Приложение 5 к приказу
от 12.01.2024 № 8

Положение об обеспечении безопасности персональных данных при их обработке в информационной системе персональных данных «Контингент»

1. Общие положения

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационной системе персональных данных «Контингент» устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Контингент» (далее – ИСПДн) ЧОУ ДО «Бритиш Клаб» (Британский Клуб) (далее – Организация).

1.2. Настоящий документ разработан в соответствии с Федеральным законом от 27 июля 2006г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18 февраля 2013г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Действие настоящего документа распространяется на всех пользователей ИСПДн.

1.4. Изменения и дополнения к настоящему документу утверждаются в установленном порядке.

2. Термины и определения

2.1. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.3. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.5. Технические средства, позволяющие осуществлять обработку персональных данных, – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

2.6. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. Особенности обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных

3.1. Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии со статьей 19 Федерального закона «О персональных данных». Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3.3. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

3.4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

3.5. В ИСПДн Организации устанавливаются уровни защищенности персональных данных в зависимости от угроз безопасности этих данных в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 1 ноября 2012г. № 1119.

3.6. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

3.7. В Организации организован режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

3.8. Безопасность персональных данных при их обработке в ИСПДн обеспечивают ответственный за обеспечение безопасности персональных данных и администратор безопасности.

4. Требования по обеспечению безопасности

4.1. При обработке персональных данных в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль над обеспечением уровня защищенности персональных данных.

4.2. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

– определение угроз безопасности персональных данных при их обработке в ИСПДн;

– применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

– учет машинных носителей персональных данных;

– обнаружение фактов несанкционированного доступа к персональным данным и принятие мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них;

– восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установление правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;

– контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн;

– ознакомление работников Организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

4.3. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе возлагается на администратора безопасности.

4.4. Список лиц, имеющих право доступа к персональным данным, уполномоченных на обработку этих данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных, утверждается Руководителем Организации.

4.5. Работники Организации, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей, для получения доступа к информационной системе обращаются с устным запросом к ответственному за обеспечение безопасности персональных данных.

4.6. При обнаружении нарушений порядка предоставления персональных данных администратор безопасности незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

4.7. Иные требования по обеспечению безопасности информации и средств защиты информации в Организации выполняются в соответствии с требованиями органов исполнительной власти Российской Федерации и соответствующего субъекта Российской Федерации, органов местного самоуправления.

5. Регистрация событий безопасности информационной системы персональных данных

5.1. В ИСПДн подлежат регистрации следующие события:

– вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;

– подключение машинных носителей информации и вывод информации на носители информации;

– запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

– попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

– попытки удаленного доступа.

5.2. Сроки хранения событий безопасности определяются заданными настройками средств защиты информации от несанкционированного доступа.

5.3. Состав и содержание информации о событиях безопасности:

– тип события;

– дата и время события;

– идентификационной информации источника события безопасности;

– результат события безопасности (успешно или неуспешно);

– субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

5.4. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения предусматривает:

– возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени: обеспечивается возможностями операционной системы и средств защиты информации от несанкционированного доступа;

– генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с п. 5.1 настоящего Положения с составом и содержанием информации, определенными в соответствии с п. 5.3 настоящего Положения.

– хранение информации о событиях безопасности в течение времени, установленного в соответствии с п. 5.2 настоящего Положения.

5.5. Доступ к записям регистрации событий и функциям управления механизмами регистрации предоставляется только администратору безопасности и обслуживающему персоналу под контролем администратора безопасности.

5.6. Резервное копирование записей регистрации событий производится в соответствии с Регламентом резервного копирования данных.

6. Порядок действий в случае возникновения внештатной ситуации в ИСПДн

6.1. Действия в случае сбоя программного обеспечения.

6.1.1. Пользователи ИСПДн в случае сбоя программного обеспечения ИСПДн уведомляют об инциденте администратора безопасности.

6.1.2. Администратор безопасности выясняет причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою.

6.2. Действия в случае отключения электропитания технических средств ИСПДн.

6.2.1. Пользователи ИСПДн в случае отключения электропитания технических средств ИСПДн уведомляют об инциденте администратора безопасности.

6.2.2. Администратор безопасности 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 с составлением акта.

6.3. Действия в случае выхода из строя технических средств ИСПДн.

6.3.1. Пользователи ИСПДн при выходе из строя технических средств (рабочей станции, источников бесперебойного питания, программных средств, средств защиты информации и т. д.) уведомляют об инциденте администратора безопасности.

6.3.2. Администратор безопасности выполняет мероприятия по ремонту неисправного технического средства ИСПДн или восстановлению программных средств. При необходимости производятся работы по восстановлению программного обеспечения из эталонных копий.

6.4. Действия в случае обнаружения вредоносной программы в программной среде ИСПДн.

6.4.1. Пользователи ИСПДн при обнаружении вредоносной программы уведомляют об инциденте администратора безопасности.

6.4.2. Администратором безопасности производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженную рабочую станцию рекомендуется физически отсоединить от локальной вычислительной сети Организации.

6.4.3. Администратору безопасности необходимо провести анализ состояния рабочей станции. После ликвидации вредоносной программы проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения из эталонных копий.

6.5. Действия в случае обнаружения утечки информации.

6.5.1. При обнаружении утечки информации ставится в известность администратор безопасности. По факту обнаружения утечки должна быть произведена процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИСПДн и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

6.6. Действия в случае несанкционированного получения доступа к ресурсам операционной системы ИСПДн.

6.6.1. При обнаружении несанкционированного получения доступа к ресурсам рабочей станции пользователем ИСПДн ставится в известность администратор безопасности. По возможности производится временное отключение рабочей станции от локальной вычислительной сети Организации для проверки наличия вредоносной программы.

6.6.2. Администратором безопасности проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, проводится анализ журналов, смена всех паролей, которые имели отношение к данной рабочей станции.

6.6.3. В случае необходимости производится восстановление программного обеспечения из эталонных копий с составлением акта.

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

6.7. Действия в случае попытки несанкционированного доступа (далее – НСД).

6.7.1. При попытке НСД администратором безопасности 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.

6.7.2. Проводится внеплановая смена паролей.

6.7.3. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, администратором безопасности устанавливаются такие обновления.

6.7.4. По факту НСД должно быть проведено служебное расследование. В случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению ИСПДн субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в правоохранительные органы для определения наличия признаков состава преступления или административного правонарушения и принятия мер к установлению виновного в попытке НСД и привлечению его к ответственности в соответствии с действующим законодательством.

6.8. Действия в случае компрометации ключевой информации (паролей доступа).

6.8.1. При компрометации ключевой информации (пароля доступа) администратором безопасности проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного или нанесенного ущерба.

6.9. Действия в случае физического повреждения или хищения оборудования технических средств ИСПДн.

6.9.1. Работником, обнаружившим физическое повреждение элементов ИСПДн, ставится в известность об инциденте администратор безопасности.

6.9.2. Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн и возможные угрозы информационной безопасности. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование.

6.9.3. Администратором безопасности проводится проверка программного обеспечения на целостность и наличие вредоносной программы, а также проверка целостности данных и анализ электронных журналов. При необходимости администратором безопасности проводятся мероприятия по восстановлению программного обеспечения из эталонных копий.

6.10. Действия в случае обнаружения факта невыполнения установленных правил информационной безопасности.

6.10.1. Работником, обнаружившим невыполнение установленных правил информационной безопасности, использование ИСПДн с нарушением требований, установленных в нормативно-технической документации, ставится в известность администратор безопасности.

6.10.2. Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента. При необходимости по фактам выявленных нарушений проводится служебное расследование.

6.11. Действия в случае ошибок работников.

6.11.1. В случае возникновения сбоя, связанного с ошибками работников, администратором безопасности 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 проводятся мероприятия по восстановлению программного обеспечения и данных из эталонных копий. В случае нанесения значительного ущерба обрабатываемым данным вследствие ошибок работников может быть проведено служебное расследование.

6.12. Действия в случае отказа в обслуживании.

6.12.1. Работником, обнаружившим отказ в обслуживании, ставится в известность администратор безопасности.

6.12.2. Администратором безопасности проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

6.12.3. Администратором безопасности проводится проверка программного обеспечения на целостность и наличие вредоносной программы, а также проверка целостности данных и анализ электронных журналов. При необходимости проводятся мероприятия по восстановлению программного обеспечения и данных из эталонных копий.

6.13. Действия в случае несанкционированных изменений состава программных и аппаратных средств (конфигурации) ИСПДн.

6.13.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИСПДн администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

6.13.2. Администратором безопасности проводятся мероприятия по восстановлению программного обеспечения, а также проверка на наличие компьютерных вредоносных программ.

6.14. Действия в случае техногенных и природных проявлений нештатных ситуаций.

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

- оповестить других работников и принять все меры для самостоятельной оперативной защиты помещения;
- позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т. д.);
- сообщить администратору безопасности о произошедшем инциденте.

6.14.2. После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента. Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

6.15. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Организация обязана с момента выявления такого инцидента уведомить уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Учреждением на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

7. Ответственность

7.1. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн работники могут быть привлечены к ответственности, предусмотренной действующим законодательством Российской Федерации.