|  |
| --- |
| **УТВЕРЖДАЮ**  Генеральный директор  ООО «ВЛАДЕЛЕЦ ИСПДН» |
| \_\_\_\_\_\_\_\_\_\_\_\_ |
|  |

**ИНСТРУКЦИЯ**

**по эксплуатации системы защиты персональных данных**

**информационной системы персональных данных**

**«ВЛАДЕЛЕЦ ИСПДН»**

**ООО «ВЛАДЕЛЕЦ ИСПДН»**

# ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция определяет порядок эксплуатации системы защиты персональных данных (далее по тексту – СЗПДн) информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» (далее по тексту – ИСПДн «ВЛАДЕЛЕЦ ИСПДН», ИС) в части обеспечения защиты информации, в т.ч. обеспечения безопасности персональных данных (далее - ПДн), порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок контроля соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты.

Действие настоящей Инструкции распространяется на вопросы, связанные с обработкой защищаемой информации, в т.ч. ПДн, в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», осуществляемой с использованием средств автоматизации.

# ОСНОВНЫЕ ТРЕБОВАНИЯ

2.1 Обеспечение защиты информации (ПДн) в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» достигается применением организационных и технических мер, причем в интересах обеспечения безопасности в обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПДн, и носители информации.

2.2 Основными мерами защиты информации (ПДн) являются:

* реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (ИР) ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и связанным с ее использованием работам, документам;
* ограничение доступа пользователей в помещения, где размещены технические средства (ТС) ИСПДн «ВЛАДЕЛЕЦ ИСПДН», позволяющие осуществлять обработку ПДн, а также хранятся носители информации;
* разграничение доступа пользователей и обслуживающего персонала к ИР, программным средствам обработки (передачи) и защиты информации;
* регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа (НСД) и действий пользователей, обслуживающего персонала и посторонних лиц;
* учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
* резервирование ТС, дублирование массивов и носителей информации;
* использование СЗИ, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации;
* использование защищенных каналов связи;
* размещение ТС, позволяющих осуществлять обработку ПДн в пределах охраняемой территории;
* размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;
* организация физической защиты помещений и собственно ТС, позволяющих осуществлять обработку ПДн;
* предотвращение внедрения в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» вредоносных программ (программ-вирусов) и программных закладок.

# ПОРЯДОК ДОПУСКА ПОЛЬЗОВАТЕЛЕЙ К РАБОТЕ НА АРМ

Разрешительная система доступа представляет собой совокупность процедур оформления прав субъектов на доступ к информационным ресурсам (ИР) (объектам доступа) ИСПДн «ВЛАДЕЛЕЦ ИСПДН», а также прав и обязанностей ответственных лиц, осуществляющих реализацию этих процедур.

Информация, подлежащая защите в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» включаются в «Перечень защищаемых информационных ресурсов в информационной системе персональных данных…», утверждаемый приказом «ВЛАДЕЛЕЦ ИСПДН»;

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» объектами доступа являются:

* информация, обрабатываемая в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», включая персональные данные;
* технические средства, включая средства вычислительной техники, машинные носители информации, технические средства обработки информации, системы и средства связи и передачи данных;
* системное, общесистемное и прикладное (специальное) программное обеспечение;
* средства защиты информации.

Субъектами доступа в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» являются:

* администраторы безопасности, осуществляющие администрирование СЗПДн;
* системные администраторы, осуществляющие администрирование системного, общесистемного и прикладного программного обеспечения;
* пользователи ИСПДн «ВЛАДЕЛЕЦ ИСПДН», осуществляющие работу с информационными ресурсами «ВЛАДЕЛЕЦ ИСПДН» в рамках выполнения своих должностных (трудовых) обязанностей.

Субъекты доступа несут персональную ответственность за соблюдение ими установленного на объекте информатизации порядка обеспечения защиты информационных ресурсов.

Ответственным лицом, осуществляющим реализацию процедур оформления прав субъектов на доступ к информационным ресурсам ИСПДн «ВЛАДЕЛЕЦ ИСПДН», является администратор системы защиты информации.

Права по установке и удалению программного обеспечения в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» предоставлены только сотрудникам, обладающим правами администратора.

Процедура регистрации (создания учетной записи) пользователя и предоставления (или изменения) ему административных прав доступа к ресурсам ИСПДн «ВЛАДЕЛЕЦ ИСПДН» осуществляется с использованием сертифицированных средств защиты информации от несанкционированного доступа.

При изменении должностных обязанностей сотрудника, имевшего административные права доступа, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя подлежит изменению (корректировке), при этом старые полномочия аннулируются.

После внесения изменений в Матрицу доступа Администратор средств и систем защиты персональных данных производит настройку средств защиты рабочих станций (автоматизированных рабочих мест).

Контроль выполнения требований разрешительной системы доступа к защищаемой информации (ПДн) возлагается на ответственного за обеспечение безопасности персональных данных.

* 1. **Контроль функционирования разрешительной системы допуска к информационным ресурсам организации**

Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

* планом основных мероприятий по защите информации на текущий год;
* функциональными обязанностями должностных лиц;
* приказами/распоряжениями руководителя структурного подразделения.

Контроль функционирования разрешительной системы допуска к информационным ресурсам ИСПДн «ВЛАДЕЛЕЦ ИСПДН» осуществляется ответственными лицами. Организация контроля возлагается на ответственного за обеспечение безопасности персональных данных.

# ПОРЯДОК ДОПУСКА СОТРУДНИКОВ И ИНЫХ ЛИЦ В ПОМЕЩЕНИЯ С ЭЛЕМЕНТАМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

**3.1 Требования к помещениям, в которых расположены элементы ИСПДн**

Бесконтрольный доступ посторонних лиц в помещения с элементами ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должен быть исключён.

Для защиты помещений, в которых расположены технические средства ИСПДн «ВЛАДЕЛЕЦ ИСПДН», должны приниматься меры для минимизации воздействий огня, дыма, воды, пыли, взрыва, химических веществ, а также кражи.

**3.2 Доступ в помещения, в которых расположены элементы ИСПДн «ВЛАДЕЛЕЦ ИСПДН»**

Должен быть определен список помещений, предназначенных для обработки ПДн средствами ИСПДн «ВЛАДЕЛЕЦ ИСПДН», и организован контроль доступа служащих в помещения, в которых установлены технические средства (далее - ТС) ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и осуществляется обработка ПДн, а также хранятся машинные носители информации (ПДн).

Доступ сотрудников структурных подразделений в помещения, в которых осуществляется обработка ПДн, организовывается на основании утвержденных руководителем «Правил доступа в помещения с информационной системой персональных данных в рабочее и нерабочее время, а также в нештатных ситуациях».

Доступ посторонних лиц в помещения с элементами ИСПДн «ВЛАДЕЛЕЦ ИСПДН», должен осуществляется только ввиду служебной необходимости и в сопровождении ответственных лиц.

На момент присутствия посторонних лиц в помещении ИСПДн «ВЛАДЕЛЕЦ ИСПДН», должны быть приняты меры по недопущению ознакомления посторонних лиц с ПДн.

По окончании рабочего дня помещения с элементами ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должны сдаваться под охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты.

1. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

## Требования к организации парольной защиты

Личные пароли пользователей, обладающих правами администратора, должны генерироваться и распределяться централизованно администратором системы защиты персональных данных либо выбираться пользователями ИСПДн «ВЛАДЕЛЕЦ ИСПДН» самостоятельно.

В случае формирования личных паролей пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на администратора средств и систем защиты персональных данных.

Полная плановая смена паролей в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» проводится не реже одного раза в 90 дней.

Внеплановая смена личного пароля пользователя или удаление учетной записи в случае прекращения его полномочий (увольнение, переход на другую должность и т.п.) должна производиться администратором средств и систем защиты персональных данных немедленно после окончания последнего сеанса работы пользователя в ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) пользователя, равное 5, после чего учетная запись блокируется.

Разблокирование учетной записи осуществляется администратором средств и систем защиты персональных данных.

В случае утечки информации о зарегистрированном пользователе необходимо немедленно удалить данные об этом пользователе и зарегистрировать заново его с новым идентификатором.

Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора средств и систем защиты персональных данных.

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора средств и систем защиты персональных данных.

Владельцы паролей должны быть предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

## Требования к формированию паролей

Администратор средств и систем защиты персональных данных ИСПДн «ВЛАДЕЛЕЦ ИСПДН» при формировании паролей должен руководствоваться следующими требованиями:

Длина пароля должна быть не менее 6 символов.

В пароле должны обязательно присутствовать символы из следующих:

буквы в верхнем регистре;

буквы в нижнем регистре;

цифры;

специальные символы, не принадлежащие алфавитно-цифровому набору (например: !, @, #, $, &, \*, % и т.п.).

Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.).

Пароль не должен содержать имя учетной записи пользователя, а также какую-либо его часть.

Пароль не должен основываться на именах и датах рождения пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о пользователе.

Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.).

Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.).

При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

## Правила ввода паролей

Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и пр.).

В случае блокировки учетной записи пользователя после превышения попыток ввода данных аутентификации (логина и пароля) в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», пользователю необходимо уведомить Администратора средств и систем защиты персональных данных для проведения процедуры разблокировки его учетной записи.

1. ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

Организация антивирусной защиты в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» осуществляется администратором средств и систем защиты персональных данных.

Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется администратором средств и систем защиты персональных данных.

## Организация антивирусного контроля в ИСПДн

К использованию в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» допускаются только лицензионные и сертифицированные ФСТЭК России антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля, а также обновление антивирусных баз в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», осуществляется администратором средств и систем защиты персональных данных в соответствии с руководствами по применению конкретных антивирусных средств.

Контроль целостности и антивирусный контроль всех дисков и файлов элементов ИСПДн «ВЛАДЕЛЕЦ ИСПДН», должен проводиться регулярно в автоматическом режиме в соответствии с установленным расписанием.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, CD-ROM и т.п

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения, администратором системы защиты персональных данных должна быть выполнена антивирусная проверка.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан поставить в известность администратора системы защиты персональных данных ИСПДн «ВЛАДЕЛЕЦ ИСПДН», который обязан в таком случае провести внеочередной антивирусный контроль.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов администратор системы защиты персональных данных обязан:

* приостановить работу ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
* совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
* провести лечение или уничтожение зараженных файлов.

Администратор средств и систем защиты персональных данных проводит лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, администратор средств и систем защиты персональных данных обязан запретить работу в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», и в возможно короткие сроки обновить пакет антивирусных программ.

1. ОРГАНИЗАЦИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ

Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационной системы в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

Резервное копирование и хранение данных должно осуществляться на периодической основе:

* 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 «ВЛАДЕЛЕЦ ИСПДН» – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Резервному копированию подлежит информация следующих основных категорий:

* персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений);
* информация, обрабатываемая пользователями в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», а также информация, необходимая для восстановления работоспособности ИСПДн «ВЛАДЕЛЕЦ ИСПДН», в т.ч. общего пользования и справочно-информационные системы общего использования;
* рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;
* регистрационная информация системы защиты персональных данных ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;
* другая информация, по мнению администраторов являющаяся критичной для работоспособности ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

В случае необходимости восстановления данных из резервной копии, для восстановления следует использовать наиболее поздний архив. В случае невозможности использования наиболее позднего архива по каким-либо причинам, архив, используемый для восстановления, выбирается решением администратора системы защиты персональных данных.

Физический доступ к архивным копиям предоставляется только администраторам, наделенным соответствующими полномочиями.

Передача машинных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

Уничтожение отделяемых машинных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию.

В случае необходимости восстановление данных из резервных копий производится администратором системы защиты персональных данных или системным администратором, наделенным соответствующими полномочиями.

Восстановление данных из резервных копий происходит в случае их исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

При частичном нарушении или исчезновении записей данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением настоящей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора системы защиты персональных данных.

1. ПОРЯДОК ОБРАЩЕНИЯ, ХРАНЕНИЯ И УНИЧТОЖЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ

При обращении с машинными носителями информации (НЖМД, CD, DVD, флэш-накопители т.д.) выполняются следующие основные правила:

* машинные носители информации, срок эксплуатации которых истек, уничтожаются в установленном порядке;
* все съемные носители информации хранятся в безопасном месте в соответствии с требованиями по их эксплуатации.

Машинные носители информации, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

Уничтожение машинных носителей информации осуществляется администратором системы защиты персональных данных.

Уничтожение магнитных, оптических, магнитооптических и электронных носителей информации производится путем их физического разрушения. Перед уничтожением носителя информация с него стирается (уничтожается), если это позволяют физические принципы работы носителя.

Перед утилизацией оборудования, участвующего в обработке информации (ПДн), администратором системы защиты персональных данных осуществляется проверка всех его компонентов, включая носители информации (жесткие диски) на отсутствие информации и лицензированного программного обеспечения (ПО).

По результатам уничтожения составляется «Акт уничтожения машинных носителей персональных данных», который в последующем хранится у администратора системы защиты персональных данных, уничтоженные машинные носители информации (утилизированное оборудование) снимаются с материального учета.

1. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ ВОЗНИКНОВЕНИЯ НЕШТАТНЫХ СИТУАЦИЙ

Общими требованиями ко всем лицам, допущенным к работе в информационной системе в случае возникновения нештатной ситуации или другого инцидента, являются:

* лицо, обнаружившее нештатную ситуацию или другой инцидент, немедленно ставит в известность администратора системы защиты персональных данных;
* администратор средств и систем защиты персональных данных обязан провести анализ ситуации и в случае невозможности исправить положение поставить в известность ответственного за обеспечение безопасности персональных данных. Для локализации (блокирования) проявлений угроз информационной безопасности ответственный за обеспечение безопасности персональных данных может привлекать администраторов ИСПДн «ВЛАДЕЛЕЦ ИСПДН», имеющих соответствующие полномочия и обладающих достаточной компетенцией;
* по факту возникновения инцидента и выяснению причин его проявления по решению руководства может быть назначена комиссия по реагированию на инциденты информационной безопасности и проведено служебное расследование.

**8.1 Действия пользователей ИСПДн при возникновении нештатных ситуаций**

8.1.1 Сбой программного обеспечения.

Администратор средств и систем защиты персональных данных выясняет причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копии акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. В случае необходимости о произошедшем инциденте администратор средств и систем защиты персональных данных сообщает ответственному за обеспечение безопасности персональных данных для принятия решения по существу.

8.1.2 Отключение электропитания технических средств ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Администратором средств и систем защиты персональных данных проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяет работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии. В случае необходимости о произошедшем инциденте администратор средств и систем защиты персональных данных сообщает ответственному за обеспечение безопасности персональных данных для принятия решения по существу.

8.1.3 Выход из строя технических средств ИСПДн «ВЛАДЕЛЕЦ ИСПДН» (серверов, источников бесперебойного питания, программно-аппаратных средств межсетевого экранирования и т.д.).

Администратор средств и систем защиты персональных данных выполняет мероприятия по ремонту неисправного технического средства информационной системы, для данных мероприятий могут привлекаться системные администраторы ИСПДн «ВЛАДЕЛЕЦ ИСПДН», обладающие соответствующими компетенциями.

При необходимости производятся работы по восстановлению программного обеспечения из эталонных копий с составлением акта.

8.1.4 Обнаружение вредоносной программы в программной среде средств автоматизации ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

При обнаружении вредоносной программы (ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженный компонент рекомендуется физически отсоединить от локальной вычислительной сети ИСПДн «ВЛАДЕЛЕЦ ИСПДН», после чего администратор средств и систем защиты персональных данных проводит анализ состояния компонента ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

После ликвидации ВП проводится внеочередная проверка на всех элементах ИСПДн «ВЛАДЕЛЕЦ ИСПДН» с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения из эталонных копий.

По факту появления ВП в локальной вычислительной сети может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается ответственным за обеспечение безопасности персональных данных.

8.1.5 Утечка информации.

При обнаружении утечки информации ставится в известность ответственный за обеспечение безопасности персональных данных. По факту может быть проведена процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

8.1.6 Взлом операционной системы средств автоматизации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» (несанкционированное получение доступа к ресурсам операционной системы).

При обнаружении взлома ставится в известность ответственный за обеспечение безопасности персональных данных. По возможности производится временное отключение ИСПДн «ВЛАДЕЛЕЦ ИСПДН» от локальной вычислительной сети для проверки на наличие ВП.

Администратором средств и систем защиты персональных данных проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, проводится анализ состояния файлов - скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данному компоненту ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

В случае необходимости производится восстановление программного обеспечения из эталонных копий.

По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

8.1.7 Попытка несанкционированного доступа (НСД).

При попытке НСД администратором системы защиты персональных данных проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, администратором средств и систем защиты персональных данных устанавливаются такие обновления.

По факту обнаружения попытки НСД может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается ответственным за обеспечение безопасности персональных данных.

В случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению к ИСПДн «ВЛАДЕЛЕЦ ИСПДН» субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

8.1.8 Компрометация ключевой информации (паролей доступа).

При компрометации ключевой информации (пароля доступа) администратором средств и систем защиты персональных данных проводится внеплановая смена пароля в соответствии с требованиями к организации парольной защиты, установленными настоящей инструкцией, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба.

8.1.9 Физическое повреждение или хищение оборудования технических средств ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Сотрудником, обнаружившим физическое повреждение элементов ИСПДн «ВЛАДЕЛЕЦ ИСПДН», ставится в известность администратор средств и систем защиты персональных данных.

Администратором средств и систем защиты персональных данных проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и возможные угрозы информационной безопасности.

О факте повреждения элементов ИСПДн «ВЛАДЕЛЕЦ ИСПДН», в случае необходимости, администратор средств и систем защиты персональных данных сообщает ответственному за обеспечение безопасности персональных данных для принятия решения по существу.

В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование.

Администратором средств и систем защиты персональных данных проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

При необходимости администратором средств и систем защиты персональных данных проводятся мероприятия по восстановлению программного обеспечения из эталонных копий с составлением акта.

8.1.10 Невыполнение установленных правил ИБ (правил работы в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»), использование ИСПДн «ВЛАДЕЛЕЦ ИСПДН» с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

Сотрудником, обнаружившим невыполнение установленных правил ИБ, использование ИСПДн «ВЛАДЕЛЕЦ ИСПДН» с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставится в известность ответственный за обеспечение безопасности персональных данных.

Ответственным за обеспечение безопасности персональных данных проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

Об обнаруженном факте ответственный за обеспечение безопасности персональных данных в случае необходимости докладывает руководителю «ВЛАДЕЛЕЦ ИСПДН».

По решению руководителя «ВЛАДЕЛЕЦ ИСПДН» по фактам выявленных нарушений может быть проведено служебное расследование.

8.1.11 Ошибки сотрудников.

В случае возникновения сбоя, связанного с ошибками сотрудников, администратором средств и систем защиты персональных данных проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения.

При необходимости администратором средств и систем защиты персональных данных проводятся мероприятия по восстановлению программного обеспечения и данных из эталонных копий с составлением акта.

В случае нанесения значительного ущерба вследствие ошибок работников по решению руководителя «ВЛАДЕЛЕЦ ИСПДН» может быть проведено служебное расследование.

8.1.12 Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИСПДн «ВЛАДЕЛЕЦ ИСПДН» администратором средств и систем защиты персональных данных проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.

Администратором средств и систем защиты персональных данных проводятся мероприятия по восстановлению программного обеспечения, а также (при необходимости) проверка на наличие компьютерных ВП.

8.1.13 Техногенные и природные проявления нештатных ситуаций.

При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), сотруднику, обнаружившему факт возникновения нештатной ситуации необходимо:

* немедленно оповестить других сотрудников и принять все меры для самостоятельной оперативной защиты помещения;
* немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);
* немедленно сообщить администратору системы защиты персональных данных.

После оперативной ликвидации причин, вызвавших пожар или наводнение, может быть назначена внутренняя комиссия по устранению последствий инцидента.

Комиссия определяет ущерб (состав и объем уничтоженных оборудования и инфор-мации) и причины, по которым произошло происшествие, а также выявляет виновных.

1. ПОРЯДОК УСТАНОВКИ, МОДИФИКАЦИИ И ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТНЫХ СРЕДСТВ ИСПДН

Все изменения конфигурации технических и программных средств, входящих в состав ИСПДн «ВЛАДЕЛЕЦ ИСПДН», должны производиться только на основании заявок, согласованных с администратором системы защиты персональных данных.

Все изменения конфигурации технических и программных средств, входящих в состав ИСПДн «ВЛАДЕЛЕЦ ИСПДН», отражаются в Техническом паспорте объекта информатизации. ЗАПРЕЩАЕТСЯ изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку ПДн без предварительной оценки влияния на защищенность ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Право внесения изменений в конфигурацию технических и программных средств ИСПДн «ВЛАДЕЛЕЦ ИСПДН» предоставляется на основании распоряжения руководителя ООО «ВЛАДЕЛЕЦ ИСПДН».

Установка и настройка программных средств осуществляется администратором средств и систем защиты персональных данных или системными администраторами, наделенными соответствующими полномочиями, согласно эксплуатационной документации.

Все добавляемые технические и программные средства должны быть предварительно установленным порядком проверены на работоспособность, а также на отсутствие опасных функций.

Установка (обновление) ПО (системного, прикладного и т.п.) на рабочих станциях производится с эталонных копий программных средств, хранящихся у администратора системы защиты персональных данных. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода в соответствии с утвержденными требованиями по организации антивирусной защиты.

После установки (обновления) ПО, администратор системы защиты персональных данных должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) эксплуатационной документацией и проверить работоспособность ПО и правильность настройки средств защиты.

В случае обнаружения недекларированных (не описанных в документации) возможностей программного обеспечения, пользователи немедленно докладывают администратору системы защиты персональных данных. Использование программного средства до получения специальных указаний запрещается. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования системы), направленные на устранение возможности использования выявленных уязвимостей.

Внесение изменений в составе технических и программных средств происходит с обязательным документированием, разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

В случае, если планируемые изменения могут быть внесены на объекте информатизации без дополнительной проверки эффективности системы защиты персональных данных, необходимо:

1. Составить распоряжение/приказ руководителя ООО «ВЛАДЕЛЕЦ ИСПДН» о внесении изменений в составе ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

2. Составить соответствующий акт изменений в составе ИСПДн «ВЛАДЕЛЕЦ ИСПДН» в произвольной форме.

3. Внести отметку в пункте «Лист регистрации изменений» технического паспорта ИСПДн «ВЛАДЕЛЕЦ ИСПДН» с указанием порядкового № и даты введения изменений, наименования документа, фиксирующего изменения; № замененных (исправленных) листов технического паспорта, зафиксировать внесенные изменения подписью внесшего их лица. При внесении изменений в технический паспорт прежняя соответствующая запись (раздел, строка или позиция паспорта) гасится, а рядом со штампом «Погашено» ставится штамп (или рукописная запись) «См. изменение N \_\_\_\_\_\_». Номер при этом должен соответствовать номеру записи в Листе регистрации изменений Технического паспорта. Все изменения вписываются в «Лист регистрации изменений» Технического паспорта в хронологическом порядке их выявления под соответствующим номером. Ссылка на номер записи, имеющаяся в техническом паспорте при этом сохраняется.

В случае, если планируемые изменения требуют дополнительной проверки эффективности системы защиты персональных данных, необходимо действовать в соответствии с указаниями, полученными от администратора системы защиты персональных данных.

1. ЗАЩИТА ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

События безопасности, подлежащие регистрации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», определяются с учетом способов реализации угроз безопасности информации. К событиям безопасности, подлежащим регистрации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», относятся любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИСПДн «ВЛАДЕЛЕЦ ИСПДН», нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также нарушения штатного функционирования средств защиты информации.

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» определены следующие события безопасности, подлежащие регистрации:

1. События, связанные с регистрацией входа (выхода) субъектов доступа в систему или загрузки операционной системы. Состав и содержание информации включают дату и время входа (выхода) в систему (из системы) или загрузки операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.
2. События, связанные с регистрацией подключения машинных носителей информации и вывода информации на носители информации. Состав и содержание регистрационных записей включает: дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, подключившего машинный носитель или осуществляющего вывод информации на носитель информации.
3. События, связанные с регистрацией запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации. Состав и содержание регистрационных записей включает: дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).
4. События, связанные с регистрацией попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. Состав и содержание регистрационных записей включает: дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).
5. События, связанные с регистрацией попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам). Состав и содержание информации должны включать: дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).
6. События, связанные с регистрацией запланированного обновления антивирусных баз. Состав и содержание информации должны включать дату и время обновления.
7. События, связанные с регистрацией запланированного обновления OC, ведутся в журнале самой OC. Состав и содержание информации должны, включать дату и время обновления, состав обновления.

События безопасности, подлежащие регистрации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», и сроки хранения соответствующих записей регистрационных журналов, обеспечивают возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется администратором средств и систем защиты персональных данных, исходя из возможностей реализации угроз безопасности информации.

Срок хранения информации о зарегистрированных событиях безопасности должен составлять не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с методическими документами, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) средств защиты информации (далее – СрЗИ) предоставляется только администратору системы защиты персональных данных.

В ИСПДн «ВЛАДЕЛЕЦ ИСПДН» для обеспечения защиты информации о событиях безопасности, перед установкой СрЗИ осуществляется синхронизация системного времени и даты. Администратор средств и систем защиты персональных данных осуществляет контроль неизменности установленного системного времени и проводит периодическую проверку журналов регистрации событий, для контроля правильности отображения временных меток.

Сбор, запись и хранение информации о событиях безопасности осуществляется с помощью встроенных средств операционной системы и установленных СрЗИ.

В целях предотвращения сбоев при регистрации событий безопасности СрЗИ и операционной системы в ИСПДн:

1. Администратору средств и систем защиты персональных данных необходимо еженедельно проверять журналы регистрации событий СрЗИ и операционной системы на наполненность и, в случае необходимости, производить их архивацию.
2. Увеличить при необходимости объем выделяемой под журналы событий безопасности СрЗИ и операционной системы памяти.
3. Включить автоматическую перезапись новых событий безопасности поверх устаревших для предотвращения возникновения ошибок переполнения журналов.
4. Настройки прав учетных записей пользователей ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должны исключать возможность внесения пользователями изменений в журналы событий безопасности, настройки СрЗИ и операционной системы.
5. При появлении в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» ошибок операционной системы или СрЗИ пользователю необходимо уведомить Администратора средств и систем защиты персональных данных и по возможности приостановить работу до устранения ошибки.

1. ПОРЯДОК ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЫВОДЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ИЗ ЭКСПЛУАТАЦИИ ИЛИ ПОСЛЕ ПРИНЯТИЯ РЕШЕНИЯ ОБ ОКОНЧАНИИ ОБРАБОТКИ ИНФОРМАЦИИ

Обеспечение защиты информации при выводе из эксплуатации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» или после принятия решения об окончании обработки информации осуществляется Владельцем ИСПДн «ВЛАДЕЛЕЦ ИСПДН», в соответствии с организационно-распорядительными документами по защите информации, и в том числе включает:

архивирование информации, содержащейся в информационной системе;

гарантированное уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности пользователя.

Гарантированное уничтожение (стирание) данных и остаточной информации с машинных носителей информации, производится при необходимости передачи машинного носителя другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации в соответствии с утвержденным порядком.

Ответственность за соблюдение требований по обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации возлагается на ответственного за обеспечение безопасности персональных данных.

**Лист ознакомления**

**с** **Инструкцией по эксплуатации системы защиты персональных данных**

**информационной системы персональных данных**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **Должность** | **Дата** | **Подпись** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |