проверки текущего уровня безопасности систем, обрабатывающих персональные данные. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующем специально составленному списку для проверки.

5.3. Обзоры безопасности содержат:

а. отчёты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имён и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;

б. проверку правомочности предоставления прав доступа пользователей к сетевым ресурсам;

в. проверку содержимого файлов конфигурации на соответствие списку для проверки;

г. обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

д. проверку прав доступа и других атрибутов системных файлов;

е. проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

ж. проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

5.4. Активное тестирование надёжности механизмов контроля доступа производится путём осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

5.5. Пассивное тестирование механизмов контроля доступа осуществляется путём анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т.е. таких состояний, в которых могут проявлять себя известные уязвимости.

6. Анализ инцидентов

6.1. Если Администратор безопасности информационной системы персональных данных подозревает или получил сообщение о том, что система подвергается атаке или уже была скомпрометирована, то он должен установить:

а. факт попытки несанкционированного доступа (НСД);
б. продолжается ли НСД в настоящий момент;
в. кто является источником НСД;
г. что является объектом НСД;
д. когда происходила попытка НСД;
е. как и при каких обстоятельствах была предпринята попытка НСД;
ж. точка входа нарушителя в систему;
з. была ли попытка НСД успешной;
и. определить системные ресурсы, безопасность которых была нарушена;
к. какова мотивация попытки НСД.

6.2. Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

6.3. При анализе системных журналов Администратору безопасности необходимо произвести следующие действия:

a. проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
б. проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
в. просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
г. проверить наличие мест в системных журналах, которые выглядят необычно;
д. выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;
е. выявить наличие неудачных попыток входа в систему.

6.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

a. проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;
б. проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
в. проверить наличие мест в журналах, которые выглядят необычно;
г. выявить попытки изменения таблиц маршрутизации и адресных таблиц;
д. проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

6.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

a. составить базовую схему того, как обычно выглядит система;
б. провести поиск подозрительных файлов и каталогов, которые могли быть использованы злоумышленниками;

в. проверить содержимое системных файлов, которые могли быть изменены злоумышленниками;
г. проверить целостность системных программ;
д. проверить систему аутентификации и авторизации.

6.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

6.7. Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

7. Контроль резервного копирования и восстановления информации

7.1. На этапе исполнения администратором «Плана резервного копирования», Администратор безопасности обязан контролировать сроки создания копий, анализировать состояние носителей (количество сбойных участков, объем свободного места) и незамедлительно докладывать руководству обо всех произошедших или ожидаемых отклонениях от плана.

7.2. Администратор безопасности согласовывает разработанный администратором ИСПДн «Регламент восстановления повреждённых или утраченных данных информационной системы».

8. Шифрование данных

8.1. При необходимости шифрования данных, обрабатываемых с помощью технических средств ИСПДн, и/или резервных копий информации ИСПДн администратор безопасности производит необходимые действия:

а. выдача персональных идентификаторов или ключевых носителей СКЗИ пользователям ИСПДн;
б. ведение журналов регистрации, учёта и выдачи носителей информации поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
в. шифрование резервных копий, содержащих персональные данные, обрабатываемые в информационной системе, сертифицированными алгоритмами.

8.2. Дополнительные требования к Администратору безопасности в связи с использованием средств шифрования данных могут быть определены в специальных регламентах работы с шифрованием информации ИСПДн.

9. Действия по фактам несоблюдения требований по защите персональных данных

9.1. При выявлении фактов несоблюдения условий и требований по защите персональных данных и использования средств защиты персональных данных, Администратор безопасности обязан произвести следующие действия:

а. Незамедлительно сообщить о происшедшем руководству;
б. Собрать возможные факты (свидетельства) несоблюдения условий и требований по защите персональных данных и использования средств защиты персональных данных;
в. Сформировать Экспертную комиссию по расследованию инцидента (при необходимости с привлечением внешних экспертов, представителей лицензиатов ФСТЭК России);
г. Экспертная комиссия составляет заключение условий и требований по защите персональных данных и использования средств защиты персональных данных.

9.2. Составленное Экспертной комиссией заключение является основанием для наложения административного и (или) дисциплинарного взыскания на виновных лиц.

9.3. Экспертная комиссия при расследовании инцидентов, связанных с нарушением обеспечения защищенности персональных данных, вправе производить обследование объектов ИСПДн с согласия ответственного лица за организацию обработки персональных данных.

10. Порядок приостановки предоставления персональных данных

10.1. Администратор безопасности, при получении информации или самостоятельно выявив нарушения порядка предоставления персональных данных данные, предпринимает следующие действия:

а. незамедлительно приостанавливает работу с персональными данными субъектов;
б. сообщает о происшедшем руководству;
в. самостоятельно или с привлечением дополнительных специалистов выявляет причины возникновения нарушения;
г. в случае выявления и устранения причины нарушения Администратор безопасности восстанавливает работу с персональными данными субъектов и сообщает о причинах нарушения и своих действиях руководству;
д. в случаях невозможности оперативного выявления причин нарушения, проводится служебное разбирательство. Только по его завершению и устранению причин нарушения восстанавливается работа с персональными данными;
е. все действия в процессе реагирования на нарушение порядка предоставления персональных данных должны документироваться администратором безопасности в «Журнале учета нарушений порядка предоставления персональных данных», форма журнала представлена в Приложении Б.

11. Права администратора безопасности информационной системы персональных данных

11.1. Администратор безопасности имеет право:

а. Требовать от сотрудников соблюдения правил работы со средствами защиты информации, СКЗИ, входящими в состав ИСПДн.

б. Осуществлять взаимодействие (давать необходимые рекомендации, проводить консультации, получать требующиеся сведения) с сотрудниками по вопросам эксплуатации технических и программных СЗПДн с целью улучшения качества их работы, а также своевременного предупреждения аварийных ситуаций.

в. Для нейтрализации актуальных угроз безопасности персональных данных осуществлять выбор средств защиты информации выполняющие меры, представленные в Приложении В, в соответствии с уровнем защищенности персональных данных, установленным в Администрации городского округа Электросталь Московской области.

12. Ответственность администратора безопасности информационной системы персональных данных

12.1. Администратор безопасности несёт ответственность:

а. за неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящей инструкцией.

б. за совершенные в процессе осуществления своей деятельности правонарушения – в пределах, определённых действующим административным, уголовным и гражданским законодательством Российской Федерации.

в. за причинение материального ущерба – в пределах, определённых действующим трудовым, уголовным и гражданским законодательством Российской Федерации.

ПРИЛОЖЕНИЕ А

Форма акта уничтожения съёмных носителей персональных данных

АКТ
уничтожения съёмных носителей персональных данных

Комиссия, наделённая полномочиями распоряжения от___ _____ 20__ г. №____ в составе:

Должность	ФИО

провела отбор съёмных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
1	2	3	4

Всего съёмных носителей _____
(цифрами и прописью)

На съёмных носителях уничтожена конфиденциальная информация путём стирания её на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены путем _____
(разрезания, демонтажа и т.п.)

измельчены и сданы для уничтожения организации, предприятию по утилизации вторичного сырья:

_____
(наименование предприятия) (Дата)

Председатель комиссии: _____ _____

Члены комиссии: _____ _____

_____ _____

_____ _____
Подпись Дата

ПРИЛОЖЕНИЕ Б

ЖУРНАЛ

учета нарушений порядка предоставления персональных данных

№ п/п	Дата, время обнаружения нарушения	ИСПДн в которой обнаружено нарушение	Дата, время устранения нарушения	Результат	Подпись ответственного сотрудника	Примечания

ПРИЛОЖЕНИЕ В

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения 3 уровня защищенности персональных данных

Условное обозначение и номер меры	**Содержание мер по обеспечению безопасности персональных данных**
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
IV. Защита машинных носителей персональных данных (ЗНИ)	
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление 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, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных