ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«Камчатский краевой противотуберкулезный диспансер»
(ГБУЗ ККПТД)

ПРИКАЗ № 1041

г. Петропавловск-Камчатский «30» 12 2020 года

О назначении группы реагирования на инциденты информационной безопасности и о правилах регистрации инцидентов информационной безопасности и реагирования на них в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана

В целях исполнения требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России № 17 от 11.02.2013 в части регистрации событий безопасности

ПРИКАЗЫВАЮ:

1. Назначить внутреннюю группу по реагированию на инциденты информационной безопасности (далее – ГРИИБ) в составе:

- Малышев М.Н

2. Утвердить прилагаемую, разработанную в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», инструкцию по реагированию на инциденты информационной безопасности.

3. ГРИИБ в своей работе руководствоваться инструкцией по реагированию на инциденты информационной безопасности, руководящими документами ФСТЭК России и ФСБ России, государственными стандартами в области информационной безопасности и общедоступными источниками об угрозах и уязвимостях информационных систем.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач А. В. Громов

УТВЕРЖДЕНА
Приказом О назначении группы реагирования на инциденты информационной безопасности и о правилах регистрации инцидентов информационной безопасности и реагирования на них в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана
от «___» _____ 2020г. №

Инструкция по реагированию на инциденты информационной безопасности в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политики информационной безопасности и меры по защите информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана не могут полностью гарантировать защиту информации, информационных систем, сервисов или сетей. Всегда существует вероятность, что после внедрения системы защиты информации останутся слабые места, которые могут сделать обеспечение информационной безопасности неэффективным, и, следовательно, инциденты информационной безопасности – возможными. Инциденты информационной безопасности могут оказывать прямое или косвенное негативное воздействие на деятельность Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана. Также неизбежно выявление новых, ранее не идентифицированных угроз безопасности информации. Исходя из вышесказанного, важно применять структурный подход к:

- обнаружению, оповещению об инцидентах безопасности и их оценке;
- реагированию на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и (или) восстановления после наступления негативных последствий вследствие инцидента безопасности информации;
- извлечению уроков из инцидентов информационной безопасности, совершенствованию системы защиты информации, введению превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности.

1.2. Регистрация событий безопасности, выявление инцидентов безопасности информации и реагирование на них производится, в том числе, с целью выполнения требований Приказа ФСТЭК № 17 от 11.02.2013 с индексами: РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7.

1.3. Для реагирования на инциденты информационной безопасности создается группа реагирования на инциденты информационной безопасности (далее – ГРИИБ).

1.4. Важным членом ГРИИБ является Администратор безопасности информации (далее – Администратор), назначаемый приказом руководителя ГБУЗ «Камчатский краевой противотуберкулезный диспансер». Он осуществляет централизованный мониторинг событий безопасности в соответствии с Инструкцией администратору безопасности.

1.5. Инцидентом информационной безопасности (далее - инцидент ИБ) является событие, нарушающее одно из свойств защищаемой информации (целостность, доступность или конфиденциальность) или несколько таких свойств одновременно.

2. РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ В ФИЛИАЛЕ № 1 "ГБУЗ ККПТД" - ПГТ. ПАЛАНА.

2.1. События безопасности, подлежащими регистрации, являются записи в журналах операционных систем, прикладного программного обеспечения и средств защиты информации (электронные журналы сообщений). К событиям безопасности относятся следующие виды записей в таких системных журналах:

- записи о входе пользователя в операционную систему или прикладное программное обеспечение;
- записи о неудачных попытках аутентификации пользователя в системе (время, количество попыток, время блокировки учетной записи);
- записи о времени окончания сеанса работы пользователя в операционной системе или в прикладном программном обеспечении;
- записи о доступе к легальной для данного пользователя защищаемой информации;
- записи о попытках доступа к запрещенной для данного пользователя защищаемой информации;
- записи об использовании разрешенных съемных носителей информации и мобильных устройств (время включения, копируемая информация, время отключения и т. д.);
- записи о попытках использования запрещенных в системе съемных носителей информации и мобильных устройств;
- записи о попытках повышения собственных полномочий в системе;
- записи об аномальной сетевой активности;
- записи о попытках доступа к управлению разграничением доступа к информации и к управлению средствами защиты информации;
- записи об обнаружениях вирусов, червей, троянов антивирусными средствами;
- записи о попытках установки запрещенного прикладного программного обеспечения;
- записи о запуске подозрительных файлов, полученных по электронной почте или по другим каналам;
- записи о нарушении правил и политик информационной безопасности;
- записи о передаче защищаемой информации по каналам связи.

2.2. Информация о событиях безопасности информации является защищаемой информацией и к ней применяются те же, утвержденные правила и политики по защите информации, что и к другой защищаемой конфиденциальной информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана.

..

2.3. Далеко не все события безопасности информации являются инцидентами безопасности информации. Инцидентами безопасности являются только запрещенные в ИС действия, с которыми может быть связано создание угрозы информационной безопасности.

2.4. Информация о событиях безопасности также может поступать Администратору безопасности от сотрудников Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана, заметивших аномальную активность в информационной системе. Информацией о событиях безопасности также являются сведения о потере, краже или компрометации машинных и других носителей информации.

2.5. Администратор анализирует электронные журналы сообщений и принимает решение, является ли событие безопасности инцидентом информационной безопасности.

2.6. По степени возможного ущерба информационной системе Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана, инциденты информационной безопасности можно условно разделить на незначительные и значительные.

2.7. Незначительными признаются инциденты информационной безопасности, соответствующие одному или нескольким критериям:

- инцидент был быстро обнаружен и локализован, значительных последствий в результате инцидента не произошло;
- инцидент затронул небольшое количество сотрудников Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана;
- инцидент не требует существенных усилий и затрат на восстановление работоспособности информационной системы или ее частей;
- в результате инцидента не была нарушена конфиденциальность, целостность и доступность больших массивов защищаемой информации (например, всей базы данных), нарушена безопасность только небольшого фрагмента информации (одной или нескольких записей базы данных);
- инцидент не требует концептуального пересмотра политик информационной безопасности в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана;
- в результате инцидента организации нанесен минимальный ущерб или не нанесено никакого ущерба;
- инцидент не вызвал долгосрочного простоя информационной системы и не нарушил технологические процессы обработки информации.

2.8. Значительными признаются все инциденты информационной безопасности, которые не могут быть признаны незначительным в соответствии с пунктом 2.7 настоящей Инструкции.

3. РЕАГИРОВАНИЕ НА ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УСТРАНЕНИЕ ПОСЛЕДСТВИЙ И ПРИЧИН ИНЦИДЕНТА

3.1. В случае обнаружения незначительных инцидентов, Администратор самостоятельно принимает меры по устранению последствий инцидента информационной безопасности.

3.2. В случае обнаружения значительных инцидентов, Администратор созывает ГРИИБ, которая оценивает инцидент и реагирует на него наиболее целесообразным и результативным способом.

3.3. После устранения последствий инцидента, ГРИИБ делаются соответствующие выводы (оформляемые в виде акта в свободной форме) и вносятся предложения по совершенствованию технических и организационных аспектов защиты информации в ГИС с целью предотвращения подобных инцидентов в будущем.

3.4. Процесс реагирования на инцидент информационной безопасности и восстановление ущерба, нанесенного ГИС, может состоять из следующих этапов:

- обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами);
- сбор информации, связанной с событиями информационной безопасности и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;
- незамедлительное реагирование на инцидент ИБ;
- 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 ИБ;
- восстановление ущерба, вызванного инцидентом ИБ;
- регистрация всех действий и решений для последующего анализа;

- правовая оценка инцидента ИБ;
- при необходимости и при наличии правовых оснований, обращение в правоохранительные органы;
- принятия мер для предотвращения подобных инцидентов в будущем.

4. РАССЛЕДОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Расследование инцидента информационной безопасности проводится с целью выявления и наказания лиц, виновных в инциденте, а также с целью выявления недоработок в политиках информационной безопасности и их оперативного устранения.

4.2. Расследование инцидента проводится Администратором безопасности самостоятельно (в случае незначительного инцидента) либо ГРИИБ (в случае значительного инцидента). В случаях, когда виновником инцидента является внешний нарушитель, к расследованию инцидента могут привлекаться сотрудники правоохранительных органов в установленном действующим законодательством порядке.

4.3. 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 появление инцидента информационной безопасности;
- анализируются сценарии действий нарушителя, в случае антропогенной природы инцидента;
- составляется список подозреваемых в инциденте лиц, в случае антропогенной природы инцидента;
- выявляются лица, виновные в инциденте информационной безопасности, в случае антропогенной природы инцидента;
- определяется степень ущерба, нанесенная информационной системе, организации, субъектам персональных данных в результате инцидента информационной безопасности;
- составляется отчет о расследовании.

4.4. В случаях, если инцидент произошел по вине сотрудников Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана руководство Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана принимает решение о мерах, которые будут применены к виновному лицу.

4.5. В случаях, если инцидент произошел по вине контрагента или сотрудника сторонней организации, осуществляющей какие-либо работы в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана, виновный в инциденте несет ответственность в соответствии с положениями договора между Филиалом № 1 "ГБУЗ ККПТД" - пгт. Палана и контрагентом/сторонней организацией.

4.6. В случаях, если инцидент произошел по вине внешнего нарушителя, виновный несет ответственность в соответствии с уголовным и административным кодексами Российской Федерации.

4.7. После выявления и наказания виновных в инциденте, Администратором безопасности после согласования с руководством Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана могут быть проведены занятия с сотрудниками Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана по разбору произошедшего инцидента с целью предотвращения повторения инцидента в будущем.

4.8. Из каждого инцидента информационной безопасности извлекаются уроки, делаются выводы о необходимости изменения и улучшения организационных и технических

частей системы защиты информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана. Изменения в системе защиты информации, призванные предотвратить появление выявленного и расследованного инцидента информационной безопасности, должны быть осуществлены в кратчайшие сроки.

5. КЛАССИФИКАЦИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Инциденты ИБ по происхождению делятся на преднамеренные и случайные. Случайные инциденты могут быть вызваны антропогенными факторами (ошибка сотрудника, техническая неграмотность), социальными явлениями, природными явлениями, техногенными факторами (аварии, катастрофы).

5.2. Инциденты ИБ также можно разделить на инциденты, вызванные техническими средствами, и инциденты, вызванные нетехническими средствами.

5.3. В целом все инциденты безопасности можно разделить на следующие категории:

- вирусная атака (заражение элементов информационной системы вирусами, троянами, бэкдорами и прочим вредоносным программным обеспечением);
- попытки несанкционированного доступа к защищаемой информации;
- отказ в обслуживании (в результате программного или аппаратного сбоя, либо в результате целенаправленной или веерной атаки);
- нарушение сотрудниками Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана предписаний внутренних руководящих документов по защите информации (политик, инструкций, регламентов);
- нарушение технологического процесса обработки и защиты информации в информационной системе;
- потеря, утрата, компрометация машинных и иных носителей информации;
- нарушение конфиденциальности защищаемой информации;
- нарушение целостности защищаемой информации;
- сетевые атаки на информационную систему (как из-за пределов защищаемого периметра, так и внутри него);
- техногенная авария;
- нештатная ситуация.

5.4. Одним из широко распространенных видов инцидентов ИБ является инцидент типа «Отказ в обслуживании». Результатом такого инцидента является неспособность систем, сервисов или сетей продолжать функционирование с прежней производительностью. Часто это сопровождается полным отказом в доступе авторизованным пользователям. Инциденты типа «отказ в обслуживании» могут быть вызваны как техническими, так и нетехническими средствами. Инциденты типа «отказ в обслуживании», вызываемые техническими средствами можно категорировать на инциденты, направленные на уничтожение ресурсов, и на инциденты, направленные на истощение ресурсов. Типовыми примерами таких преднамеренных технических инцидентов ИБ являются:

- зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;
- передача данных в непредусмотренном формате в систему, сервис или сеть в попытке разрушить или нарушить их нормальную работу;
- одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать их ресурсы.

Инциденты ИБ типа «Отказ в обслуживании», создаваемые нетехническими средствами и приводящие к утрате информации, сервиса и (или) устройств обработки информации, могут вызываться, например, следующими факторами:

- нарушения систем физической защиты, приводящие к хищениям, преднамеренному нанесению ущерба или разрушению оборудования;
- случайное нанесение ущерба техническим средствам ИС и или месту их расположения от огня или воды;
- экстремальные условия окружающей среды, например высокая температура воздуха, вызванная выходом из строя системы кондиционирования воздуха;
- неправильной функционирование или перегрузка системы;
- неконтролируемые изменения в системе;
- неправильное функционирование программного и аппаратного обеспечения.

5.5. Инциденты ИБ типа «Сбор информации» подразумевают действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, работающих на идентифицированных целях атаки. Подобные инциденты ИБ предполагают проведение разведки с целью определения:

- наличия цели, получения представления об окружающей ее сетевой топологии;
- потенциальных уязвимостей цели или непосредственно окружающей ее сетевой среды, которые можно использовать для атаки.

Типичными примерами атак, направленных на сбор информации техническими средствами, являются:

- сбрасывание записей DNS;
- отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;
- зондирование системы с целью идентификации операционной системы хоста;
- сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов и версий программного обеспечения этих сервисов;
- сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов.

Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, приводят к:

- прямому или косвенному раскрытию или модификации информации;
- хищению интеллектуальной собственности;
- нарушению учетности, например, при регистрации учетных записей;
- неправильному использованию информационных систем (например, с нарушением закона или политики организации).

Инциденты могут вызываться, например, следующими факторами:

- нарушениями физической защиты, приводящими к несанкционированному доступу к информации и хищению устройств хранения данных, содержащих значимые данные, например ключи шифрования;
- неудачно и (или) неправильно сконфигурированными операционными системами по причине неконтролируемых изменений в системе или неправильным функционированием программного или аппаратного обеспечения, приводящим к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

5.6. Несанкционированный доступ как тип инцидента включает в себя инциденты, не вошедшие в первые два типа. Главным образом этот тип инцидентов состоит из несанкционированных попыток доступа в систему или неправильного использования

системы, сервиса или сети. Некоторые примеры несанкционированного доступа с помощью технических средств включают в себя:

- попытки извлечь файлы с паролями;
- атаки переполнения буфера с целью получения привилегированного доступа к сети;
- использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;
- попытки расширить привилегии доступа к ресурсам или информации по сравнению с легитимно имеющимися у пользователя.

5.7. Более подробное описание угроз безопасности ИС, а, следовательно, и возможности для возникновения инцидентов ИБ приводится в документе «Модель угроз безопасности информации».