ПРАВИТЕЛЬСТВО ХАБАРОВСКОГО КРАЯ
ПОСТАНОВЛЕНИЕ

29 декабря 2022 г. № 715-пр
г. Хабаровск

О внесении изменений в постановление Правительства Хабаровского края от 20 февраля 2019 г. № 48-пр "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Хабаровского края, аппарате Губернатора и Правительства Хабаровского края"

В целях совершенствования нормативного правового акта Хабаровского края Правительство края
ПОСТАНОВЛЯЕТ:

1. Внести в постановление Правительства Хабаровского края от 20 февраля 2019 г. № 48-пр "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Хабаровского края, аппарате Губернатора и Правительства Хабаровского края" следующие изменения:

1) в наименовании слова "органах исполнительной власти Хабаровского края, аппарате" заменить словами "исполнительных органах Хабаровского края, администрации";

2) в пункте 1 слова "органами исполнительной власти Хабаровского края, аппаратом" заменить словами "исполнительными органами Хабаровского края, администрацией";

3) в пункте 2 слова "Органам исполнительной власти края, аппарату" заменить словами "Исполнительным органам края, администрации".

2. Внести изменение в Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых органами исполнительной власти Хабаровского края, аппаратом Губернатора и Правительства Хабаровского края, утвержденный постановлением Правительства Хабаровского края от 20 февраля 2019 г. № 48-пр "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в органах исполнительной власти Хабаровского края, аппарате Губернатора и Правительства Хабаровского края", изложив его в новой редакции согласно приложению к настоящему постановлению.

Губернатор, Председатель Правительства края М.В. Дегтярев

ПП 013051

ООО «Эффект» 2019 г. Зак. Б-82. Тираж 2000 экз.

ПРИЛОЖЕНИЕ
к постановлению
Правительства
Хабаровского края
от 29 декабря 2022 г. № 715-пр

"УТВЕРЖДЕН
постановлением
Правительства
Хабаровского края
от 20 февраля 2019 г. № 48-пр

ПЕРЕЧЕНЬ

угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых исполнительными органами Хабаровского края, администрацией Губернатора и Правительства Хабаровского края*

Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, эксплуатируемых исполнительными органами Хабаровского края, администрацией Губернатора и Правительства Хабаровского края (далее также – информационные системы), являются:

угрозы, связанные с особенностями функционирования технических, программно-технических и программных средств, обеспечивающих хранение, обработку и передачу информации;

угрозы несанкционированного доступа (воздействия) к отчуждаемым носителям персональных данных, включая переносные персональные компьютеры пользователей информационных систем;

угрозы воздействия вредоносного кода и (или) вредоносной программы, внешних по отношению к информационным системам;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, обладающими полномочиями в информационных системах, в том числе в ходе создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации информационных систем и дальнейшего хранения содержащейся в их базах данных информации;

угрозы использования методов воздействия на лиц, обладающих полномочиями в информационных системах;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в организации защиты персональных данных;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах,

с использованием уязвимостей в программном обеспечении информационных систем;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационных систем;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств защиты информации;

угрозы целенаправленных действий с использованием аппаратных и (или) программных средств в целях нарушения безопасности защищаемых с использованием средств криптографической защиты информации персональных данных или создания условий для этого, определяемые операторами информационных систем в соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденными приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378.

---

*Угрозы безопасности с учетом содержания персональных данных, характера и способов их обработки в информационных системах персональных данных уточняются операторами информационных систем персональных данных – исполнительными органами Хабаровского края в частных моделях угроз безопасности персональных данных в соответствии с описанием информационных систем персональных данных, эксплуатируемых исполнительными органами Хабаровского края, администрацией Губернатора и Правительства Хабаровского края, и определением актуальных угроз безопасности персональных данных в указанных информационных системах согласно приложению к настоящему Перечню.

ПРИЛОЖЕНИЕ

к Перечню угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых исполнительными органами Хабаровского края, администрацией Губернатора и Правительства Хабаровского края

ОПИСАНИЕ

информационных систем персональных данных, эксплуатируемых исполнительными органами Хабаровского края, администрацией Губернатора и Правительства Хабаровского края, и определение актуальных угроз безопасности персональных данных в указанных информационных системах

1. Описание информационных систем персональных данных, эксплуатируемых исполнительными органами Хабаровского края, администрацией Губернатора и Правительства Хабаровского края

1.1. Исполнительные органы Хабаровского края, администрация Губернатора и Правительства Хабаровского края (далее также – операторы и край соответственно) эксплуатируют информационные системы персональных данных (далее также – ИСПДн) при осуществлении деятельности, связанной с реализацией служебных и (или) трудовых отношений, а также в связи с оказанием государственных услуг и (или) осуществлением государственных функций.

Настоящие Описание и определение распространяются на ИСПДн, эксплуатируемые исполнительными органами края, администрацией Губернатора и Правительства края, которые подключены к единой информационно-телекоммуникационной сети исполнительных органов края (далее – ЕИТКС), сегментированной на территориальном и канальном уровнях, имеющей централизованное управление, систему мониторинга и оповещения о критических событиях, одноточечное подключение к сетям связи общего пользования и информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет").

1.2. В ИСПДн обрабатываются персональные данные различных категорий и объема, которые принадлежат субъектам персональных данных, являющимся как сотрудниками операторов, так и иными лицами.

Категория и объем обрабатываемых в ИСПДн персональных данных, а также уровень защищенности персональных данных для этих ИСПДн определяются их операторами, оформляются актом классификации ИСПДн и утверждаются руководителем оператора.

1.3. В зависимости от характера и способов обработки персональных данных операторы осуществляют их обработку в ИСПДн, которые имеют

различную структуру (разноплановые ИСПДн).

По структуре ИСПДн подразделяются на автоматизированные рабочие места, локальные информационные системы и распределенные информационные системы.

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к сети "Интернет", ИСПДн подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

По режиму обработки информации ИСПДн подразделяются на однопользовательские и многопользовательские.

По разграничению прав доступа пользователей ИСПДн подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

1.4. В ИСПДн могут применяться технологии виртуализации, клиент(файл)-серверные технологии, виртуальные частные сети (VPN), удаленный доступ, веб-технологии, кластеризация, сегментирование. При этом в ИСПДн не применяются технологии автоматизации управления технологическим процессом, облачные технологии, технологии больших данных, беспроводные сети связи, мобильные устройства, суперкомпьютеры и грид-вычисления, посредством которых могут возникнуть дополнительные угрозы безопасности персональных данных.

Факт применения (использования) каждой из таких информационных технологий или структурно-функциональных характеристик в ИСПДн должен быть отражен оператором в утвержденной им частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – частная модель угроз).

1.5. Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты персональных данных, средства, в которых они реализованы, а также средства контроля эффективности защиты информации (далее – средства защиты ИСПДн) размещаются в пределах Российской Федерации. Контролируемой зоной ИСПДн являются административные здания, группы помещений или отдельные помещения операторов. В пределах контролируемой зоны находятся рабочие места пользователей, серверное оборудование, а также сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны могут находиться линии передачи данных и телекоммуникационное оборудование, используемое только для информационного обмена по сетям связи. Неконтролируемое пребывание посторонних лиц и неконтролируемый вынос средств защиты ИСПДн за пределы административных зданий операторов не допускаются.

1.6. Помещения, в которых ведется обработка персональных данных (далее также – Помещения), оснащаются входными дверями с замками. Операторами устанавливается порядок доступа в Помещения, препятствующий возможности неконтролируемого проникновения в Помещения или пребывания в Помещениях лиц, не имеющих права самостоятельного

доступа в Помещения. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в Помещения, а также в нерабочее время двери Помещений закрываются на ключ. Доступ посторонних лиц в Помещения допускается только в присутствии лиц, имеющих право самостоятельного доступа в Помещения, на время, ограниченное служебной необходимостью. При этом операторами предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным, в том числе через устройства ввода/вывода информации, а также возможность доступа к носителям персональных данных.

Устройства ввода/вывода информации, участвующие в обработке персональных данных, располагаются в Помещениях таким образом, чтобы исключить случайный просмотр обрабатываемой информации посторонними лицами, вошедшими в Помещение, а также через двери и окна Помещений.

1.7. Ввод персональных данных в ИСПДн и вывод персональных данных из ИСПДн осуществляются с использованием бумажных и машинных носителей информации, в том числе отчуждаемых машинных носителей информации. Операторами устанавливается порядок, обеспечивающий сохранность используемых машинных носителей персональных данных, осуществляется их учет.

1.8. В целях обеспечения целостности обрабатываемых в ИСПДн персональных данных операторы определяют порядок резервного копирования персональных данных и осуществляют резервирование персональных данных.

1.9. Оператор ИСПДн принимает меры по обеспечению безопасности персональных данных, в том числе посредством применения в ИСПДн средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

1.10. В ИСПДн, имеющих подключение к ЕИТКС, должны быть реализованы одноточечное подключение к сетям общего пользования и сети "Интернет" через централизованный и защищенный канал с использованием средств разграничения доступа в виде межсетевых экранов, сертифицированных на соответствие требованиям безопасности информации, установленным федеральным законодательством, и система обнаружения и предупреждения вторжений.

1.11. В ИСПДн в целях обеспечения безопасности персональных данных при их передаче по сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе сети "Интернет", применяются сертифицированные Федеральной службой безопасности Российской Федерации средства криптографической защиты информации (далее также – СКЗИ). Необходимость или отсутствие необходимости применения СКЗИ для обеспечения безопасности персональных данных в ИСПДн определяется ее оператором в разрабатываемой для этой ИСПДн частной модели угроз.

Операторами, применяющими СКЗИ, определяется порядок обеспечения безопасности применяемых СКЗИ и ключевых документов к ним, обеспечивающий сохранность документации на СКЗИ, машинных носителей информации с комплектами восстановления СКЗИ, а также носителей ключевой, парольной и аутентифицирующей информации. Документация на СКЗИ и носители хранятся только в Помещениях в сейфах или закрываемых на ключ шкафах (ящиках) в условиях, препятствующих свободному доступу к ним посторонних лиц.

1.12. С учетом особенностей функционирования, используемых структурно-функциональных характеристик и применяемых информационных технологий, а также опасности реализации угроз безопасности персональных данных и наступления последствий в результате несанкционированного или случайного доступа можно выделить следующие типы разноплановых ИСПДн, эксплуатируемых в исполнительных органах края, администрации Губернатора и Правительства края:

1-й тип – автоматизированные рабочие места, не имеющие подключения к сетям связи;

2-й тип – локальные ИСПДн (автоматизированные рабочие места и (или) комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, объединенного в единую информационную систему в пределах одного административного здания оператора), имеющие подключение к сетям связи, включая ЕИТКС, сети связи общего пользования и (или) сеть "Интернет";

3-й тип – кампусные ИСПДн (комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, объединенного в единую информационную систему в пределах нескольких административных зданий оператора, объединенных между собой с использованием защищенных каналов связи), имеющие подключение к сетям связи, включая ЕИТКС, сети связи общего пользования и (или) сеть "Интернет";

4-й тип – распределенные ИСПДн, имеющие подключение к ЕИТКС, сетям связи общего пользования и (или) сети "Интернет".

Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, эксплуатируемых исполнительными органами края, администрацией Губернатора и Правительства края, определяется операторами в частных моделях угроз применительно к перечисленным типам разноплановых ИСПДн.

1.13. К объектам защиты в ИСПДн относятся:

- персональные данные;
- носители персональных данных;
- средства защиты информации, в том числе СКЗИ;
- среда функционирования средств защиты информации;
- информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, в которых отражена защищаемая информация,

относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;

- носители защищаемой ключевой, парольной и аутентифицирующей информации пользователей ИСПДн;

- помещения, в которых осуществляется обработка персональных данных и (или) размещены средства защиты ИСПДн;

- каналы (линии) связи.

1.14. В ИСПДн обработка информации осуществляется в однопользовательском и многопользовательском режимах, осуществляется разграничение прав доступа пользователей ИСПДн. Обслуживание программных средств и средств защиты ИСПДн, средств защиты информации, в том числе СКЗИ и среды их функционирования, включая настройку, конфигурирование и распределение носителей ключевой информации между пользователями ИСПДн, осуществляется привилегированными пользователями (системные администраторы, ответственные за обеспечение безопасности персональных данных, администраторы безопасности информации), назначенными операторами.

1.15. ИСПДн с учетом их структурно-функциональных характеристик и условий эксплуатации, а также применяемых информационных технологий и предпринятых мер обеспечения безопасности персональных данных, указанных в настоящем разделе, имеют средний уровень исходной защищенности.

1.16. Операторы на постоянной основе реализуют меры обеспечения безопасности персональных данных, описанные в настоящем разделе.

2. Оценка возможностей нарушителей по реализации угроз безопасности персональных данных

2.1. Нарушителем является физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке в ИСПДн.

С учетом наличия прав доступа и возможностей доступа к информации и (или) компонентам ИСПДн нарушители подразделяются на два типа:

1) внешние нарушители – лица, не имеющие права доступа к ИСПДн или ее отдельным компонентам;

2) внутренние нарушители – лица, имеющие право постоянного или разового доступа к ИСПДн или ее отдельным компонентам.

2.2. С учетом состава и объема обрабатываемых персональных данных в ИСПДн, а также целей и задач их обработки в качестве возможных целей реализации нарушителями угроз безопасности персональных данных в ИСПДн могут быть:

- получение выгоды путем мошенничества или иным преступным путем;

- выявление уязвимостей в целях дальнейшей продажи уязвимостей и получения выгоды;

- любопытство или желание самореализации;

- реализация угроз безопасности персональных данных из мести;

- реализация угроз безопасности персональных данных непреднамеренно из-за неосторожности или неквалифицированных действий.

2.3. Для ИСПДн 1 – 4 типов с заданными структурно-функциональными характеристиками и особенностями функционирования (осуществляется разграничение прав доступа пользователей), а также с учетом сделанных предположений (прогноза) о возможных целях реализации угроз безопасности персональных данных рассматриваются следующие виды нарушителей:

1) лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ, – внутренние нарушители;

2) лица, обслуживающие инфраструктуру оператора (охрана, уборщики), – внутренние нарушители;

3) пользователи ИСПДн – внутренние нарушители.

2.4. Для ИСПДн 2 – 4 типов в дополнение к видам нарушителей, указанным в пункте 2.3 настоящего раздела, рассматриваются следующие виды нарушителей:

1) преступные группы (криминальные структуры) – внешние нарушители;

2) внешние субъекты (физические лица) – внешние нарушители;

3) уволенные (уволившиеся) сотрудники (пользователи) – внешние нарушители.

2.5. Нарушители могут обладать следующими возможностями по реализации угроз безопасности персональных данных в ИСПДн:

- получать информацию об уязвимостях отдельных компонентов ИСПДн, размещенных в общедоступных источниках;

- получать информацию о методах и средствах реализации угроз безопасности персональных данных (компьютерные атаки), размещенных в общедоступных источниках;

- самостоятельно осуществлять создание способов атак, подготовку и проведение атак на ИСПДн за пределами контролируемой зоны;

- самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом и без физического доступа к ИСПДн или ее отдельным компонентам, на которых реализованы меры и средства защиты информации, в том числе СКЗИ и среда их функционирования.

2.6. С учетом имеющейся совокупности предположений о целях и возможностях нарушителей по реализации угроз безопасности персональных данных в ИСПДн потенциал нападения при реализации угроз безопасности персональных данных для рассматриваемых видов нарушителей рассматривается как базовый (низкий).

Нарушитель с базовым (низким) потенциалом является непрофессионалом, использует стандартное оборудование, имеет ограниченные знания об ИСПДн или совсем их не имеет, возможность доступа к ИСПДн или ее отдельным компонентам ограничена и контролируется организационными мерами и средствами ИСПДн.

2.7. В ИСПДн угрозы безопасности персональных данных могут быть реализованы внешними и внутренними нарушителями с базовым (низким) потенциалом следующими способами:

- несанкционированный доступ и (или) воздействие на объекты защиты на аппаратном уровне (программы (микропрограммы), установленные производителями в аппаратных компонентах (чипсетах);

- несанкционированный доступ и (или) воздействие на объекты защиты на общесистемном уровне (операционные системы, гипервизоры);

- несанкционированный доступ и (или) воздействие на объекты защиты на прикладном уровне (системы управления базами данных, браузеры, веб-приложения, иные прикладные программы общего и специального назначения);

- несанкционированный доступ и (или) воздействие на объекты защиты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), кроме ИСПДн 1 типа;

- несанкционированный физический доступ и (или) воздействие на объекты защиты (каналы (линии) связи, технические средства, носители информации).

3. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

3.1. Угрозы безопасности персональных данных являются актуальными для ИСПДн, если существует вероятность их реализации нарушителем с базовым (низким) потенциалом и такая реализация приведет к негативным последствиям (ущербу) от нарушения конфиденциальности, целостности или доступности обрабатываемых персональных данных.

3.2. С учетом среднего уровня исходной защищенности ИСПДн, состава (категории) и объема обрабатываемых в ИСПДн персональных данных, а также особенностей их обработки для ИСПДн актуальны угрозы безопасности персональных данных, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

3.3. С учетом особенностей функционирования, используемых структурно-функциональных характеристик, применяемых информационных технологий, характера и способов обработки персональных данных и предпринятых операторами мер по обеспечению безопасности персональных данных, приведенных в разделе 1 настоящих Описания и определения, а также возможных негативных последствий от их реализации преднамеренные угрозы утечки персональных данных по техническим каналам для ИСПДн являются неактуальными, вследствие чего из преднамеренных угроз безопасности персональных данных следует учитывать только угрозы, реализуемые за счет несанкционированного доступа.

3.4. В качестве базовых угроз безопасности персональных данных для ИСПДн операторами определяются угрозы, определенные в Перечне угроз

безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых исполнительными органами Хабаровского края, администрацией Губернатора и Правительства Хабаровского края, утвержденном постановлением Правительства Хабаровского края от 20 февраля 2019 г. № 48-пр "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в исполнительных органах Хабаровского края, администрации Губернатора и Правительства Хабаровского края" (далее – перечень базовых угроз безопасности). При этом в перечень базовых угроз безопасности не включаются угрозы безопасности информации, связанные с информационными технологиями автоматизации управления технологическим процессом, облачными технологиями, технологиями больших данных, беспроводными сетями связи, мобильными устройствами, суперкомпьютерами и грид-вычислениями.

Перечень базовых угроз безопасности для ИСПДн устанавливается операторами в разрабатываемой для соответствующей ИСПДн частной модели угроз.

3.5. Оценка возможности реализации и актуальности угроз безопасности персональных данных осуществляется операторами в соответствии с методическим документом "Методика оценки угроз безопасности информации", утвержденным Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г., и приводится в частной модели угроз.

Актуальной следует определять угрозу, которая может быть реализована в ИСПДн и представляет опасность для персональных данных.

Для оценки возможности реализации угрозы применяются следующие показатели:

- уровень исходной защищенности ИСПДн;
- частота (вероятность) реализации рассматриваемой угрозы.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация конкретной угрозы безопасности персональных данных для данной ИСПДн в складывающихся условиях. С учетом базового (низкого) потенциала возможных нарушителей и среднего уровня исходной защищенности ИСПДн частота (вероятность) реализации угроз безопасности персональных данных для ИСПДн, эксплуатируемых исполнительными органами края, администрацией Губернатора и Правительства края, оценивается не выше средней.

Опасность угроз безопасности персональных данных определяется экспертным путем и характеризуется возможными негативными последствиями от их реализации для оператора и субъектов персональных данных. С учетом состава (категории) и объема обрабатываемых в ИСПДн персональных данных, а также необходимости обеспечения уровня защищенности персональных данных, не превышающего второй уровень защищенности,

опасность угроз безопасности персональных данных для ИСПДн, эксплуатируемых исполнительными органами края, администрацией Губернатора и Правительства края, оценивается не выше средней.

Оценка возможности реализации и актуальности угроз безопасности персональных данных, включенных в перечень базовых угроз безопасности для ИСПДн, осуществляется операторами с учетом максимальных оценочных значений частоты (вероятности) реализации и опасности угроз.

3.6. При наличии актуальных угроз безопасности персональных данных, которые могут быть нейтрализованы только с помощью СКЗИ, операторы ИСПДн разрабатывают частные модели угроз с учетом раздела 3 методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных Федеральной службой безопасности Российской Федерации 31 марта 2015 г. № 149/7/2/6-432."