**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ ПЕРМСКОГО КРАЯ**

**«ПОЛАЗНЕНСКАЯ РАЙОННАЯ БОЛЬНИЦА»**

(ГБУЗ ПК «ПОЛАЗНЕНСКАЯ РБ»)

# П Р И К А З

02.05.2024г. 98

**«Об организационных мерах защищаемой информации, не содержащей сведения, составляющие государственную тайну в Государственном бюджетном учреждении здравоохранения Пермского края «Полазненская районная больница»»**

В целях исполнения требований Федерального закона от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных», постановления Правительства РФ от 01 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства РФ от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без средств автоматизации», приказа 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»

**ПРИКАЗЫВАЮ:**

1. Утвердить и ввести в действие прилагаемые документы:
   1.1. Перечень лиц, осуществляющих обработку защищаемой информации, не содержащей сведения, составляющие государственную тайну, и имеющих доступ к обрабатываемой защищаемой информации, не составляющие государственную тайну в Государственном бюджетном учреждении здравоохранения Пермского края «Полазненская районная больница» (далее – Приложение 1);
   1.2. Инструкцию пользователя, осуществляющего обработку защищаемой информации, не содержащей сведения, составляющие государственную тайну, и имеющего доступ к обрабатываемой защищаемой информации, не содержащей сведения, составляющие государственную тайну в Государственном бюджетном учреждении здравоохранения Пермского края «Полазненская районная больница» (далее – Приложение 2);

1.3. Перечень лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационных систем, локально-вычислительных сетей и систем защиты информации в Государственном бюджетном учреждении здравоохранения Пермского края «Полазненская районная больница» (далее – Приложение 3);

1.4. Перечень лиц, ответственных за выявление инцидентов информационной безопасности и реагирование на них в информационных системах и локально-вычислительных сетях Государственного бюджетного учреждения здравоохранения Пермского края «Полазненская районная больница» (далее – Приложение 4);

1.5. Инструкцию по выявлению инцидентов информационной безопасности и реагирование на них в информационных системах и локально-вычислительных сетях Государственного бюджетного учреждения здравоохранения Пермского края «Полазненская районная больница» (далее – Приложение 5)

2. Назначить программиста Масленникову О.В. ответственной за регистрацию и ведение учета пользователей в информационных системах ГБУЗ ПК «Полазненская районная больница»;
3. Назначить программиста Масленникову О.В. ответственным за планирование и контроль мероприятий по защите информации в информационных системах ГБУЗ ПК «Полазненская районная больница»;
4. Калашникова А.С., главный врач ответственный за управление (администрирование) системой защиты информации в информационных системах ГБУЗ ПК «Полазненская районная больница»;
5. Допустить к обработке защищаемой информации, не относящейся к государственной тайне, в том числе персональным данным, сотрудников, включенных в Приложение 1.
   5.1. Сотрудникам, включенным в Приложение 1 при выполнении должностных обязанностей, руководствоваться документом «Инструкция пользователя, осуществляющего обработку защищаемой информации, не содержащей сведения, составляющие государственную тайну, и имеющего доступ к обрабатываемой защищаемой информации, не содержащей сведения, составляющие государственную тайну».
6. Разрешить сотрудникам, включенным в Приложение 3, внесение изменений в конфигурацию информационных систем ГБУЗ ПК «Полазненская районная больница», в конфигурацию системы защиты информации в их составе.
7. Сотрудникам, включенным в Приложение 3 выявлять и проводить расследования инцидентов в соответствии с документом «Инструкция по выявлению инцидентов информационной безопасности и реагирование на них».
8. Признать утратившими силу приказы ГБУЗ ПК «Полазненская РБ» от 18.08.2023г. №190б «О мерах защиты при работе с информацией ограниченного доступа, не составляющих государственную тайну в ГБУЗ ПК «Полазненская РБ», от 19.08.2023г. №191а «Об утверждении Политики и регламента обработки и защиты персональных данных в ГБУЗ ПК «Полазненская РБ»».
9. Контроль за исполнением приказа оставляю за собой

Главный врач А.С. Калашникова

Приложение №2

УТВЕРЖДЕНА
приказом ГБУЗ ПК «Полазненская РБ»
02.05.2024г. №98

**Инструкция**
**пользователя, осуществляющего обработку информации, не содержащей сведения, составляющие государственную тайну, и имеющих доступ к обрабатываемой защищаемой информации, не содержащей сведения, составляющие государственную тайну в ГБУЗ ПК «Полазненская РБ»**

**1. Общие положения**

Настоящая инструкция определяет общие положения работы пользователей в информационных системах персональных данных ГБУЗ ПК «Полазненская РБ» (далее – пользователь, системы).

Допуск пользователей для работы с информацией, обрабатываемой в системах осуществляется в соответствии с Приложением 1.

Вход пользователя в системы осуществляется на основе ввода (по запросу системы) имени учетной записи и пароля.

Пользователь несет персональную ответственность за свои действия.

**2. Правила эксплуатации системы защиты информации**

Перед эксплуатацией системы защиты информации, пользователю систем необходимо внимательно ознакомиться с эксплуатационной и технической документацией.

Системы должны обеспечивать конфиденциальность, доступность и целостность данных, обрабатываемых в системах, исключающих несанкционированный, в том числе случайный доступ к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных не санкционированных действий.

**3. Квалификационные требования**

Пользователь должен знать:

- законодательные и нормативные правовые акты, регламентирующие деятельность в сфере обработки информации ограниченного доступа, не относящейся к государственной тайне, в том числе персональных данных;
- внутренние локальные акты оператора, регламентирующие обработку информации ограниченного доступа, не относящейся к государственной тайне, в том числе персональных данных;
- внутренние локальные акты оператора, регламентирующего обработку информации ограниченного доступа, не относящейся к государственной тайне.

**4. Права пользователя**

Пользователь имеет право:

- в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам систем, присвоенным ему лицом, ответственным за обеспечение безопасности информации ограниченного доступа, не относящейся к государственной тайне (далее – администратор безопасности информации)

**5. Основные функциональные обязанности пользователя**

Пользователь обязан:

- выполнять требования действующих нормативных правовых актов и руководящих документов Российской Федерации, а также локальных актов оператора, регламентирующих порядок действий по обеспечению безопасности информации ограниченного доступа, не относящейся к государственной тайне;
- выполнять в системах только те процедуры, которые определены для него его обязанностями;
- соблюдать правила при работе в сетях общего доступа и (или) международного информационного обмена в сети «интернет» и других;
- экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информации посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты);
- обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций по вопросам информационной безопасности, необходимо обращаться к администратору безопасности информации;
- при отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш «Ctrl+Alt+Del» и выбрать опцию блокировка либо заблокировать доступ иным способом, предусмотренным в операционной системе;
- при использовании планировщика заданий, состав запускаемого программного обеспечения на рабочем месте согласовывается с администратором;
- в пределах возложенных функций принимать меры по реагированию в случае возникновения внештатных или аварийных ситуаций с целью ликвидации их последствий;
- по окончании работы выйти из системы, выключить компьютер;
- соблюдать правила работы со съемными носителями информации ограниченного доступа, не относящейся к государственной тайне;

Пользователю запрещается:

- разглашать информацию ограниченного доступа, не относящейся к государственной тайне третьим лицам;
- копировать информацию ограниченного доступа, не относящуюся к государственной тайне, на внешние носители без разрешения своего руководителя;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к каталогам в системах;
- подключать к системам личные отчуждаемые съемные машинные носители информации и мобильные устройства;
- отключать (блокировать) установленные средства защиты информации;
- обрабатывать в системах информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к объектам доступа систем;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам систем;
- привлекать посторонних лиц для осуществления ремонта или настройки средств систем без согласования с администратором безопасности информации;
- осуществлять установку и эксплуатацию средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации в системах;
- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

- осуществлять перемещение физических (или виртуальных) машин систем за пределы центра обработки данных.

### 6. Организация парольной защиты

Правила формирования пароля:

- пароль не должен содержать имя учетной записи или какую-либо его часть;
- пароль должен состоять не менее чем из 8 символов, специального символа, заглавной буквы;
- запрещается использовать в качестве пароля простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе полученной из свободного доступа или на основе социальной инженерии;
- пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем на четыре символа;
- смена пароля пользователя должна производиться не реже одного раза в 120 дней.

Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;
- во время ввода пароля необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами;

Правила хранения пароля:

- запрещается записывать пароль на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям и администраторам личный пароль и регистрировать их в системе под своим паролем;
- лица, использующие паролирование, обязаны четко знать и строго выполнять требования настоящей инструкции;
- своевременно сообщать администратору безопасности информации об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

### 7. Правила работы в сетях общего доступа и (или) международного обмена

Работа в сетях общего доступа и (или) международного информационного обмена (сеть Интернет и другие)(далее – сеть) на элементах систем должна проводиться при служебной необходимости.

При работе в сети необходимо:

- настроить веб-обозреватель на блокирование выполнения мобильного кода, сценариев и активного содержимого веб-сайтов, блокирования показа рекламных баннеров и ссылок на веб-сайтах, исключения сохранения логинов и паролей в веб-обозревателе, исключения сохранения истории посещенных веб-сайтов, исключения сохранения cookie-файлов после закрытия веб-обозревателя, исключить автозаполнения форм на веб-сайтах, исключения автоматической установки и обновления дополнений для веб-обозревателя;
- соблюдать правила распознавания методов социальной инженерии: фишинга, фарминга, обмана пользователей, навязывания ложных убеждений, использование прозрачных кнопок, подмена надписей на элементах управления и прочие методы.

При работе в сети запрещается:

- осуществлять работы при отключенных средствах защиты (антивирус и другие);

- передавать по сети информацию ограниченного доступа, не относящуюся к государственной тайне, без использования средств шифрования;

- скачивать из сети программное обеспечение и другие файлы;

- посещать сайты с сомнительной репутацией (сайты, содержащие нелегально распространяемое программное обеспечение, фильмы, музыку, и другие);

- нецелевое использование подключения к сети.

### 8. Обязанности пользователя по обеспечению антивирусной защиты

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно или вместе с администратором безопасности информации должен провести внеочередной контроль систем.

В случае обнаружения при проведении антивирусной поверки зараженных файлов компьютерными вирусами пользователь обязан:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

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

При необходимости пополнения базы систем данными, полученными со стороны с помощью съемных машинных носителей информации, контролировать отсутствие вирусного заражения информации на съемном машинном носителе информации.

Пользователь обязан периодически, не реже одного раза в неделю, проводить проверку антивирусом на наличие вирусного заражения.

Пользователь обязан следить за тем, чтобы антивирус был все время включен, а также следить за своевременным обновлением антивирусных баз.

### 9. Правила работы со съемными носителями информации ограниченного доступа, не относящейся к государственной тайне

К носителям информации ограниченного доступа, не относящейся к государственной тайне, относятся:

- съемные машинные носители информации (флеш-накопители, внешние накопители на жестких дисках и иные устройства);

- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичное по функциональности устройства);

- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках);

- графические и текстовые распечатки на бумажных носителях, содержащие информацию ограниченного доступа, не относящейся к государственной тайне.

- использование портативных вычислительных устройств, имеющих встроенные носители информации, для администрирования серверных частей систем не допускается.

- выдачу съемных машинных носителей информации ограниченного доступа, не относящей к государственной тайне, осуществляет администратор безопасности информации. Пользователь получает учтенный съемный машинный носитель от администратора безопасности информации для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. Использование неучтенных машинных накопителей информации не допускается.

При использовании носителей с информацией ограниченного доступа, не относящейся к государственной тайне, запрещается:

- хранить носители с информацией ограниченного доступа, не относящейся к государственной тайне, вместе с носителями открытой информации на рабочих столах, оставлять их без присмотра или передавать на хранение другим людям;

- выносить носители с информацией ограниченного доступа, не относящейся к государственной тайне, из служебных помещений для работы с ними на дому, в гостиницах и т.д., без соответствующего на то разрешения руководителя или лица, выдавшего съемный машинный носитель.

- при отправке или передачи информации ограниченного доступа, не относящейся к государственной тайне, на носители записываются только предназначенные адресатам данные. Вынос носителей информации ограниченного доступа, не относящейся к государственной тайне, для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя оператора или руководителя работ.

В случае утраты носителей информации ограниченного доступа, не относящейся к государственной тайне, либо разглашения содержащихся в них сведений немедленно ставится в известность руководство оператора, а также администратор безопасности информации. Организуется служебное расследование с оформлением акта и разработкой мер, устраняющих повторный факт утраты носителей информации ограниченного доступа, не относящейся к государственной тайне. На утраченные носители составляется акт. Соответствующие отметки вносятся в журнал учета съемных машинных носителей информации, а также распечаток текстовой, графической и иной информации.

В случае необходимости использования съемных машинных носителей информации для исполнения конкретных должностных обязанностей, предусматривающих использование съемных машинных носителей информации, администратор запрашивает у администратора безопасности информации выдать такие устройства. По окончанию работ, требующих использования съемных машинных носителей информации, администратор сдает такие устройства администратору безопасности информации.

### 10. Противодействие социальной инженерии

Социальная инженерия – это совокупность приемов, методов, технологий реализации такого пространства, условий, которые обеспечивают конкретный необходимый результат, основанный на человеческом факторе.

Методы по противодействию социальной инженерии:

- разработка четкого плана действий для сотрудников в случае обнаружения атаки социальной инженерии;

- разработка вежливого отклонения запроса о важной информации, пока не будет установлена личность запрашивающего и его право на доступ к этой информации.

- обучение и тренинг персонала навыкам противодействия методам социальной инженерии, разработка тренингов по установлению бдительности персонала, периодическая проверка знаний и навыков сотрудников путем проведения специальных проверок;

Правила предотвращения обмана пользователей:

- в случае попытки посторонних лиц получить от сотрудника сведения конфиденциального характера, немедленно сообщить об этом непосредственному руководителю.

Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – связке логин-пароль.

Правила предотвращения фишинга:

- осуществлять проверку URL-адреса любого сайта, который запрашивает идентификационную информацию;

- рекомендуется проверять сертификат безопасности веб-узла перед вводом личной информации в системах;

- запрещается работа с информационными ресурсами в системах, не находящихся под контролем пользователя.

Фарминг – это вид интернет-мошенничества, целью которого является автоматическое перенаправление злоумышленниками пользователя интернета на ложный сайт или сайт-копию.

Правила предотвращения фарминга:

- использовать вовремя обновленное программное обеспечение;

- рекомендуется отключить функции в системах, которые несут ответственность за предварительный просмотр.

**11. Ответственность**

Пользователь несет ответственность за:

- неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в пределах, определенных законодательством Российской Федерацией;

- совершенные в процессе осуществления своей деятельности правонарушения в пределах, определенных уголовным и гражданским законодательством Российской Федерации;

- невыполнение или ненадлежащее выполнение приказов, распоряжений и поручений оператора;

- некачественное и несвоевременное выполнение обязанностей, возложенных на него настоящей инструкцией;

- неправильное заполнение и ведение всей документации, регламентированной требованиями оператора;

- разглашение информации ограниченного доступа, не относящейся к государственной тайне.

Приложение 5
УТВЕРЖДЕНА
приказом ГБУЗ ПК «Полазненская РБ»
02.05.2024г. №98

# ИНСТРУКЦИЯ
## по выявлению инцидентов в информационной безопасности и реагированию на них в информационных системах и сетях ГБУЗ ПК «Полазненская РБ»

### 1. Общие положения

Настоящая инструкция по выявлению инцидентов информационной безопасности и реагированию на них в информационных системах и сетях в Государственном бюджетном учреждении здравоохранения Пермского края «Полазненская районная больница» (далее – инструкция) устанавливает порядок действий лица, ответственного за выявление инцидентов информационной безопасности и реагирование на них в информационных системах и сетях в Государственном бюджетном учреждении здравоохранения Пермского края «Полазненская районная больница» (далее – ответственный), при выявлении а также порядок проведения расследования инцидента информационной безопасности.

Настоящая инструкция разработана в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
- *Методический документ «Меры защиты информации в государственных* информационных системах», утвержден ФСТЭК России 11.02.2014;
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержден ФСТЭК России 18.02.2013 №21
- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утверждено приказом ФСБ России от 09.02.2005 №66;
- Состав и содержание 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, утвержден приказом ФСБ России от 10.07.2014 №378;
- Приказ ФАПСИ от 13.06.2001 №152 «Об утверждении инструкции об организации и обеспечении безопасности, хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведения, составляющих государственную тайну»;
- ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

Ответственный, назначается приказом руководителя организации, и осуществляет мониторинг событий безопасности в соответствии с настоящей инструкцией.

Инцидент информационной безопасности (далее – инцидент) в рамках настоящей инструкции – это одно или серия событий, которое привело к уничтожению, модификации, копированию, распространению (только в отношении информации ограниченного доступа) информации, обрабатываемой на автоматизированных рабочих местах и (или) серверах

информационных систем в Государственном бюджетном учреждении здравоохранения Пермского края «Полазненская районная больница», а также блокировке доступа к ним.

К инцидентам не относятся события информационной безопасности – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение принятых организационно-распорядительных документов по защите информации или отказ защитных мер, или возникновение неизвестной раннее ситуации, которая может иметь отношение к безопасности.

Событие может быть результатом случайных или преднамеренных попыток компрометации защитных мер, но в большинстве случаев событие само по себе не означает, что попытка в действительности была успешной и, следовательно, каким-то образом повлияла на конфиденциальность, целостность и (или) доступность, то есть не все события будут отнесены к категории инцидентов.

Информация об инцидентах является защищаемой информацией и к ней применяются те же утвержденные правила и политики по защите информации, что и к другой защищаемой конфиденциальной информации в информационных системах Государственном бюджетном учреждении здравоохранения Пермского края «Полазненская районная больница».

## 2. Выявление инцидента

Основными источниками, от которых ответственный может получить сведения об инцидентах являются:

- сообщения от сотрудников организации о выявленных фактах нарушения информационной безопасности;
- результаты работы средств мониторинга информационной безопасности, результаты проверок и аудита (внутреннего или внешнего);
- электронные журналы и оповещения операционных систем и серверов, рабочих станций, систем резервного копирования, систем защиты информации и других систем.

Ответственный должен регулярно информировать сотрудников о необходимости немедленного его оповещения о возникновении инцидента с указанием контактной информации и способов предоставления информации.

## 3. Порядок действий ответственного при обнаружении инцидента

### 3.1 Анализ исходной информации и принятие решения о проведении расследования инцидента

Ответственный с момента получения информации о предполагаемом инциденте незамедлительно проводит первоначальный анализ получения данных. По усмотрению ответственного в случае если инцидент не привел к негативным последствиям в связи с уничтожением, модификацией, копированием, распространением (только в отношении информации ограниченного доступа) информации, обрабатываемой на автоматизированных рабочих местах и (или) серверах, а также блокировке доступа к ним (например, случайное удаление файлов с информацией, имеющей резервные копии, не имеет негативный последствий для функционирования информационных систем ГБУЗ ПК «Полазненская РБ») расследование может не проводиться.

В случае если инцидент привел к негативным последствиям, ответственный собирает группу реагирования на инцидент в целях совместного принятия решения о необходимости проведения расследования инцидента. В группу включаются компетентные сотрудники в области информационных технологий в организации.

В случае принятия группой решения о необходимости проведения расследования инцидента, ответственный информирует об инциденте руководителя организации.

### 3.2 Реагирование на инцидент (устранение причин и последствий инцидента)

Ответственный совместно с группой реагирования на инциденты по согласованию с руководителем организации определяет в кратчайшие сроки, не превышающие одного рабочего дня, инициирует первоочередные меры, направленные на локализацию инцидента и минимизацию его последствий.

Процесс реагирования на инцидент и восстановление ущерба, нанесенного информационным система ГБУЗ ПК «Полазненская РБ», состоит из следующих этапов:

- обнаружение и оповещение о возникновении инцидента (человеком или автоматическими средствами);
- сбор информации, связанной с инцидентом, и оценка этой информации с целью определения, какие события можно отнести к категории инцидента;
- незамедлительное реагирование на инцидент;
- локализация АРМ или сегмента сети, на который распространились негативные последствия инцидента;
- при необходимости – привлечение специалистов сторонних организаций для получения качественных консультаций;
- выполнение мер по нейтрализации факторов, вызвавших инцидент;
- восстановление ущерба, вызванного инцидентом;
- регистрация всех действий и решений для последующего анализа;
- правовая оценка инцидента;
- при необходимости и при наличии правовых оснований, обращение в правоохранительные органы;
- принятие мер для предотвращения подобных инцидентов в будущем.

В случае если инцидент связан с совершением компьютерных атак или внедрением вредоносного программного обеспечения, ответственный в целях совместной выработки и реализации мер по их локализации, устранению и ликвидации последствий должен незамедлительно информировать:

- дежурную службу Управления ФСБ России по Пермскому краю, тел. +7(342)2393939
- Главное управление МВД России по Пермскому краю, тел. 102.

**3.3 Расследование (проведение служебного расследования) инцидента**

После локализации инцидента и восстановления штатного режима работы проводится расследование инцидента.

Расследование инцидента проводится в следующем порядке:

- проводится сбор информации об инциденте из всех возможных источников, проводится анализ собранной информации, формируется доказательная база;
- анализируются каналы атаки, уязвимости и другие факторы, которые сделали возможным возникновение инцидента;
- анализируется сценарий действий нарушителя, в случае антропогенной природы инцидента;
- составляется список подозреваемых в инциденте лиц, в случае антропогенный природы инцидента;
- определяется степень ущерба, нанесенная информационным системам ГБУЗ ПК «Полазненская РБ», организации, субъектам персональных данных в результате инцидента;
- составляется заключение о расследовании.

Важным является обеспечение сохранности и целостности доказательств факта возникновения инцидента для их представления на судебном процессе при необходимости привлечения лица, по вине которого произошел инцидент, к ответственности в соответствии с действующим законодательством Российской Федерации.

По результатам расследования ответственный формирует заключение по расследованию инцидента, согласовывает его со всеми участниками расследования и передает имеющиеся материалы (в объеме, достаточном для принятия решения) руководителю организации для решения вопроса о привлечении виновного в инциденте к ответственности.

**3.4 Порядок документирования процедур**

На основании собранной в процессе расследования инцидента информации ответственный заполняет отчет об инциденте, в целях систематизации информации об инцидентах и ее дальнейшего анализа. В отчете указывается следующая информация:

1) Дата и время совершения инцидента.

2) Источник информации, от которого ответственный получил информацию об инциденте.

3) Ф.И.О, должность лица, по вине которого произошел инцидент.

Если инцидент произошел по причине некорректной работы средств защиты информации или их некорректной настройки, ответственность за инцидент несет лицо, ответственное за установку, настройку и функционирование средств защиты информации.

Если инцидент произошел по причине некорректной работы программного обеспечения или технических средств, ответственность несет лицо, ответственное за функционирование программного обеспечения и технических средств.

В случае если инцидент произошел вследствие невыполнения сотрудниками требований организационно-распорядительных документов по защите информации организации, персональную ответственность несут сотрудники, нарушившие требования документов, в том числе сотрудники на которых возложен контроль соблюдения требований данных документов.

4) Описание инцидента.

В данном разделе необходимо указать какое из свойств информации было нарушено (конфиденциальность, целостность, доступность) в результате инцидента и указать функциональное воздействие инцидента на функционирование информационных систем и сетей в ГБУЗ ПК "Полазненская РБ»:

Несуществующий: воздействие на способность информационных систем и сетей ГБУЗ ПК «Полазненская РБ» выполнять свои функции отсутствует;

Низкий: минимальный эффект, информационные системы и сети ГБУЗ ПК «Полазненская РБ» все еще могут выполнять все основные функции, но со сниженной эффективностью;

Средний: информационные системы и сети ГБУЗ ПК «Полазненская РБ» потеряли способность обеспечить часть основных функций;

Высокий: информационные системы и сети ГБУЗ ПК «Полазненская РБ» не в состоянии выполнять свои функции.

5) Причины инцидента.

6) Меры, принятые для устранения причин, последствий инцидента

Данный пункт позволит в случае повторного возникновения инцидента в минимальные сроки устранить его.

По результатам формирования отчета об инциденте ответственным заполняется «Журнал учета инцидентов информационной безопасности» (далее – Приложение 6).

Журнал позволяет вести статистику всех инцидентов информационной безопасности, которая является показателем эффективности функционирования системы защиты информации. Статистику инцидентов следует регулярно анализировать в рамках проведения оценки защищенности информационных систем ГБУЗ ПК «Полазненская РБ»

### 3.5 Выработка корректирующих и превентивных мероприятий

По результатам расследования инцидента принимается решение о необходимости принятия дополнительных организационных и технических мер, направленных на предотвращение или минимизацию рисков возникновения подобных нарушений в будущем (в некоторых случаях последствия инцидента незначительны по сравнению с корректирующими и превентивными действиями, и тогда целесообразно не совершать дальнейших шагов после устранения последствий инцидента).

После выявления и наказания виновных в инциденте, ответственным после согласования с руководством организации могут быть проведены занятия с сотрудниками организации по разбору произошедшего инцидента с целью предотвращения повторения инцидента в будущем.

Приложение
к Инструкции по выявлению
инцидентов информационной
безопасности и реагирование на них в
ГБУЗ ПК «Полазненская РБ»

**Журнал №__**

Учета инцидентов информационной безопасности, произошедших в информационных системах и сетях ГБУЗ ПК «Полазненская РБ»

Том №____
Начат:_____20__г.
Окончен:_____20__г.
На ____ листах
Срок хранения:_____ лет

Заверен _____ _____
подпись ФИО

Пермь, 20__г.

**Правила ведения журнала**

1. Журнал учета инцидентов информационной безопасности, произошедших в «Наименование ИС» (далее – журнал инцидентов) должен быть пронумерован, прошнурован, скреплен печатью;
2. Журнал инцидентов заверяется подписью председателя комиссии по вопросам информационной безопасности;
3. Срок хранения журнала – пять лет с даты внесения последней записи;
4. Порядок заполнения граф:

Графа 1. – проставляется порядковый номер инцидента информационной безопасности.
Графа 2. – указывается краткое описание инцидента информационной безопасности, включающие: описание затронутых инцидентом информационных ресурсов информационных систем ГБУЗ ПК «Полазненская РБ», характер воздействия, источник воздействия, наличие лог-файлов, и другие сведения об инциденте.
Графа 3. – указывается фамилия, имя, отчество, должность сотрудника, обнаружившего инцидент, дата и время обнаружения. Дата пишется в формате «дд.мм.гггг» или «дд/мм/гггг». Время пишется в формате «чч:мм».
Графа 4. – дата пишется в формате «дд.мм.гггг» или «дд/мм/гггг». Время пишется в формате «чч:мм».
Графа 5. – указываются дата, время доведения информации об инциденте, фамилия, имя, отчество, должность сотрудника, принявшего информацию об инциденте.
Графа 6. – подпись ответственного лица за реагирование на инциденты информационной безопасности в информационных системах и сетях ГБУЗ ПК «Полазненская РБ».

| № п/п | Краткое описание инцидента | ФИО, должность сотрудника, обнаружившего инцидент, дата и время обнаружения | Дата и время пресечения несанкционированного воздействия | Дата, время доведения информации об инциденте; ФИО, должность сотрудника, принявшего информацию | Подпись ответственного за реагирование на инцидент |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |