Изображение выглядит как корона

Автоматически созданное описание

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

**Практическая работа №8**

по дисциплине «Управление информационной безопасностью»

Выполнил:

Феденёв А.В.

Проверил:

Пимонов Р.В.

Москва 2024

# Общие положения

* 1. Настоящий План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак в Федеральном государственном бюджетном учреждении «НМИЦ им. В.А. Алмазова» (далее – План Центра) разработан в соответствии с нормативными документами РФ и устанавливает организационные и технические мероприятия с целью подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак в Центре.
  2. Настоящий План Центра является частью комплекта организационно-распорядительной документации по вопросам информационной безопасности (защиты информации) Центра (далее – ОРД), и, в частности, обеспечению безопасности ЗО КИИ Центра.
  3. Процесс управления инцидентами ИБ включает:
* учет и регистрацию инцидентов ИБ;
* оповещение должностных лиц (работников), ответственных за выявление инцидентов ИБ и реагирование на них (далее – специалисты по безопасности);
* расследование обнаруженных инцидентов ИБ;
* устранение причин и последствий инцидентов ИБ;
* определение плана корректирующих и превентивных мероприятий.
  1. Ответственность за выявление инцидентов ИБ возлагается на лиц (работников), ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее – специалисты по безопасности), а в случае введения в Центре централизованной системы регистрации событий безопасности на освобожденное от иных обязанностей лицо (работника).
  2. Контроль над исполнением настоящего Плана осуществляет должностное лицо (работник), ответственное за обеспечение безопасности значимых объектов критической инфраструктуры (далее – ЗО КИИ).

# Технические характеристики и состав ЗО КИИ

Информация о технических характеристиках и составе ЗО КИИ Центра представлена в таблице 1.

Таблица 1. Технические характеристики и состав ЗО КИИ

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование объекта | Технические характеристики и состав ЗО КИИ |
| 1 | Центральный узел информационной системы обеспечения основной деятельности медицинской организации | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Центральный узел информационной системы обеспечения основной деятельности медицинской организации» от . .2018 г.,  утверждённом главным врачом. |
| 2 | Информационно- телекоммуникационная сеть связи «Технологическая сеть Центра | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Информационно- телекоммуникационная сеть связи медицинской организации  «Технологическая сеть  Центра от 2018  г., утверждённом главным врачом. |
| 3 | Автоматизированная система  «Шлюз подключения к ведомственной сети передачи данных Министерства здравоохранения | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Автоматизированная система  «Шлюз подключения к ведомственной сети передачи данных Министерства здравоохранения» от 2018 г.,  утверждённом главным врачом. |
| 4 | Информационная система  «Парус» | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Информационная система «Парус» от . .2018 г., утверждённом главным врачом. |
| 5 | Автономная автоматизированная система | Технические характеристики и состав представлены в документе «Описание |

|  |  |  |
| --- | --- | --- |
|  | (ультразвуковое оборудование)  «SonoAce R3 Samsung Medison» | объекта критической информационной инфраструктуры  «Автономная автоматизированная система (ультразвуковое оборудование) «SonoAce R3 Samsung Medison» от 2018 г.,  утверждённом главным врачом. |
| 6 | Автономная автоматизированная система (ультразвуковое оборудование)  «Sonoscape SSI-1000» | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Автономная автоматизированная система (ультразвуковое оборудование) «Sonoscape SSI-1000» от . .2018 г., утверждённом  главным врачом. |
| 7 | Автономная автоматизированная система (ультразвуковое оборудование)  «Sonoscape S20 PRO» | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Автономная автоматизированная система (ультразвуковое оборудование) «Sonoscape S20 PRO» от . .2018 г., утверждённом  главным врачом. |
| 8 | Автоматизированная система контроля за состоянием пациента «Аппарат для электроэнцефалографии Нейрон-Спектр-1» | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Автоматизированная система контроля за состоянием пациента  «Аппарат для  электроэнцефалографии Нейрон- Спектр-1» от . .2018 г.,  утверждённом главным врачом. |
| 9 | Радиологическая информационная система  «Флюорограф малодозовый цифровой сканирующий с рентгенозащитной кабиной ПроСкан 7000» | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Радиологическая информационная система «Флюорограф малодозовый цифровой сканирующий с рентгенозащитной кабиной ПроСкан  7000» от . .2018 г., утверждённом главным врачом. |

|  |  |  |
| --- | --- | --- |
| 10 | Радиологическая информационная система  «Кабинет флюорографический ПроСкан подвижной цифровой (КФПЦ) на базе шасси КАМАЗ» | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Радиологическая информационная система «Кабинет  флюорографический ПроСкан подвижной цифровой (КФПЦ) на базе шасси КАМАЗ» от . .2018 г.,  утверждённом главным врачом. |
| 11 | Автономная автоматизированная система  «Фетальный монитор  «СОНОМЕД-200 с  мультианализом КТГ» | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Автономная автоматизированная система «Фетальный монитор  «СОНОМЕД-200 с мультианализом КТГ» от . .2018 г., утверждённом  главным врачом. |
| 12 | Автономная автоматизированная система  «Офтальмологический бесконтактный тонометр Topcon CT-800» | Технические характеристики и состав представлены в документе «Описание объекта критической информационной инфраструктуры  «Автономная автоматизированная система «Офтальмологический бесконтактный тонометр Topcon CT- 800» от . .2018 г., утверждённом  главным врачом. |

# События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий.

а) Внедрение (заражение) вредоносного программного обеспечения. б) Распространение вредоносного программного обеспечения:

* использование контролируемого ресурса для распространения или управления модулями вредоносного программного обеспечения;
* попытки внедрения модулей вредоносного программного обеспечения.

в) Нарушение или замедление работы контролируемого информационного ресурса:

* компьютерная атака типа "отказ в обслуживании";
* распределенная компьютерная атака типа "отказ в обслуживании";
* несанкционированный вывод системы из строя;
* непреднамеренное отключение системы. г) Несанкционированный доступ в систему:
* успешная эксплуатация уязвимости;
* компрометация учетной записи.

д) Попытки НСД в систему или к информации:

* попытки эксплуатации уязвимости;
* попытки авторизации в информационном ресурсе.

е) Сбор сведений с использованием информационно- коммуникационных технологий:

* сканирование информационного ресурса;
* прослушивание (захват) сетевого трафика;
* социальная инженерия.

ж) Нарушение безопасности информации:

* несанкционированное разглашение информации.
* несанкционированное изменение информации.

з) Распространение информации с неприемлемым содержимым:

* рассылка незапрашиваемых электронных сообщений;
* публикация запрещенной законодательством РФ информации.

и) Мошенничество с использованием информационно- коммуникационных технологий:

* злоупотребление при использовании информационного ресурса;
* публикация мошеннического информационного ресурса.

к) Наличие уязвимости или недостатка конфигурации в информационном ресурсе.

# Мероприятия по реагированию на компьютерные инциденты

* + 1. **Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности**
       1. Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности (далее – механизмы РСБ) операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем, обеспечивающие:

а) автоматическую фиксацию в аппаратных (электронных) журналах событий безопасности;

б) автоматическое определение уровня опасности (критичности) события безопасности или присвоение событиям безопасности меток в ручном режиме;

в) сортировку и (или) группировку событий безопасности по заданным критериям в автоматическом и (или) ручном режиме;

г) автоматическую передачу записей о событиях безопасности в централизованную систему сбора и обработки событий безопасности и (или) экспорт записей событий безопасности в электронный файл;

* + - 1. В обязательном порядке должны регистрироваться следующие события безопасности:
* попытки входа (выхода) пользователей в операционную систему (из операционной системы);
* загрузка и инициализация операционной системы и ее программного останова для рабочих станций и серверов;
* попытка доступа к средствам виртуализации;
* факт изменения конфигурации средств виртуализации;
* запуск и остановка служб (системных сервисов) средств виртуализации;
* попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.
  + - 1. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:
* тип события;
* дата и время события;
* результат события;
* источник события;
* идентификатор пользователя информационной системы, предъявленный при попытке доступа.
  + - 1. Все данные регистрации событий безопасности должны анализироваться специалистом по безопасности на предмет выявления инцидентов ИБ, а также храниться не менее 30 (тридцати дней), для обеспечения возможности проведения анализа действий (тактики) злоумышленника, приведших к инциденту ИБ.
      2. В случае, если зафиксированный инцидент ИБ был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», специалист по безопасности обязан провести внеплановый анализ выявленного инцидента ИБ и, в случае необходимости, инициировать процедуру служебного расследования в соответствии с порядком, установленным в пункте 4.3. настоящего Плана Центра.

# Порядок реагирования на инциденты информационной безопасности

* + - 1. В случае выявления инцидента ИБ специалист по безопасности должен незамедлительно выполнить процедуру, предусмотренную п. 4.1.5 настоящего Плана Центра.
      2. При получении уведомления, предусмотренного п. 4.1.5 настоящего Плана Центра специалист по безопасности незамедлительно:

а) проводит анализ источника и способа реализации угрозы информационной безопасности;

б) определяет способы и средства противодействия;

в) осуществляет процедуры по блокированию источника, в том числе способом отключения атакуемых компонентов ЗО КИИ, а в случае невозможности такого блокирования, по ограничению области воздействия на ЗО КИИ и тяжести последствий (объема утраченной или раскрытой информации);

г) определяет необходимость привлечения к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак подразделений и должностных лиц ФСБ России и(или) отдельных экспертов, осуществляющих деятельность в этой области;

д) сообщает Главному врачу Центра о принятых мерах и полученном в ходе инцидента ИБ ущербе;

е) передает сведения в ГосСОПКА в соответствии с положениями документа "Порядок взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

* + - 1. Специалист по безопасности инициирует процедуры проведения расследования инцидента ИБ.

# Порядок расследования обнаруженных инцидентов информационной безопасности

* + - 1. Проведение служебного расследования инициируется приказом Главного врача Центра, или лицом (работником). В этом же приказе указываются члены постоянно действующей комиссии (далее – Комиссии) для проведения служебного расследования.
      2. Служебное расследование может быть возбуждено:
* по инициативе лица (работника), ответственного за обеспечение безопасности ЗО КИИ в Центре;
* по инициативе любого работника Центра на основании служебной записки в произвольной форме на имя лица (работника), ответственного за обеспечение безопасности ЗО КИИ в Центре;
  + - 1. Комиссия для проведения служебного расследования в рабочем порядке в максимально короткие сроки, привлекая все необходимые ресурсы, проводит служебное расследование.
      2. Результаты работы Комиссии оформляются в виде аналитического экспертного заключения на имя Главного врача, с предложениями:
* по внесению изменений в организационные и (или) технические меры по обеспечению безопасности ЗО КИИ;
* по внесению изменений и улучшений в комплект организационно- распорядительной документации Центра по вопросам обеспечения безопасности ЗО КИИ;
* по расширению или дополнению списка инцидентов ИБ, установленного данным Планом Центра, если это необходимо.
  + - 1. В аналитическом экспертном заключении должен быть приведен перечень ответственных за выполнение запланированных работ и сроки выполнения запланированных работ.
      2. Материалы служебного расследования, его выводы и заключения могут быть использованы как основание для реализации уголовной, гражданской, административной или дисциплинарной ответственности, в порядке, определяемом действующим законодательством и локальными правовыми актами Центра.

# Меры по ликвидации последствий от компьютерных атак

Перед принятием мер по ликвидации последствий компьютерных атак Центра определяет:

а) состав подразделений и должностных лиц Центра, ответственных за проведение

мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак, и их задачи в рамках принимаемых мер;

б) перечень средств (организационных/технических), необходимых для принятия мер по ликвидации последствий компьютерных атак;

Информация о компьютерном инциденте, связанном с функционированием ЗО КИИ, направляется Центром в НКЦКИ в срок не позднее 3 часов с момента обнаружения компьютерного инцидента.

Информация о компьютерном инциденте, связанном с функционированием иных ОКИИ, направляется Центром в НКЦКИ в срок не позднее 24 часов с момента обнаружения компьютерного инцидента.

Таблица 2. Меры по ликвидации последствий от компьютерных атак.

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование события/условия, при которых реализуются мероприятия настоящего Плана Центра** | **Организационные/технические меры** | **Подразделения и (или) должностные лица,**  **ответственные за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий**  **компьютерных атак** |
| 1 | Внедрение (заражение) вредоносного программного обеспечения. | Стадии защиты от вредоносного ПО:  1. **Предотвращение** (профилактика) – знание обо всех изменениях сетей и компьютерных систем, поддержание их актуальности. Дополнительно:   * Ограничение физического доступа к производственным системам обработки данных и в особенности к системам |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | резервного копирования и восстановления;   * ограничение доступа к сети путем установки брандмауэров и минимизации использования портов; * развертывание системы авторизации пользователей и управления доступом на основе ролей; * фильтрация URL и адресов электронной почты; * отработка процедур ликвидации последствий атак; * обучение пользователей основам безопасности.   2. **Обнаружение** – быстрое реагирование на события безопасности. Реализация следующих мер:   * Защита пользовательских конечных систем; * антивирусная защита (Dr.Web, Kaspersky Anti-Virus); * обнаружение вторжений (Secret Net Studio, Dallas Lock, ViPNet IDS, UserGate); * обнаружение известных вредоносных программ; * мониторинг сетевых портов; * централизованное ведение журналов для сопоставления событий;   3. Ликвидация последствий – быстрое и надежное восстановление.  Зараженные системы необходимо немедленно изолировать, затем ликвидировать угрозу, далее восстановить работоспособность систем (программное обеспечение для резервного копирования и восстановления данных).  **Примечание**. Acronis, Dell (EMC Avamar), HP Data Protector. |  |
| 2 | Распространение | 2. **Обнаружение** – быстрое реагирование на события |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | вредоносного программного обеспечения:   * использование контролируемого ресурса для   распространения или управления модулями вредоносного программного обеспечения;   * попытки внедрения модулей вредоносного программного обеспечения. | безопасности. Реализация следующих мер:   * Защита пользовательских конечных систем; * антивирусная защита (Dr.Web, Kaspersky Anti-Virus); * обнаружение вторжений (Secret Net Studio, Dallas Lock, ViPNet IDS, UserGate); * обнаружение известных вредоносных программ; * мониторинг сетевых портов; * централизованное ведение журналов для сопоставления событий;   3. Ликвидация последствий – быстрое и надежное восстановление.  Зараженные системы необходимо немедленно изолировать, затем ликвидировать угрозу, далее восстановить работоспособность систем (программное обеспечение для резервного копирования и восстановления данных).  **Примечание**. Acronis, Dell (EMC Avamar), HP Data Protector. |  |
| 3 | Нарушение или замедление работы контролируемого информационного ресурса:   * компьютерная атака типа "отказ в обслуживании"; * распределенная компьютерная атака | Стадии защиты от вредоносного ПО:  1. **Предотвращение** (профилактика) – знание обо всех изменениях сетей и компьютерных систем, поддержание их актуальности. Дополнительно:   * Ограничение физического доступа к производственным системам обработки данных и в особенности к системам резервного копирования и восстановления; * ограничение доступа к сети путем установки брандмауэров и минимизации использования портов; * развертывание системы авторизации пользователей и |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | типа "отказ в обслуживании";  -  несанкционированный вывод системы из строя;  - непреднамеренное отключение системы. | управления доступом на основе ролей;   * фильтрация URL и адресов электронной почты; * отработка процедур ликвидации последствий атак; * обучение пользователей основам безопасности. Примечание. АПКШ «Континент»   2. **Обнаружение** – быстрое реагирование на события безопасности. Реализация следующих мер:   * Защита пользовательских конечных систем; * антивирусная защита (Dr.Web, Kaspersky Anti-Virus); * обнаружение вторжений (Secret Net Studio, Dallas Lock, ViPNet IDS, UserGate); * обнаружение известных вредоносных программ; * мониторинг сетевых портов; * централизованное ведение журналов для сопоставления событий;   3. Ликвидация последствий – быстрое и надежное восстановление.  Зараженные системы необходимо немедленно изолировать, затем ликвидировать угрозу, далее восстановить работоспособность систем (программное обеспечение для резервного копирования и восстановления данных).  **Примечание**. Acronis, Dell (EMC Avamar), HP Data Protector. |  |
| 4 | Несанкционированны й доступ в систему:  - успешная  эксплуатация | Меры защиты компьютерных систем:  1. **Аутентификация пользователей**. Выполнение процедуры входа в систему, использование уникальных паролей, не являющихся комбинациями личных данных |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | уязвимости;  - компрометация учетной записи. | пользователей.  2. **Защита пароля. Правила**:   * запрет на распространение сведений о пароле; * сложный пароль, состоящий из следующей комбинации:   + минимальная длина – 8 символов;   + использование букв верхнего и нижнего регистра (чувствительность к регистру)   + включение одной или нескольких цифр   + включение специальных символов, таких как @, #, $ * запрет слов, найденных в черном списке паролей (Пароль1, Qwerty123, или Qaz123wsx и т.д.) * запрет слов, содержащихся в личной информации пользователя * запрет на использование названия компании или аббревиатуры * запрет паролей, совпадающих с форматом даты, номерами машин, телефонными номерами, адресом, псевдонимом, именем родственника или другими распространенными значениями; * снижение отражательных характеристик при вводе пароля (вывод символов на экран в виде звездочек \*); * не хранить пароли на бумаге; * периодическая смена пароля – каждые 90/180 дней; * назначение пароля для каждого сотрудника индивидуально; * смена пароля после увольнения сотрудника. * уничтожение данных компрометированной учетной записи. |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | 3. **Обнаружение** – быстрое реагирование на события безопасности. Реализация следующих мер:   * Защита пользовательских конечных систем; * антивирусная защита (Dr.Web, Kaspersky Anti-Virus); * обнаружение вторжений (Secret Net Studio, Dallas Lock, ViPNet IDS, UserGate); * обнаружение известных вредоносных программ; * мониторинг сетевых портов; * централизованное ведение журналов для сопоставления событий;   4. **Ликвидация последствий** – быстрое и надежное восстановление.  Зараженные системы необходимо немедленно изолировать, затем ликвидировать угрозу, далее восстановить работоспособность систем (программное обеспечение для резервного копирования и восстановления данных).  Примечание. Acronis, Dell (EMC Avamar), HP Data  Protector. |  |
| 5 | Попытки НСД в систему или к информации:   * попытки   эксплуатации уязвимости;   * попытки   авторизации в информационном | Стадии защиты от вредоносного ПО:  1. **Предотвращение** (профилактика) – знание обо всех изменениях сетей и компьютерных систем, поддержание их актуальности. Дополнительно:   * Ограничение физического доступа к производственным системам обработки данных и в особенности к системам резервного копирования и восстановления; * ограничение доступа к сети путем установки брандмауэров и минимизации использования портов; |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | ресурсе. | * развертывание системы авторизации пользователей и управления доступом на основе ролей; * фильтрация URL и адресов электронной почты; * отработка процедур ликвидации последствий атак; * обучение пользователей основам безопасности. Примечание. АПКШ «Континент»   2. **Обнаружение** – быстрое реагирование на события безопасности. Реализация следующих мер:   * Защита пользовательских конечных систем; * антивирусная защита (Dr.Web, Kaspersky Anti-Virus); * обнаружение вторжений (Secret Net Studio, Dallas Lock, ViPNet IDS, UserGate); * обнаружение известных вредоносных программ; * мониторинг сетевых портов; * централизованное ведение журналов для сопоставления событий;   3. Ликвидация последствий – быстрое и надежное восстановление.  Зараженные системы необходимо немедленно изолировать, затем ликвидировать угрозу, далее восстановить работоспособность систем (программное обеспечение для резервного копирования и восстановления данных).  **Примечание**. Acronis, Dell (EMC Avamar), HP Data Protector. |  |
| 6 | Сбор сведений с  использованием информационно- | Стадии защиты от вредоносного ПО:  1. **Предотвращение** (профилактика) – знание обо всех изменениях сетей и компьютерных систем, поддержание |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | коммуникационных технологий:   * сканирование информационного ресурса; * прослушивание (захват) сетевого трафика; * социальная инженерия. | их актуальности. Дополнительно:   * Ограничение физического доступа к производственным системам обработки данных и в особенности к системам резервного копирования и восстановления; * ограничение доступа к сети путем установки брандмауэров и минимизации использования портов; * развертывание системы авторизации пользователей и управления доступом на основе ролей; * фильтрация URL и адресов электронной почты; * отработка процедур ликвидации последствий атак; * обучение пользователей основам безопасности. Примечание. АПКШ «Континент»   2. **Обнаружение** – быстрое реагирование на события безопасности. Реализация следующих мер:   * Защита пользовательских конечных систем; * антивирусная защита (Dr.Web, Kaspersky Anti-Virus); * обнаружение вторжений (Secret Net Studio, Dallas Lock, ViPNet IDS, UserGate); * обнаружение известных вредоносных программ; * мониторинг сетевых портов; * централизованное ведение журналов для сопоставления событий;   3. Ликвидация последствий – быстрое и надежное восстановление.  Зараженные системы необходимо немедленно изолировать, затем ликвидировать угрозу, далее восстановить работоспособность систем (программное обеспечение для резервного копирования и восстановления |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | данных).  **Примечание**. Acronis, Dell (EMC Avamar), HP Data Protector.  4. Осуществление работ по обучению сотрудников,  информирования о методах, возможностях социальной инженерии. |  |
| 7 | Нарушение | Основные составляющие системы предотвращения утечки |  |
|  | безопасности | защищаемой информации: |
|  | информации: | 1. **Работа с персоналом**. |
|  | - | Выполнение требований безопасности, повышение |
|  | несанкционированное | осведомленности сотрудников и применение мер |
|  | разглашение | пресечения к нарушителям (назначить ответственного за |
|  | информации. | обеспечение безопасности ЗОКИИ, ознакомление |
|  | - | сотрудников и контроль над выполнением требований |
|  | несанкционированное | Законодательства РФ, локальных нормативно-правовых |
|  | изменение | актов БУЗОО «Нововаршавская ЦРБ», подписание |
|  | информации. | соглашение о неразглашении конфиденциальной |
| 8 | Распространение | информации, отражение требований к сотруднику к |  |
|  | информации с | трудовых соглашениях). |
|  | неприемлемым | 2. **Повышение осведомленности**. |
|  | содержимым: | Обучение и контроль знаний пользователей по следующим |
|  | - рассылка | вопросам: |
|  | незапрашиваемых | * правила политики безопасности организации; |
|  | электронных | * правила выбора, смены и использования паролей; |
|  | сообщений; | * правила получения доступа к ресурсам информационной |
|  | - публикация | системы; |
|  | запрещенной | * правила обращения с конфиденциальной информацией; |
|  | законодательством РФ | * процедуры информирования об инцидентах, уязвимостях, |

|  |  |  |  |
| --- | --- | --- | --- |
|  | информации. | ошибках и сбоях программного обеспечения и др. (далее – Организационно-распорядительная документация (ОРД) БУЗОО «Нововаршавская ЦРБ»).   1. **Дисциплинарный процесс** в отношении нарушителей безопасности, предусматривающий расследование, ликвидацию последствий инцидентов и адекватные меры воздействия 2. Осуществление работ по обучению сотрудников, информирования о методах, возможностях социальной инженерии. |  |
| 9 | Мошенничество с использованием информационно- коммуникационных технологий:   * злоупотребление при использовании информационного ресурса; * публикация мошеннического информационного ресурса. |  |
| 10 | Наличие уязвимости или недостатка конфигурации в информационном ресурсе. | Стадии защиты от вредоносного ПО:  1. **Предотвращение** (профилактика) – знание обо всех изменениях сетей и компьютерных систем, поддержание их актуальности. Дополнительно:   * Ограничение физического доступа к производственным системам обработки данных и в особенности к системам резервного копирования и восстановления; * ограничение доступа к сети путем установки брандмауэров и минимизации использования портов; * развертывание системы авторизации пользователей и управления доступом на основе ролей; * фильтрация URL и адресов электронной почты; * отработка процедур ликвидации последствий атак; * обучение пользователей основам безопасности. |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Примечание. АПКШ «Континент»  2. **Обнаружение** – быстрое реагирование на события безопасности. Реализация следующих мер:   * Защита пользовательских конечных систем; * антивирусная защита (Dr.Web, Kaspersky Anti-Virus); * обнаружение вторжений (Secret Net Studio, Dallas Lock, ViPNet IDS, UserGate); * обнаружение известных вредоносных программ; * мониторинг сетевых портов; * централизованное ведение журналов для сопоставления событий;   3. Ликвидация последствий – быстрое и надежное восстановление.  Зараженные системы необходимо немедленно изолировать, затем ликвидировать угрозу, далее восстановить работоспособность систем (программное обеспечение для резервного копирования и восстановления данных).  **Примечание**. Acronis, Dell (EMC Avamar), HP Data Protector. |  |

# Устранение причин и последствий инцидентов информационной безопасности

* + 1. Для инициирования работ по устранению причин и последствий инцидентов ИБ лицо (работник), ответственное за обеспечение безопасности ЗО КИИ в Центре, направляет аналитическое экспертное заключение по электронной почте главному врачу Центра и ответственным за выполнение запланированных работ.
    2. Если ответственный за выполнение запланированных работ не согласен с установленными сроками, он вправе обратиться к лицу (работнику), ответственному за обеспечение безопасности ЗО КИИ в Центре, с просьбой перенести срок с обоснованием причин переноса.
    3. При изменении сроков реализации действий, лицо (работник), ответственное за обеспечение безопасности ЗО КИИ в Центре, вносит необходимые изменения в экспертное заключение и информирует о них по электронной почте ответственного за выполнение запланированных работ и главного врача Центра.
    4. После реализации запланированных работ ответственное лицо должно направить по электронной почте лицу (работнику), ответственному за обеспечение безопасности ЗО КИИ в Центре, подтверждение выполнения работ, не позднее срока реализации, установленного в экспертном заключении.
    5. Лицо (работник), ответственное за обеспечение безопасности ЗО КИИ в Центре, вправе запросить у назначенного лица информацию о выполнении в случае, если ему не поступило подтверждение выполнения работ в течение 2 (двух) рабочих дней с даты, установленной в экспертном заключении.
    6. Оценку результативности предпринятых мер осуществляет лицо (работник), ответственное за обеспечение безопасности ЗО КИИ в Центре, ежемесячно на основании анализа информации, содержащейся в отчетах о проведении служебного расследования и в сводном отчете об инцидентах ИБ.
    7. О результативности предпринятых корректирующих и превентивных мер свидетельствует отсутствие повторных инцидентов ИБ.

# Ответственность

* + 1. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет лицо (работник), ответственное за обеспечение безопасности ЗО КИИ в Центре.
    2. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет специалист по безопасности, назначенный главным врачом Центра.
    3. Ответственность за выделение требуемых ресурсов (в том числе финансовых и трудовых) для реализации положений настоящего документа несет заместитель главного врача Центра, ответственный за вопросы разработки, принятия и внедрения мер защиты информации.