РОССИЙСКАЯ ФЕДЕРАЦИЯ
БЕЛГОРОДСКАЯ ОБЛАСТЬ
АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА
«КРАСНОЯРУЖСКИЙ РАЙОН»

РАСПОРЯЖЕНИЕ

«17» 12.2024 года № 793

Об утверждении порядков действий по обеспечению безопасности и технической защиты информации в администрации Краснояружского района

В соответствии с письмом Федеральной службы по техническому и экспортному контролю России от 1 июля 2024 года № 2393/1 «О применении методического документа, утверждённого ФСТЭК России»:

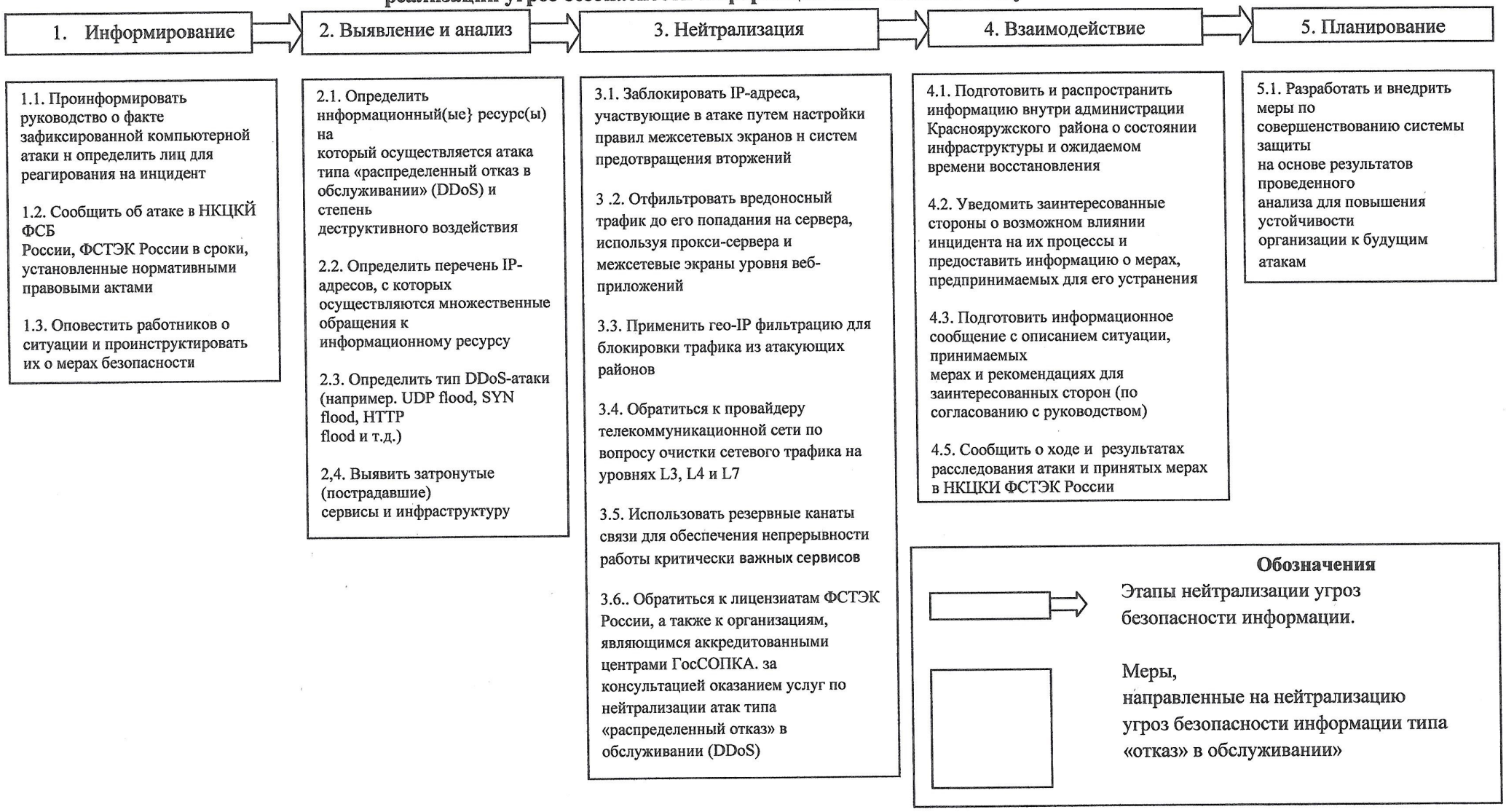
1. Утвердить порядки действий по обеспечению безопасности и технической защиты информации в администрации Краснояружского района (прилагаются).
2. Контроль за исполнением распоряжения возложить на заместителя главы администрации района - руководителя аппарата главы администрации района Носова М.В.

Глава администрации Краснояружского района **А.Е. Миськов**

Администрация Краснояружского района Белгородской области
Управление делами

Утвержден
распоряжением администрации
Краснояружского района
от «17» 12 2024 года
№793

Порядок действий по обеспечению безопасности и технической защиты информации в администрации Краснояружского района при реализации угроз безопасности информации типа «отказ в обслуживании»



Порядок действий по обеспечению безопасности и технической защиты информации в администрации Краснояружского района при реализации угроз безопасности информации, связанных с несанкционированным доступом к защищаемой информации

1.Информирование

1.1.Проинформировать руководство о факте зафиксированной компьютерной атаки н определить лиц для реагирования на инцидент

1.2. Сообщить об атаке в НКЦКЙ ФСБ России, ФСТЭК России в сроки, установленные нормативными правовыми актами

1.3. Оповестить работников о ситуации и проинструктировать их о мерах безопасности

2. Выявление и анализ

2.1. Оценить масштаб и критичность утечки данных, определить, к каким данным был получен несанкционированный доступ

2.2. Задокументировать все детали инцидента, включая время, обстоятельства атаки и предполагаемые цели злоумышленников

2.3. Использовать антивирусное программное обеспечение для выявления ВПО, а также признаков осуществления несанкционированного доступа

2.4. Перед удалением ВПО из зараженных систем сохранить образцы вредоносного кода или других данных, для дальнейшего анализа и расследования. Эти образны должны быть изолированы и храниться в безопасной среде

2.5. Сохранить журналы событий (сетевые логи, дампы памяти, снимки экрана и другие данные), которые могут быть полезны для расследования. Убедится, что данные защищены от изменений и доступны для последующего анализа

3. Нейтрализация

3.1. Отключить затронутые системы от сетевых соединений, чтобы предотвратить дальнейшее распространение вредоносной активности и защитить остальные сегменты сети

3.2. Перевести все пораженные ресурсы в режим технологического обслуживания, чтобы провести диагностику и восстановление без риска для пользователей и данных

3.3. Изменить пароли всех | учетных записей.. Убедится, что все старые сессии были завершены, чтобы предотвратить доступ по устаревшим учетным данным

3.4. Провести полную проверку всех систем и данных с использованием актуальных антивирусных баз для обнаружения и удаления возможных вредоносных программ.

3.5. Провести проверку всех учетных записей на предмет выявления и удаления несанкционированных или скомпрометированных учетных записей, а также учетных записей, для которых осуществлялось повышение привилегий

4. Взаимодействие

4.1. В случае невозможности удаления ВПО восстановить операционные системы и данные из последних безопасных резервных копий, проверенных на отсутствие вредоносной активности

4.2. При невозможности восстановления данных из резервных копий рассмотреть возможность привлечения организации лицензиатов ФСТЭК России или производителей средств антивирусной зашиты для восстановления информационной инфраструктуры и данных

4.3 Обновить все программное обеспечение и установить последние обновления безопасности для всех программных компонентов предварительно протестировав их работоспособность и совместимость

5. Взаимодействие

5.1. Не платить выкуп вымогателям, так как это не гарантирует безопасность данных и способствует дальнейшей преступной деятельности

5.2 Обратиться к лицензиатам ФСТЭК России, а также к организациям, являющимся аккредитованными центрами ГосСОПКА за консультацией и оказанием услуг по расследованию инцидента

4.3. Сообщите о ходе н результатах расследования атаки и принятых мерах в НКЦКИ ФСТЭК России, Роскомнадзор (в случае утечки ПДн)

6. Планирование

6.1. Разработать и внедрить меры по совершенствованию системы зашиты на основе результатов проведенного анализа для повышения устойчивости организации к к актуальным угрозам безопасности

Порядок действии во обеспечению безопасности
и технической защиты информации в администрации Краснояружского района при реализации
угроз безопасности информации, связанных с внедрением нежелательного контента на информационном ресурсе

1.Информирование

1.1.Проинформировать руководство о факте зафиксированной компьютерной атаки н определить лиц для реагирования на инцидент

1.2. Сообщить об атаке в НКЦКЙ ФСБ России, ФСТЭК России в сроки, установленные нормативными правовыми актами

1.3. Оповестить работников о ситуации и проинструктировать их о мерах безопасности

2. Выявление и анализ

2 1. Проанализировать фанзы и базы данных для определения внесенных изменений

2.2. Проанализировать журналы Событий веб-сервера и систем для
выявления источника методов проникновения

2.3. Проверить внешнюю инфраструктуру, плагины, темы, счетчики и другие компоненты веб-ресурсов на наличие известных
уязвимостей

2.4. Использовать антивирусное программное обеспечение для выявления ВПО

2.5.. Задокументировать все детали
инцидента. включая время, обстоятельства атаки и предполагаемые щели злоумышленников

2.6. Перед удалением ВПО из зараженных систем сохранить образны вредоносного кода или других данных, для дальнейшего анализа и расследования.. Эти образцы должны быть изолированы и храниться в безопасной среде

2.7. Сохранить журналы событии (сетевые логи, дампы памяти, снимки экрана и другие данные), которые могут быть полезны для расследования. Убедитесь, что данные защищены от изменений и доступны для последующего анализа.

3. Нейтрализация

3.1. Отключить затронутые системы от сетевых соединений, чтобы предотвратить дальнейшее распространение вредоносной Активности и защитить остальные сегменты сети

3.2. Перевести все пораженные ресурсы в режим технологического обслуживания, чтобы провести диагностику к восстановление без риска для пользователей и данных

3.3. Заблокировать все внешние соединения для предотвращения дальнейших попыток.

3.4. Немедленно изменить пароли всех учетных записей. Убедится. что все старые сессии были завершены, чтобы предотвратить доступ по устаревшим учетным данным.

3.5. Провести проверку всех учетных записей на предмет выявления и удаления несанкционированных или скомпрометированных аккаунтов, а также учетных записей, для которых осуществлялось повышение привилегий

3.6. Проверить все смежные ресурсы на предмет аналогичных атак, даже если они не были непосредственно затронуты

3.7. Провести полную проверку всех систем и данных с использованием актуальных антивирусных баз для обнаружения и удаления возможных вредоносных программ

4. Взаимодействие

4.1. В случае невозможности удаления ВПО восстановить операционные системы а данные
из последних безопасных резервных копий, проверенных на отсутствие вредоносной активности

4.2. При невозможности восстановления данных из резервных копий рассмотреть возможность привлечения организации лицензиатов из перечня рекомендованных ФСГЭК
России ила поставщика антивирусного средства зашиты
для: восстановления работоспособности информационного ресурса

4.3. Обновить все программное
обеспечение и установит последние обновления безопасности для всех программных компонентов

5. Взаимодействие

5.1. Подготовить и распространить информацию внутри администрации о состоянии инфраструктуры и ожидаемом времени восстановления

5.2. Обратиться к лицензиатам ФСТЭК России, а также к организациям, являющимся аккредитованными центрами ГосСОПКА, за консультацией и оказанием услуг по расследованию

5.3. У:ведомить заинтересованные стороны о возможном влиянии инцидента на их процессы и предоставить информацию о мерах, предпринимаемых для его устранения

5.4. Подготовить информационное сообщение с описанием ситуации, принимаемых
мерах и рекомендациях для заинтересованных сторон (по согласованию с руководством)

5.6. Сообщите о ходе и результатах расследования атаки и принятых мерах в НКЦКИ, ФСТЭК России

6. Планирование

6.1. Разработать и внедрить меры по совершенствованию системы зашиты на основе результатов проведенного анализа для повышения устойчивости организации *к*

Порядок действий по обеспечению безопасности и технической защиты информации в администрации Краснояружского района при реализации угроз безопасности информации, связанных с внедрением вирусов шифровальщиков

1.Информирование

1.1. Проинформировать руководство о факте зафиксированной компьютерной атаки н определить лиц для реагирования на инцидент

1.2. Сообщить об атаке в НКЦКЙ ФСБ России, ФСТЭК России в сроки, установленные нормативными правовыми актами

1.3. Оповестить работников о ситуации и проинструктировать их о мерах безопасности

2.Выявление и анализ

2.1. Выявить зараженные элементы информационной инфраструктуры (ПК, серверы, сегменты сети), а также затронутые данные.

2.2. Задокументировать все детали инцидента, включая время, обстоятельства атаки и предполагаемые цели злоумышников.

2.3. Перед удалением ВПО из зараженных систем сохранить образцы вредоносного кода или других данных для дальнейшего анализы и расследования. Эти образцы должны быть изолированы и храниться в безопасной среде.

2.4. Сохранить журналы событий (сетевые логии, дампы памяти, снимки экрана и другие данные), которые могут быть полезны для расследования. Убедиться, что данные защищены для последующего анализа.

2.5.Осуществлять непрерывный мониторинг изолированных сегментов сети на предмет новых –заражений

3.Нейтрализация

3.1. Отключать затронутые системы от сетевых соединений, чтобы предотвратить дальнейшее распространение вредоносной активности и защитить остальные сегменты сети.

3.2.Запретить подключение внешних машинных носителей информации к зараженным персональным компьютерам, серверам и сегментам сети органа.

3.3. Настроить межсетевые экраны для блокировки вредоносного трафика.

3.4. Перевести все пораженные ресурсы в режим технологического обслуживания, чтобы провести диагностику и восстановление без риска для пользовательских данных.

3.5.Идентифицировать и остановить процессы и службы, которые не должны быть активными в нормальных условиях или вызывают подозрения.

3.6.Изменить пароли всех учетных записей. Убедиться, что все старые сессии были завершены, чтобы предотвратить доступ по устаревшим данным.

3.7.Провести анализ подозрительных процессов служб для подтверждения их вредоносной активности.

3.8. Провести средствами антивирусной защиты полную проверку всех систем и данных с использованием актуальных антивирусных баз для обнаружения и удаления возможных вредоносных программ.

3.9. Удалить ВПО с зараженных систем, а также все вредоносные процессы, службы связанные с ними файлы.

4.Восстановление

4.1. В случае невозможности удаления ВПО восстановить операционные системы и данные из последних безопасных резервных копий проверенных на отсутствие вредоносной активности

4.2. При невозможности восстановления данных из резервных копий рассмотреть возможность привлечения организации лицензиатов ФСТЭК России или производителей средств антивирусной защиты для восстановления зашифрованных данных.

4.3. Обновить все программное обеспечение и установить последние обновления безопасности для всех программных компонентов предварительно протестировав их работоспособность и совместимость.

5.Взаимодействие

5.1. Подготовить и распространить информацию внутри администрации о состоянии инфраструктуры и ожидаемом времени восстановления.

5.2.не платить выкуп вымогателям так как это не гарантирует безопасность данных и способствует дальнейшей преступной деятельности.

5.3. Уведомить заинтересованные стороны о возможном влиянии инцидента на их процессы и предоставить информацию о мерах, предпринимаемых для его устранения.

5.4. Подготовить информационное сообщение с описанием ситуации, принимаемых мерах и рекомендациях для заинтересованных сторон (по согласованию с руководителем)

5.5. Обратиться при необходимости к лицензиатам ФСТЭК России, а также к организациям являющимися аккредитованными центрами ГосСОПКА, за консультацией и оказанием услуг расследованию инцидента.

6.Планирование

6.1. Разработать и внедрить меры по совершенствованию системы защиты на основе результатов проведенного анализа для повышения устойчивости организации к будущим атакам.