ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ БИОТУМ»

УТВЕРЖДАЮ
Генеральный директор
ООО «НПП БИОТУМ»
_____ Ф.Н. Волков
«12» 03 2024 г.

Положение

по защите информации.

37363269.425790.017.ПИ.01

Владимир
2024

Содержание

1. Определения.

1.1 **Администратор безопасности** – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации информационной системы в соответствии с установленной ролью.

1.2 **Администратор** системный – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) в соответствии с установленной ролью.

1.3 **Инцидент информационной безопасности –** непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

1.4 **Компьютерный вирус** - компьютерная программа либо иная компьютерная информация, предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации.

1.5 **Конфигурация ИСПДн и ее системы защиты информации** – состав и взаимосвязи (электрические, логические, программные, геометрические) составных частей ИСПДн и СЗИ.

1.6 **Пользователь –** лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

1.7 **Последствия инцидента** – нарушение конфиденциальности информации и (или) нарушение целостности информации (программного обеспечения) и (или) нарушение доступности информации.

1.8 **Событие информационной безопасности** – идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

1.9 **Ответственный за защиту информации** – должностное лицо Организации, эксплуатирующей информационную систему, содержащую персональные данные, отвечающее за организацию защиты информации персональных данных.

1.10 **Внутренний пользователь** – пользователь информационной системы, являющийся сотрудником Организации, эксплуатирующей информационную систему.

1.11 **Внешний пользователь** – пользователь информационной системы, не являющийся сотрудником Организации, эксплуатирующей информационную систему.

2. Сокращения.

2.1 **ИСПДн** – информационная система.

2.2 **ОРД** – организационно – распорядительная документация.

2.3 **ПДн** – персональные данные.

2.4 **СЗИ** – средства защиты информации.

2.5 **ТС** – технические средства.

3. Общие положения.

3.1 Настоящее Положение по защите информации информационных систем персональных данных (далее – ИСПДн) разработано в соответствии со следующими нормативными правовыми актами и документацией на ИСПДн и ее систему защиты информации:

3.1.1 Федеральный закон от 27.07.2006 года **№ 149 – ФЗ** «Об информации, информационных технологиях и защите информации».

3.1.2 Федеральный закон от 27.07.2006 года **№ 152 – ФЗ** «О персональных данных».

3.1.3 Методический документ, утвержден ФСТЭК России 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

3.1.4 Приказ ФСТЭК России от 18.02.2013 года **№21** «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.1.5 Постановление Правительства РФ от 01.11.2012 **№1119** «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.1.6 Нормативно – технический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) (Утвержден приказом Гостехкомиссии России №282 от 30.08.2002).

3.1.7 ГОСТ Р ИСО/МЭК ТО 2712-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».

3.1.8 ГОСТ Р 53114 – 2008 «Обеспечение информационной безопасности в организации. Основные термины и определения».

3.1.9 Система защиты информации ИСПДн.

3.2 Настоящее Положение предназначено для организации защиты информации ИСПДн, содержащей персональные данные не выше **3 уровня** защищенности.

3.3 Настоящее Положение определяет порядок действий пользователей при защите информации, в том числе персональных данных, содержащихся в ИСПДн.

3.4 Перечень информации (в том числе персональные данные) требующей защиты утверждает Генеральный директор ООО "НПП БИОТУМ" (далее – Организация) по форме документа «Списки и перечни (формы)» 37363269.425790.017.ТБ.03 (Форма 1).

3.5 Настоящее Положение вступает в силу после его утверждения генеральным директором Организации и действует бессрочно, до момента его замены новым.

3.6 Все пользователи ИСПДн, должны быть ознакомлены с настоящим Положением под роспись.

3.7 **Для координации и контроля выполнения мероприятий по защите информации и для организации обработки персональных данных в ИСПДн,** Приказа ФСТЭК №21, Генеральный директор Организации приказом назначает должностное лицо Организации **ответственным за защиту информации**. Форма приказа о назначении ответственного за защиту информации приведена в документе «Приказы (формы)» 37363269.425790.017.ДО.01 (Форма 1). При выполнении своих обязанностей Ответственный за защиту информации действует в соответствии с требованиями «Руководства ответственного за защиту информации» 37363269.425790.017.И3.03.

3.8 Для непосредственного выполнения работ по защите информации с использованием программно-аппаратных средств защиты информации (далее СЗИ), Генеральный директор Организации (в соответствии с требованиями Постановления правительства РФ №1119 п.14 и с требованиями мер по защите информации Приказа №21) назначает **администратора безопасности**. На администратора безопасности приказом генерального директора Организации возлагается ответственность за обеспечение безопасности информации, в том числе персональных данных, обрабатываемых в ИСПДн. Форма приказа о назначении администратора безопасности приведена в документе «Приказы (формы)» 37363269.425790.017.ДО.01 (Форма 2). При выполнении своих обязанностей по обеспечению безопасности информации, обрабатываемой в ИСПДн, администратор безопасности действует в соответствии с требованиями «Руководство администратора безопасности» 37363269.425790.017.И3.02 и требованиями эксплуатационной документации на СЗИ.

3.9 Все пользователи информационной системы участвуют в защите информации, в том числе персональных данных, содержащейся в ИСПДн, и обязаны знать и выполнять требования:

3.9.1 нормативно – правовых документов по защите информации, в том числе по защите персональных данных;

3.9.2 настоящего Положения и перечисленных в нем инструкций, в части их касающейся;

3.9.3 «Руководство пользователя» 37363269.425790.017.И3.01.

3.10 В соответствии с требованиями п.8 Приказа ФСТЭК №21 защита информации, в том числе персональных данных, в ходе эксплуатации ИСПДн осуществляется выполнением процедур:

3.10.1 управления (администрирования) системой защиты информации ИСПДн;

3.10.2 выявления инцидентов и реагирования на них;

3.10.3 управления конфигурацией ИСПДн и ее системы защиты информации;

3.10.4 контроля обеспечения уровня защищенности информации, содержащейся в ИСПДн.

3.11 В соответствии с требованиями Постановления правительства РФ №211 организация обработки и защиты персональных данных в государственных и муниципальных информационных системах, содержащих персональные данные, требует документирования и утверждения генеральным директором Организации локальных актов, определяющих политику в отношении обработки персональных данных (далее – ПДн). В настоящем Положении политика в отношении обработки ПДн определена:

3.11.1 правилами обработки ПДн;

3.11.2 правилами рассмотрения запросов субъектов ПДн;

3.11.3 правилами осуществления внутреннего контроля соответствия обработки ПДн требованиям к их защите;

3.11.4 рабочими документами по организации обработки ПДн.

4. Раздел 1. Управление системой защиты информации ИСПДн.

4.1 Общие положения.

4.1.1 Процедуры управления системой защиты информации обеспечивают:

4.1.1.1 функционирование системы защиты информации в штатном режиме с характеристиками, установленными в проектной документации;

4.1.1.2 документированный поток информации о событиях безопасности в ИСПДн и системе защиты информации, на основании которой возможна реализация процедур управления инцидентами, управления конфигурацией ИСПДн и ее системы защиты и процедуры контроля уровня защищенности информации, обрабатываемой в ИСПДн.

4.2 Идентификация и аутентификация пользователей ИСПДн.

4.2.1 Порядок действий пользователей ИСПДн при прохождении процедур идентификации (узнавании) и аутентификации (подтверждении подлинности узнанного пользователя) при входе в ИСПДн описаны в «Инструкции по идентификации и аутентификации пользователей» 37363269.425790.017.И2.01.

4.2.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения пользователями требований инструкции 37363269.425790.017.И2.01 обеспечивает администратор безопасности.

4.3 Управление доступом пользователей ИСПДн.

4.3.1 Порядок управления доступом пользователей к информационным ресурсам ИСПДн описаны в «Инструкции по управлению доступом пользователей к информации» 37363269.425790.017.И2.02.

4.3.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения пользователями требований инструкции 37363269.425790.017.И2.02 обеспечивает администратор безопасности.

4.4 Управление программным обеспечением ТС ИСПДн и СЗИ.

4.4.1 Порядок действий пользователей ИСПДн при реализации ограничений в применении программного обеспечения, установки разрешенного программного обеспечения, его настройки и обновления, описаны в «Инструкции по управлению программным обеспечением» 37363269.425790.017.И2.03.

4.4.2 Выполнение требований инструкции обеспечивает администратор безопасности.

4.5 Защита машинных носителей информации ИСПДн.

4.5.1 Порядок действий пользователей ИСПДн при работе с машинными носителями информации, правила учета, хранения и доступа к машинным носителям и к

информации, содержащейся на машинных носителях описаны в «Инструкции по защите машинных носителей информации» 37363269.425790.017.И2.04.

4.5.2 Выполнение требований инструкции обеспечивает администратор безопасности.

4.6 Управление событиями информационной безопасности в ИСПДн.

4.6.1 Порядок действий администратора безопасности и администраторов системных ИСПДн при появлении событий безопасности описаны в «Инструкции по управлению событиями информационной безопасности» 37363269.425790.017.И2.05.

4.6.2 Выполнение требований инструкции обеспечивает администратор безопасности.

4.7 Управление антивирусной защитой ИСПДн.

4.7.1 Порядок действий пользователей при обнаружении в ИСПДн компьютерных вирусов, описаны в «Инструкции по антивирусной защите» 37363269.425790.017.И2.06.

4.7.2 Выполнение требований инструкции обеспечивает администратор безопасности.

4.8 Контроль защищенности ИСПДн.

4.8.1 Порядок действий администраторов системных и администратора безопасности с целью:

4.8.1.1 выявления ошибок и недостатков программного обеспечения и аппаратных средств ИСПДн и средств защиты информации;

4.8.1.2 контроля установки обновлений программного обеспечения, контроля работоспособности и настроек программного обеспечения;

4.8.1.3 контроля состава технических и программных средств ИСПДн и системы защиты информации;

4.8.1.4 контроля правил работы с паролями и учетными записями,

описан в «Инструкции по контролю защищенности информации» 37363269.425790.017.И2.07.

4.8.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения администраторами системными требований инструкции 37363269.425790.017.И2.07 обеспечивает администратор безопасности.

4.9 Управление целостностью программных средств и информации ИСПДн.

4.9.1 Порядок действий администраторов системных и администратора безопасности с целью:

4.9.1.1 обеспечения возможности восстановления программных средств и информации, содержащейся в ИСПДн, при возникновении нештатных ситуаций;

4.9.1.2 обеспечения восстановления программных средств и информации, содержащейся в ИСПДн, после инцидентов, разрушивших программные средства и информацию

ИСПДн, описан в «Инструкции по устранению причин и последствий инцидентов» 37363269.425790.017.И2.08.

4.9.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения администраторами системными требований инструкции 37363269.425790.017.И2.08 обеспечивает администратор безопасности.

4.10 Управление защитой технических средств информационной системы.

4.10.1 Порядок доступа пользователей к техническим средствам ИСПДн и СЗИ, описан в «Инструкции по защите технических средств информационной системы» 37363269.425790.017.И2.09.

4.10.2 Выполнение требований инструкции в части его касающейся и контроль соблюдения пользователями требований инструкции 37363269.425790.017.И2.09 обеспечивает администратор безопасности.

5. Раздел 2. Выявление инцидентов и реагирование на них.

5.1 Общие положения.

5.1.1 Инциденты информационной безопасности ИСПДн разделены на **категории**:

5.1.1.1 **категория 1 –** отказ технических средств ИСПДн и СЗИ (отказ в обслуживании сервисов, средств обработки информации, оборудования);

5.1.1.2 **категория 2 –** системные сбои или перегрузки технических средств ИСПДн и СЗИ;

5.1.1.3 **категория 3 –** сбои программного обеспечения ИСПДн и СЗИ;

5.1.1.4 **категория 4 –** неконтролируемые изменения конфигурации ИСПДн и СЗИ;

5.1.1.5 **категория 5 –** нарушение физических мер защиты информации ИСПДн;

5.1.1.6 **категория 6 –** нарушение правил доступа к информации, содержащейся в ИСПДн;

5.1.1.7 **категория 7 –** несоблюдение пользователями ИСПДн требований ОРД по защите информации ИС;

5.1.1.8 **категория 8 –** ошибки пользователей ИСПДн;

5.1.2 Любое событие или группа событий информационной безопасности, приводящие к реализации или вероятности реализации любой из категорий п. 4.1.1. должны ориентироваться в установленном порядке как инциденты.

5.2 Порядок выявления инцидентов.

5.2.1 Правила и порядок сбора информации о событиях информационной безопасности приведены в «Инструкции по управлению событиями информационной безопасности» 37363269.425790.017.И2.05.

5.2.2 Выявление и учет инцидентов организует **ответственный за защиту информации** совместно с **администратором безопасности** на основе сообщений пользователей и анализа журналов регистрации событий информационной безопасности.

5.2.3 Если администратор безопасности определяет текущее событие безопасности как инцидент, то он незамедлительно докладывает об инциденте ответственному за защиту информации и по его указанию принимает меры для устранения последствий инцидента в рамках своих должностных полномочий и в соответствии с «Инструкцией по устранению причин и последствий инцидентов» 37363269.425790.017.И2.08.

5.2.4 Учет выявленных инцидентов осуществляет ответственный за защиту информации в журнале регистрации инцидентов. Форма журнала регистрации инцидентов приведена в документе «Журналы (формы)» 37363269.425790.017.ТБ.01 (Форма 1).

5.2.5 При выявлении инцидента осуществляют оповещение пользователей ИСПДн об инциденте. Форму и порядок оповещения устанавливает ответственный за защиту информации.

5.3 Порядок реагирования на инциденты.

5.3.1 При реагировании на инциденты:

5.3.1.1 осуществляют **анализ** инцидента:

- оценка нанесенного материального ущерба;
- выявление неучтенных в системе защиты информации угроз безопасности;
- расследование причин инцидента;

5.3.1.2 устраняют причины и последствия инцидента;

5.3.1.3 формируют перечень мероприятий по недопущению инцидента в будущем.

5.3.2 Анализ инцидента организует **ответственный за защиту информации** с привлечением администратора безопасности, администраторов системных ИСПДн и пользователей - непосредственных участников инцидента. Анализ проводится комиссией, состав которой определяет ответственный за защиту информации. Сроки анализа инцидента определяются по категории инцидента. Анализ инцидентов 1,2,3 категорий проводят немедленно после возникновения инцидента в целях максимального ускорения устранения последствий инцидента. Анализ инцидентов 4 – 8 категорий проводят не позднее 1 дня с момента возникновения инцидента. Анализ инцидента оформляется Актом расследования инцидента информационной безопасности, приведенного в документе «Акты (формы)» 37363269.425790.017.ДО.02 (Форма 1).

5.3.3 Устранение причин и последствий инцидента осуществляет администратор безопасности совместно с администраторами системными ИСПДн по правилам и в сроки, установленные в «Инструкции по устранению причин и последствий инцидентов» 37363269.425790.017.И2.08. Результат устранения инцидента администратор безопасности заносит в журнал регистрации инцидентов.

5.3.4 Перечень мероприятий, направленных на недопущение инцидента в будущем, формирует и организует их выполнение ответственный за защиту информации. При необходимости ответственный за защиту информации утверждает перечень мероприятий у Генерального директора Организации. Форма перечня мероприятий не регламентируется.

6. Раздел 3. Управление обработкой персональных данных в ИСПДн.

6.1 Правила обработки ПДн.

6.1.1 Порядок действий пользователей ИСПДн при обработке персональных данных, содержащихся в ИСПДн, приведен в документе «Правила обработки персональных данных» 37363269.425790.017.И2.10.

6.1.2 Контроль выполнения требований документа осуществляет ответственный за защиту информации.

6.2 Правила рассмотрения запросов субъектов ПДн.

6.2.1 Порядок действий сотрудника, ответственного за организацию обработки ПДн (в ИСПДн – ответственного за защиту информации) при рассмотрении запросов субъектов персональных данных, содержащихся в ИСПДн, приведен в документе «Правила рассмотрения запросов субъектов персональных данных» 37363269.425790.017.И2.11.

6.3 Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн.

6.3.1 Порядок действий пользователей ИСПДн при осуществлении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, содержащихся в ИС, приведен в документе «Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к их защите» 37363269.425790.017.И2.12.

6.3.2 Контроль выполнения требований документа осуществляет ответственный за защиту информации.

6.4 Рабочие документы по организации обработки ПДн.

6.4.1 Рабочие документы предназначены для организации рабочего процесса обработки персональных данных.

6.4.2 К рабочим документам в Организации отнесены:

6.4.2.1 Перечень информации, в том числе персональные данные, обрабатываемые в ИСПДн по форме «Списки и перечни (формы)» Форма 1.

6.4.2.2 Типовое обязательство лица, непосредственно осуществляющего обработку персональных данных о неразглашении персональных данных по форме «Типовые административные документы (формы)» 37363269.425790.017.03ДО.03 Форма 1.

6.4.2.3 Типовое согласие на обработку ПДн по форме «Типовые административные документы (формы)» 37363269.425790.017.03ДО.03 Форма 2.

6.4.2.4 Типовое разъяснение субъекту ПДн юридических последствий отказа в предоставлении ПДн по форме «Типовые административные документы (формы)» 37363269.425790.017.03ДО.03 Форма 3.

7. Заключительные положения.

7.1 Пользователи ИСПДн должны быть предупреждены об ответственности за действия с информацией, в том числе персональными данными, содержащимися в ИСПДн и действия с техническими средствами ИСПДн и СЗИ, нарушающие требования настоящего Положения и других организационных и правовых документов, определяющих меры по защите информации, в том числе персональных данных, содержащихся в ИСПДн.

7.2 Пользователи ИСПДн, в том числе администратор безопасности и администраторы системные ИСПДн, должны быть ознакомлены в части их касающейся, с настоящим Положением до начала работы с ИСПДн под роспись. Обязанность ознакомления пользователей с настоящим Положением лежит на ответственном за защиту информации.