

АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА

ГОРОДА ПЕРЕСЛАВЛЯ-ЗАЛЕССКОГО

ЯРОСЛАВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

От 24.03.2020 № ПОС.03-0502/20

г. Переславль-Залесский

Об утверждении документов по обработке

и защите персональных данных

В соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", с целью выполнения требований Постановления Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами",

Администрация города Переславля-Залесского постановляет:

1. Утвердить:

1.1. План внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных (приложение 1).

1.2. Инструкцию по организации парольной защиты (приложение 2).

1.3. Инструкцию пользователя по обеспечению безопасности обработки персональных данных (далее-ПД) при возникновении внештатных ситуаций (приложение 3).

1.4. Инструкцию по организации антивирусной защитыинформационных систем персональных данных Администрации города Переславля-Залесского (приложение 4).

1.5. Инструкцию лица, ответственного за организацию обработки персональных данных в Администрации города Переславля-Залесского (приложение 5).

2. Начальнику управления делами и кадрами (Павлов О.В.) ознакомить с настоящим постановлением под подпись операторов обработки персональных данных Администрации городского округа города Переславля-Залесского.

3. Контроль за исполнением настоящего постановления возложить на заместителя Главы Администрации города Переславля-Залесского Маркову В.В.

Глава городского округа

города Переславля-Залесского В.А. Астраханцев

Приложение 1

УТВЕРЖДЕН

постановлением Администрации

г. Переславля-Залесского

от 24.03.2020 № ПОС.03-0502/20

ПЛАН

внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

|  |  |  |
| --- | --- | --- |
| Тема проверки | Периодичность | Исполнитель |
| Проверка соблюдения пользователями  информационной системы персональных данных (далее- ИСПДн) парольной политики | Раз в полгода |  |
| Проверка соблюдения пользователями  ИСПДн антивирусной  политики | Раз в полгода |  |
| Проверка соблюдения пользователями  ИСПДн правил работы со  съемными носителями  персональных данных | Раз в полгода |  |
| Проверка соблюдения порядка  доступа в помещения, где  расположены элементы  ИСПДн | Раз в полгода |  |
| Проверка соблюдения порядка  резервирования баз данных  и хранения резервных  копий | Ежеквартально |  |
| Проверка знаний пользователей  ИСПДн о своих действиях  во внештатных ситуациях | Раз в полгода |  |
| Проверка хранения бумажных  носителей с персональными  данными | Раз в полгода |  |
| Проверка доступа к бумажным  носителям с персональными  данными | Раз в полгода |  |
| Проверка доступа в помещения, где  обрабатываются и хранятся  бумажные носители с  персональными данными | Раз в полгода |  |

Протокол № \_\_\_\_

проведения внутренней проверки соответствия обработки персональных данных требованиям к защите персональных данных в администрации городского округа города Переславля-Залесского

Настоящий Протокол составлен в том, что \_\_.\_\_\_\_\_\_.20\_\_ ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю проведена проверка

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(тема проверки)

Проверка осуществлялась в соответствии с требованиями

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(название документа)

В ходе проверки проверено:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок устранения нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Председатель комиссии \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.О. Фамилия

Члены комиссии:

Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.О. Фамилия

Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.О. Фамилия

Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.О. Фамилия

Приложение 2

УТВЕРЖДЕНА

постановлением Администрации

г. Переславля-Залесского

от 24.03.2020 № ПОС.03-0502/20

Инструкция по организации парольной защиты

1. Общие положения

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее - ИСПДн) Администрации г. Переславля-Залесского, а также контроль над действиями пользователей и обслуживающего работника системы при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПДн.

2. Правила формирования паролей

2.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационной системы самостоятельно с учётом следующих требований:

− длина пароля должна быть не менее 6 символов;

− в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.);

− пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

− при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

2.2. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Ротлвцф9?).

2.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на системного администратора.

2.4. Для обеспечения возможности использования имён и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учётных записей системному администратору в запечатанном конверте или опечатанном пенале. Опечатанные конверты (пеналы) с паролями работников должны храниться в опечатанном сейфе, к которому исключен доступ других работников Администрации и посторонних лиц. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии), либо печать системного администратора. Все конверты (пеналы) с паролями в обязательном порядке фиксируются в «Журнале учёта паролей пользователей».

3. Ввод пароля

3.1. При вводе пароля работнику необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

3.2. При неверном вводе пароля более 5 раз, учётная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

4. Порядок смены личных паролей

4.1. Смена паролей должна проводиться регулярно, не реже одного раза в 6 месяцев, самостоятельно каждым пользователем.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за обеспечение безопасности персональных данных, системного администратора и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Системный администратор ведет «Журнал учёта паролей пользователей», в котором он отмечает причины внеплановой смены паролей пользователей.

4.5. Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

5. Хранение паролей

5.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах, и носителях информации.

5.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

5.3. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учётной записью и паролем другого пользователя.

6. Действия в случае утери и компрометации пароля

6.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

7. Ответственность

7.1. Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

7.2. Ответственность за контроль проведения мероприятий по организации парольной защиты в отделах возлагается на ответственного за обеспечение безопасности персональных данных Администрации г. Переславля-Залесского.

7.3. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Лист ознакомления с «Инструкцией по организации парольной защиты»

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Фамилия И.О. сотрудника | Дата ознакомления | Расписка сотрудника в ознакомлении |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение 3

УТВЕРЖДЕНА

постановлением Администрации

г. Переславля-Залесского

от 24.03.2020 № ПОС.03-0502/20

Инструкция

пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

1. Назначение и область действия

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн управления, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей данной Инструкции является:

* определение мер защиты от прерывания;
* определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех пользователей управления, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

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

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

2. Порядок реагирования на аварийную ситуации.

2.1. Действия при возникновении аварийной ситуации

- В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

- Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в Журнале по учету мероприятий по контролю.

- В кратчайшие сроки, ответственные за реагирование сотрудники управления (Системный администратор и Пользователи ИСПДн предпринимают меры по восстановлению работоспособности). Предпринимаемые меры по возможности согласуются с лицом, ответственным за информационную безопасность Администрации г. Переславля-Залесского.

2.2. Уровни реагирования на инцидент

- уровень 1 – инцидент информационной безопасности является локальным и может быть разрешен силами оператора;

- уровень 2 – инцидент информационной безопасности может привести к существенному ущербу и может быть разрешен силами учреждения лишь частично;

- уровень 3 – последствия инцидента информационной безопасности являются критическими, и он не может быть разрешен силами учреждения.

В случае отнесения инцидента информационной безопасности к уровню 2 или уровню 3 незамедлительно уведомляется руководитель оператора.

1. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

2.3. Технические меры

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

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

Обеспечение отказоустойчивости ключевых элементов ИСПДн достигается дублированием серверов ИСПДн и использованием для них систем бесперебойного питания с двойным преобразованием. Контроль за данным оборудованием осуществляет системный администратор соответствующих ресурсов.

Контроль физического доступа достигается использованием во всех помещениях расположения элементов ИСПДн режимом доступа в помещения.

2.4. Организационные меры

Ответственные за реагирование сотрудники знакомит всех сотрудников управления, находящихся в их зоне ответственности, с данной Инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу.

Должно быть проведено обучение должностных лиц управления, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- защита материальных и информационных ресурсов;

- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

- выключение оборудования, электричества, водоснабжения, газоснабжения.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

3. Действия при возникновении наиболее распространенных нештатных ситуаций в Администрации г. Переславля-Залесского

- Отключение электричества. Системный администратор проводит анализ на наличие потерь и (или) разрушения данных и программного обеспечения (далее-ПО), а так же проверяют работоспособность оборудования. В случае необходимости, производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта.

- Сбой в локальной вычислительной сети (далее-ЛВС). Системный администратор проводит анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости, производится восстановление ПО и данных из последней резервной копии с составлением акта.

- Выход из строя сервера. Сотрудник, ответственный за эксплуатацию сервера, проводит меры по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы управления. При необходимости производятся работы по восстановлению ПО и данных из резервных копий с составлением акта.

- Потеря данных. При обнаружении потери данных администратор информационной безопасности совместно с Администратором ИСПДн проводят мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий с составлением акта.

- Обнаружен вирус. При обнаружении вируса следует руководствоваться инструкцией по эксплуатации применяемого антивирусного ПО.

- Обнаружена утечка информации (уязвимость в системе защиты). При обнаружении утечки информации ставится в известность администратор информационной безопасности и начальник подразделения. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищённости системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

- Попытка несанкционированного доступа (далее-НСД). При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Также рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

- Компрометация пароля. При компрометации пароля необходимо руководствоваться Инструкцией по организации парольной защиты. Проводиться служебное расследование.

- Физическое повреждение локальной вычислительной сети (далее-ЛВС) или персональной электронной вычислительной машины (далее-ПЭВМ). Ставится в известность системный администратор. Проводится анализ на утечку или повреждение информации. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий с составлением акта.

Лист ознакомления с «Инструкцией пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций»

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Фамилия И.О. сотрудника | Дата ознакомления | Расписка сотрудника в ознакомлении |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение 4

УТВЕРЖДЕНА

постановлением Администрации

г. Переславля-Залесского

от 24.03.2020 № ПОС.03-0502/20

Инструкция

по организации антивирусной защиты информационных систем

персональных данных Администрации города Переславля-Залесского

1. Общие положения

1.1. Инструкция по организации антивирусной защиты информационных систем персональных данных администрации города Переславля-Залесского определяет требования к организации защиты информационных систем персональных данных (далее- ИСПДн) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (ПО) и устанавливает ответственность руководителей и сотрудников отделов, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников отделов, использующих в работе ИСПДн.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые системный администратор семинары и персональные инструктажи (при необходимости) пользователей ИСПДн.

1.4. Доведение Инструкции до сотрудников в части их касающейся осуществляется системным администратором под роспись в листе ознакомления.

2. Применение средств антивирусной защиты

2.1. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.2. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

2.4. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

3. Функции системного администратора по обеспечению антивирусной безопасности.

Системный администратор обязан:

3.1. При необходимости проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты.

3.2. Настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

3.3. Предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов.

3.4. При необходимости производить обновление антивирусных программных средств.

3.5. Производить получение и рассылку (при необходимости) обновлений антивирусных баз.

3.6. Проводить работы по обнаружению и обезвреживанию вирусов.

3.7. Участвовать в работе комиссии по расследованию причин заражения ПЭВМ и серверов.

3.8. Хранить эталонные копии антивирусных программных средств.

3.9. Осуществлять периодический контроль за соблюдением пользователями ПЭВМ требований настоящей Инструкции;

3.10. Проводить периодический контроль работы программных средств системы антивирусной защиты информации на ПЭВМ (серверах).

4. Функции пользователей

4.1. Пользователи ИСПДн:

4.2. Получают по ЛВС или от системного администратора носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.3. Проводят обновления антивирусных баз на ПЭВМ (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.4. 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.) сотрудник подразделения самостоятельно или вместе с системным администратором должен провести внеочередной антивирусный контроль ПЭВМ. При необходимости он должен привлечь системного администратора для определения факта наличия или отсутствия компьютерного вируса.

4.5. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники управления обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя управления и системного администратора, а также смежные управления, использующие эти файлы в работе;

- провести анализ необходимости дальнейшего использования зараженных вирусом файлов;

- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь системного администратора);

- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, привлечь системного администратора;

- по факту обнаружения зараженных вирусом файлов составить служебную записку системного администратора, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

5. Порядок пересмотра инструкции.

5.1. Инструкция подлежит полному пересмотру в случае приобретения новых средств защиты, существенно изменяющих порядок работы с ними.

5.2. В остальных случаях Инструкция подлежит частичному пересмотру.

5.3. Полный пересмотр данной Инструкции проводится с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн.

5.4. Вносимые изменения не должны противоречить другим положениям Инструкции. При получении изменений к данной Инструкции, руководители упарвлений в течение трех рабочих дней вносят свои предложения и/или замечания к поступившим изменениям.

6. Ответственные за организацию и контроль выполнения инструкций.

6.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников.

6.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на системного администратора.

6.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн Администрации города Переславля-Залесского.

Лист ознакомления с «Инструкцией по организации антивирусной защиты информационных систем персональных данных Администрации города Переславля-Залесского»

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Фамилия И.О. сотрудника | Дата ознакомления | Расписка сотрудника в ознакомлении |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение 5

УТВЕРЖДЕНА

постановлением Администрации

г. Переславля-Залесского

от 24.03.2020 № ПОс.03-0502/20

Инструкция

лица, ответственного за организацию обработки персональных данных

в Администрации города Переславля-Залесского

1. Введение

1.1. Данная инструкция определяет круг задач, основные права и обязанности лица, ответственного за организацию обработки персональных данных (далее по тексту – ПДн) в Администрации города Переславля-Залесского (далее – организация).

2. Общие положения

2.1. Назначение лица ответственным за организацию обработки ПДн, закрепление за данным лицом определенных полномочий и обязанностей производится приказом руководителя организации.

2.2. В своей деятельности лицо, ответственное за организацию обработки ПДн в учреждении, руководствуется требованиями действующего законодательства Российской Федерации в области ПДн, принятых в соответствии с ним нормативных правовых актов и внутренних документов организации, обеспечивает их выполнение в организации.

2.3. Лицо, ответственное за организацию обработки ПДн, непосредственно подчиняется администратору информационной безопасности учреждения и, помимо обязанностей, закрепленных настоящей Инструкцией, исполняет их указания и распоряжения в рамках выполнения своих основных задач.

3. Основные задачи лица, ответственного за организацию обработки ПДн

3.1. Основными задачами лица, ответственного за организацию обработки ПДн, являются:

- обеспечение соблюдения в организации требований внутренних документов учреждения, а также нормативных правовых актов, регулирующих сферу обработки ПДн;

- обеспечение правомерности обработки ПДн в организации;

- обеспечение соответствия договоров и соглашений, заключаемых учреждением с третьими лицами и связанных с передачей, совместной обработкой или поручением обработки ПДн, требованиям законодательства РФ о ПДн;

- поддержание в актуальном состоянии внутренних документов учреждения, регламентирующих процессы обработки и обеспечения безопасности ПДн;

- доведение до сведения работников организации положений законодательства РФ о ПДн, внутренних документов организации по вопросам обработки ПДн, требований по обеспечению безопасности ПДн при их обработке и хранении;

- организация приема и обработки (рассмотрения, подготовки ответов) обращений и запросов субъектов ПДн или их представителей, а также иных органов и организаций по вопросам, связанным с обработкой, передачей или защитой ПДн;

- участие в выборе методов и способов защиты ПДн, обрабатываемых в ИСПДн, формирование требований по обеспечению безопасности ПДн с помощью организационно-режимных мер защиты;

- организация физической защиты помещений с установленными техническими средствами, участвующими в обработке ПДн, а также помещений, где хранятся материальные носители ПДн, дистрибутивы и документация к средствам защиты информации;

- участие по решению администратора информационной безопасности организации в реагировании на инциденты информационной безопасности, связанные с нарушением заданных характеристик безопасности ПДн;

- осуществление текущего контроля соблюдения работниками организации правил обработки ПДн и требований по обеспечению их безопасности.

4. Обязанности лица, ответственного за организацию обработки ПДн

4.1. На лицо, ответственное за организацию обработки ПДн, возлагается ответственность за обеспечение соблюдения в учреждении требований законодательства РФ в области ПДн, а также нормативных правовых актов, регулирующих сферу обработки и обеспечения безопасности ПДн.

4.2. В случае внесения изменений в обрабатываемые ПДн, лицо, ответственное за организацию обработки ПДн, обязано обеспечить (организовать) уведомление третьих лиц, которым были переданы ПДн, о внесенных в них изменениях.

4.3. Лицо, ответственное за организацию обработки ПДн, несет ответственность за поддержание в актуальном состоянии внутренних организационно-распорядительных документов по вопросам обработки ПДн (в части обработки ПДн в учреждении) и обеспечения безопасности ПДн при их обработке и хранении, а также:

- Перечня должностей, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;

- Перечня лиц, имеющих право доступа в помещения, в которых установлены технические средства, участвующие в обработке ПДн, либо хранятся материальные носители ПДн;

- Перечня целей и сроков обработки ПДн в учреждении.

4.4. Лицо, ответственное за организацию обработки ПДн, обеспечивает своевременную передачу сведений, необходимых для актуализации соответствующих документов, администратору информационной безопасности учреждения.

4.5. Лицо, ответственное за организацию обработки ПДн, обеспечивает ознакомление работников соответствующего структурного подразделения учреждения с внутренними документами организации, регламентирующими процессы обработки и обеспечения безопасности ПДн, в части, их касающейся.

4.6. Лицо, ответственное за организацию обработки ПДн, несет ответственность за недопущение к обработке ПДн (запрет доступа к ПДн) работников организации, не ознакомленных с положениями законодательства РФ о ПДн, внутренних документов по вопросам обработки ПДн, требованиями по обеспечению безопасности ПДн при их обработке и хранении.

4.7. Лицо, ответственное за организацию обработки ПДн, обеспечивает соблюдение установленных сроков рассмотрения обращений и запросов субъектов ПДн или их представителей, а также иных органов и организаций по вопросам, связанным с обработкой, передачей или защитой ПДн, соблюдение требований законодательства РФ в области ПДн и внутренних документов организации при рассмотрении обращений и запросов и ответе на них.

4.8. В случае поступления в организацию обращения или запроса, связанного с требованием уточнения, блокирования или уничтожения ПДн, обрабатываемых в учреждении, лицо, ответственное за организацию обработки ПДн, обязано обеспечить блокирование (временное прекращение обработки) ПДн на период проведения проверки сведений, изложенных в запросе, в случае, если блокирование не нарушает права и законные интересы субъекта ПДн или третьих лиц.

4.9. Лицо, ответственное за организацию обработки ПДн, формирует перечень требований по обеспечению физической защиты помещений с установленными техническими средствами, участвующими в обработке ПДн, а также помещений, где хранятся материальные носители ПДн, в учреждении, организует проведение работ по обеспечению физической защиты таких помещений.

4.10. Лицу, ответственному за организацию обработки ПДн, запрещается использовать предоставленные полномочия в целях, отличных от целей, предусмотренных служебными обязанностями.

5. Права лица, ответственного за организацию обработки ПДн

5.1. Лицо, ответственное за организацию обработки ПДн, имеет право:

- осуществлять оперативное вмешательство в работу сотрудников организации при явной угрозе безопасности информации в результате несоблюдения установленного режима обработки ПДн и (или) невыполнения требований по обеспечению безопасности ПДн с последующим докладом системному администратору организации;

- вносить свои предложения по совершенствованию мер защиты обрабатываемых ПДн.

Лист ознакомления с «Инструкцией лица, ответственного за организацию обработки персональных данных

в Администрации города Переславля-Залесского

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Фамилия И.О. сотрудника | Дата ознакомления | Расписка сотрудника в ознакомлении |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |