РОССИЙСКАЯ ФЕДЕРАЦИЯ БЕЛГОРОДСКАЯ ОБЛАСТЬ

АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА «ИВНЯНСКИЙ РАЙОН» РАСПОРЯЖЕНИЕ

Посёлок Ивня

I9 декабря 2024 г.

_№ 763-p

Об утверждении Порядка действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации

В соответствии с письмом ФСТЭК России от 1 июля 2024 года № 2393/1 «О применении методического документа, утверждённого ФСТЭК России», в целях повышения уровня безопасности в области защиты информации администрации Ивнянского района и координации работ в данной сфере:

- 1. Утвердить Порядок действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации (прилагается).
- 2. Контроль за исполнением распоряжения возложить на заместителя главы администрации Ивнянского района руководителя аппарата главы администрации Ивнянского района Позднякову Н.А.

Исполняющий обязанности главы администрации Ивнянского района

ANS ANSWERS OF STATE OF STATE

Л.А. Родионова

Приложение

УТВЕРЖДЕН распоряжением администрации Ивнянского района от «<u>19</u>» де набря 2024 г. № 763-р

Порядок

действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации

- 1. Порядок действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в администрации Ивнянского района и подведомственных учреждениях при реализации угроз безопасности информации, связанных с внедрением вирусов-шифровальщиков.
- 2. Порядок действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в администрации Ивнянского района и подведомственных учреждениях при реализации угроз безопасности информации, связанных с внедрением нежелательного контента на информационном ресурсе.
- 3. Порядок действий по обеспечению безопасности объектов критической инфраструктуры технической информации информационной И защиты в администрации Ивнянского района и подведомственных учреждениях безопасности реализации угроз информации, при связанных с несанкционированным доступом к защищаемой информации.
- 4. Порядок действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в администрации Ивнянского района и подведомственных учреждениях при реализации угроз безопасности информации типа «отказ в обслуживании».

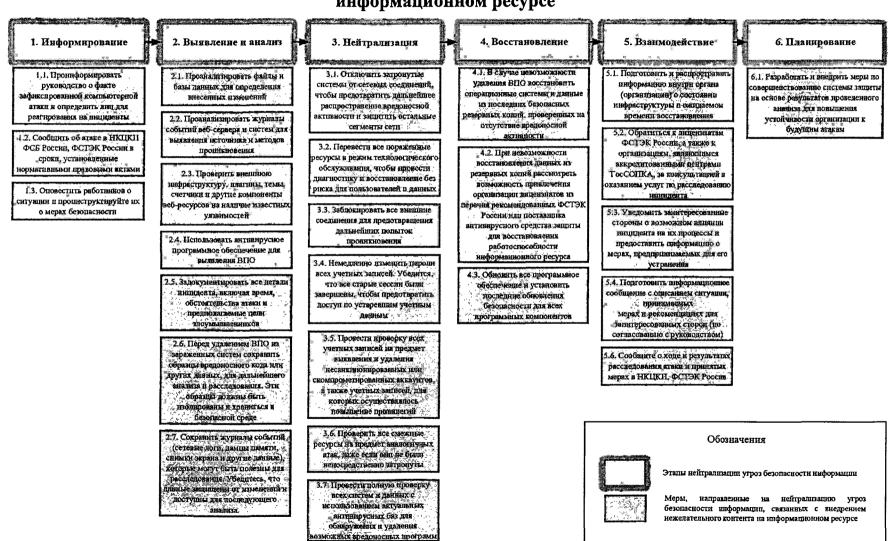
1. Порядок действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в администрации Ивнянского района и подведомственных учреждениях

при реализации угроз безопасности информации, связанных с внедрением вирусов-шифровальщиков 1. Информирование 5. Взанмодействие 6. Планирование .4. Восстановление 2. Выявление и анализ 3. Нейтрализация 2.1. Выявить зараженные элементы 3.1. Отключить затронутые системы 4.1. В случае невозможности 5.1. Подготовить и распространить 1.1. Проинформировать 6.1. Разработать и внедрить меры удаления ВПО восстановить пиформационной инфраструктуры от сетевых соединений, чтобы информацию внутри органа по совершенствованию системы руководство органа (организации) о (персональные компьютеры. предотвратить дальнейщее перационные системы и данные из (организации) о состоянии защиты на основе результатов факте зафиксированной сервера, сегменты сети) органа распространение вредоносной последних безопасных резервных проведенного анализа для компьютерной атаки и определить инфраструктуры и ожидаемом активности и защитить остальные организации), а также затронутые копнії, проверенных на отсутствие времени восстановления повышения устойчивости лиц для реагирования на инцидент вредоносной активности панные. сегменты сетп организации к будущим атакам 1.2. Сообщить об атаке в НКЦКИ 3.2. Запретить полключение 4.2. При невозможности Не платить выкуп вымогателям 2.2. Залокументировать все детали ФСБ России, ФСТЭК России в так как это не гарантирует внешних манинных носителей восстановления данных из инцидента, включая время, сроки, установленные безопасность данных и информации к зараженным резервных коний рассмотреть обстоятельства атаки й нормативными правовыми актами способствует дальнейшей персональным компьютерам, возможность привлечения предполагаемые целії преступной деятельности. серверам и сегментам сети органа организации дицензиатов ФСТЭК злоумыниленник**ов** 1.3. Оповестить работников органа (пипвенначии) оссии или производителей средств (организации) о ситуации и антивирусной защиты для Уведомить заинтересованные 2.3. Перед удалением ВПО из проинструктировать их о мерах 3.3. Настроить межсетёвые экраны восстановления защифрованных стороны о возможном влиянии зараженных систем сохранить: безопасности для блокировки вредоносного данных пицидента на их процессы п ображцы вредоносного кода или трафика предоставить пиформацию о мерах, пругих данных, для дальнейшего 4.3. Обновить все программное предпринимаемых для его анализа и расследования. Эти обеспечение и установить 3.4. Перевести все пораженные устранения образны должны быть изолированы последние обновления есурсы в режим технологического и храниться в безопасной среде безопасности пля всех 5.4. Подготовить информационное обслуживания, чтобы провести программных компонентов циагностику и восстановление без сообщение с описанием ситуации. 2.4. Сохранить журналы событий предварительно протестировав их риска для пользователей и данных принимаемых мерах и (сетевые логи, дампы памяти. работоспособность и рекомендациях для силмки экрана и другие данные), совместимость заинтересованных сторон (по 3.5. Идентифицировать и которые могут быть полезны для согласованию с руководством) остановить процессы и службы, расследования. Убедиться, что котооые не должны быть[»] данные запипцены от изменений и ктивными в вормальных условнях 5. Обратиться при необходямости доступны для последующего к лицензиатам ФСТЭК России, а анализа или вызывают подозрения гакже к организациям, являющимся 2.5. Осуществлять непрерывный 3.6. Изменить пароли всех учетных аккредитованными центрами ваписей. Убедится, что все старые ГосСОПКА, за консультацией и мониторинг изолированных сессии были завершены, чтобы оказанием услуг по расследовани сёгментов сети на предмет новых «заражений предотвратить доступ по инпилёнта устаревшим учетным данным 3.7. Провести анализ 5.6. Сообивите о ходе и результатах расследования атаки и принятых подозрительных процессов и служб мерах в НКЦКИ, ФСТЭК России для подтверждения их вредоносной активности 3.8: Провести средствами антивирусной защиты полную проверку всех систем и данных с использованием актуальных Обозначения антивирусных баз для обнаружения и удаления возможных Этапы нейтрализации угроз безопасности пиформации вредоносных программ Меры, направленные на нейтрализацию угроз безопасности 3.9. Удалить ВПО с зараженных информации, связанных с внедрением вирусов-шифровальщиков систем, а также все вредоносные процессы, службы и связанные с

ними файлы

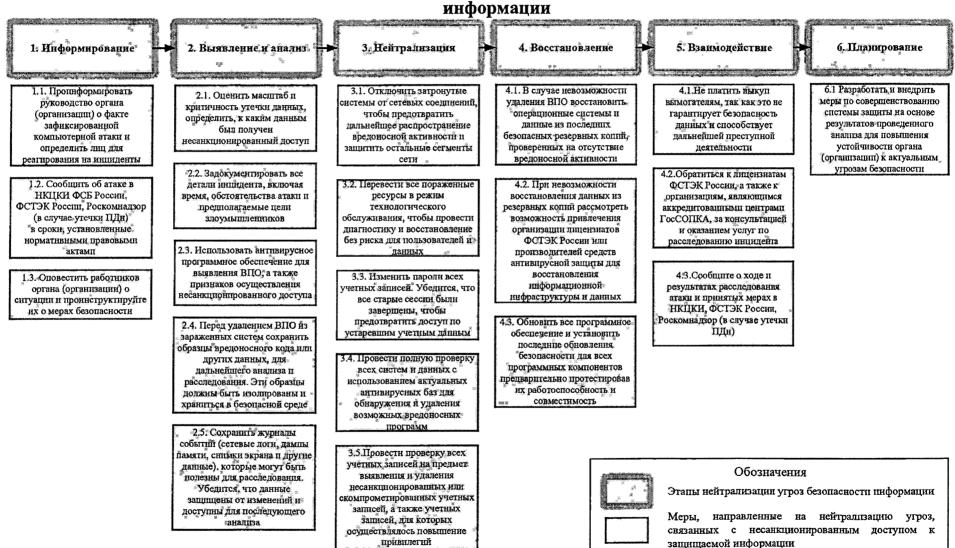
Реализация указанного порядка не должна противоречить мероприятиям, предусмотренным Планом реагирования на компьютерные инциденты, разработка и реализация которых предусмотрена нормативными правовыми актами ФСБ России

2. Порядок действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в администрации Ивнянского района и подведомственных учреждениях при реализации угроз безопасности информации, связанных с внедрением нежелательного контента на информационном ресурсе



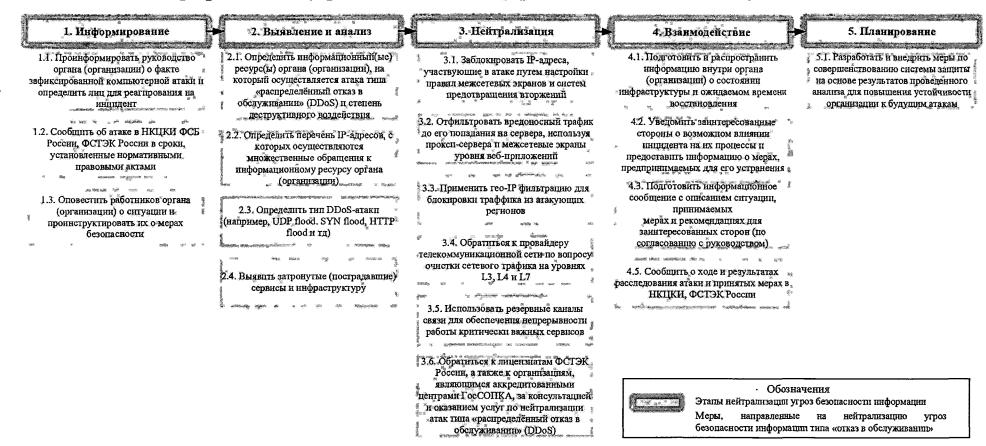
^{*} Реализация указанного порядка не должна противоречить мероприятиям, предусмотренным Планом реагирования на компьютерные инциденты, разработка и реализация хоторых предусмотрена вормативными правовыми актами ФСБ России

3. Порядок действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в администрации Ивнянского района и подведомственных учреждениях при реализации угроз безопасности информации, связанных с несанкционированным доступом к защищаемой



^{*} Реализация указанного порядка не должна противоречить мероприятиям, предусмотренным Планом реагирования на компьютерные инциденты, разработка и реализация которых предусмотрена нормативными правовыми актами ФСБ России

4. Порядок действий по обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в администрации Ивнянского района и подведомственных учреждениях при реализации угроз безопасности информации типа «отказ в обслуживании»



^{*} Реализация указанного порядка не должна противоречить мероприятиям, предусмотренным Планом реагпрования на компьютерные инциденты, разработка и реализация которых предусмотрена нормативными правовыми актами ФСБ России

