Для служебного пользования

|  |  |
| --- | --- |
| СОГЛАСОВАНОРуководитель Управления ФСТЭК России по Приволжскому Федеральному округу\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П.В. Максяков«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г. | УТВЕРЖДАЮРуководитель Учреждения\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.И. Иванов«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г. |

План мероприятий, реализуемых ГБУЗ НО «НАИМЕНОВАНИЕ УЧРЕЖДЕНИЯ» при установлении в отношении принадлежащих ему объектов информационной инфраструктуры уровней опасности проведения целевых компьютерных атак

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование мероприятия | Ответственные | Срок исполнения | Примечание |
| 1. При установлении критического («красного») уровня опасности проведения целевых компьютерных атак
 |
| 1.1 | Информирование руководителя об установленном критическом («красном») уровне опасности проведения компьютерной атаки | Руководитель учреждения / Заместитель руководителя учреждения | Ч1 + ≤ 1 час | В соответствии с нормативным правовым актом, определяющим порядок получения и оперативного доведения решения об установлении уровня опасности проведения целевых компьютерных атак, а также информации о необходимости принятия дополнительных мер по повышению защищённости объектов информационной инфраструктуры, утвержденным высшим должностным лицом субъекта Российской Федерации |
| 1.2 | Информирование работников, имеющих доступ к объектам информационной инфраструктуры, в отношении которых установлен уровень опасности, о вероятной компьютерной атаке | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 12 часов |  |
| 1.3 | Информирование работников, поставщиков продуктов и услуг в сфере информационных технологий, подрядных организаций в сфере информационных технологий, иных юридических и физических лиц, имеющих доступ к объектам информационной инфраструктуры, о необходимости принятия мер по блокированиюугроз и о необходимости соблюдения требований по безопасности при предоставлении услуг | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 24 часов | Способ уведомления определяется с учетом того, что не должны быть раскрыты уровень проведения целевых компьютерных атак и подробности реализации мероприятия |
| 1.4 | Организация круглосуточного мониторинга информационной безопасности объектов информационной инфраструктуры и круглосуточного дежурства групп оперативного реагирования на компьютерные инциденты из числа наиболее подготовленных специалистов Учреждения, предусматривающего круглосуточную готовность к реализации мер по обеспечению безопасности объектов информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток | На организацию мониторинга выделяется до 3.5 суток. Далее мониторинг проводится в круглосуточном режиме до окончания уровня опасности |
| 1.5 | Организация круглосуточных дежурств инженеров и иного технического персонала, ответственных за обеспечение функционирования объектов информационной инфраструктуры, в отношении который установлен уровень опасности | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток | На организацию дежурства выделяется до 3.5 суток. Далее дежурство проводится в круглосуточном режиме до окончания действия уровня опасности |
| 1.6 | Организация процесса приоритетной обработки информации об аномалиях, обнаруженных в работе объектов информационной инфраструктуры. При этом любой сбой в работе объектов информационной инфраструктуры по причине, не установленной достоверно, в первую очередь рассматривается как результат компьютерной атаки | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток | Любой сбой в работе объектов информационной инфраструктуры по причине, не установленной достоверно, в первую очередь рассматривается как результат компьютерной атаки |
| 1.7 | Организация экстренного взаимодействия подразделений и работниковУчреждения, а также проверка установленных способов взаимодействия работников Учреждения, обеспечивающих функционирование объектов информационной инфраструктуры, с центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток |  |
| 1.8 | Реализация мер обеспечения бесперебойного функционирования Учреждения при осуществлении в отношении принадлежащих ему объектов информационной инфраструктуры компьютерной атаки | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток |  |
| 1.9 | Реализация временного ограничения доступа к объектам информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток | В течении действия критического («красного») уровня опасности |
| 1.10 | Проверка актуальности версий программного обеспечения средств защиты информации (далее - СЗИ), применяемых для обеспечения безопасности объектов информационной инфраструктуры, а также их баз данных, осуществляемая не реже, чем раз в неделю, при наличии их обновлений - незамедлительное применение этих обновлений | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток | Не реже чем 1 раз в день. При наличии обновлений – незамедлительная их установка |
| 1.11 | Внеплановый контроль (анализ) защищенности объектов информационной инфраструктуры,включающий:а) выявление возможных точек проникновения внешнего нарушителя на объекты информационной инфраструктуры (каналы удаленного доступа, подключения к сети «Интернет», через взаимодействие с иными информационными (автоматизированными)системами, через беспроводные сети и другие способы);б) анализ уязвимостей узлов объектов информационной инфраструктуры, являющихся точками проникновения внешнего нарушителя на объекты информационной инфраструктуры, в том числе контроль состава программного обеспечения, установленного на этих узлах, уязвимостей программного обеспечения узлов, включая прикладное и системное программное обеспечение; | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток |  |
| 1.12 | Минимизация состава программного обеспечения, установленного насоответствующих узлах сети, с учетом технологической необходимости | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток |  |
| 1.13 | Анализ актуальности учетных записей пользователей программного обеспечения и смена аутентификаторов учетных записей пользователей программного обеспечения, установленного на соответствующих узлах сети(при необходимости) и анализ их стойкости | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток |  |
| 1.14 | Удаление неактуальных учётных записей пользователей программного обеспечения, установленного на соответствующих узлах сети | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток |  |
| 1.15 | Проверку конфигурации системы доменных имен на стороне Учреждения и на стороне регистратора доменов и устранение выявленных в результате такой проверки недостатков обеспечения безопасности | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток |  |
| 1.16 | Проверка настроек средств межсетевого экранирования и активного сетевого оборудования, находящегося на границе периметра Учреждения,включая актуальные обновления прошивок, отключение неиспользуемыхпортов и ограничение на доступ пользователей в сеть «Интернет» | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 3,5 суток |  |
| 1.17 | Исключение из состава объектов информационной инфраструктуры беспроводных сетей | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток |  |
| 1.18 | Принятие организационных и технических мер по обеспечению физической защиты компонентов объектов защиты, в том числе средств их администрирования | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток |  |
| 1.19 | Ограничение количества подключаемых к объектам информационной инфраструктуры съемных машинных носителей информации до минимально необходимого состава или полного исключения применения съемных машинных носителей информации | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток | Постоянно в течении действия критического («красного») уровня опасности |
| 1.20 | Настройка средств антивирусной защиты, средств предотвращения утечек данных, систем обнаружения вторжений и систем управления событиями информационной безопасности, применяемых для обеспечения безопасности объектов защиты, на максимально детализированный анализсоответствующих данных | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток |  |
| 1.21 |  Обеспечение ежедневного резервирования информации,обрабатываемой в объектах информационной инфраструктуры, а также хранения резервных копий, исключающих несанкционированный доступ к ним в результате компьютерных атак | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток |  |
| 1.22 | Ограничение до минимально необходимого количестваавтоматизированных рабочих мест, на которых реализованы сервисы электронной почты, и обеспечение контроля почтовых вложений на предмет наличия вредоносного программного обеспечения | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток | Постоянно в течении действия критического («красного») уровня опасности |
| 1.23 | Информирование не менее одного раза в день работников Управления ФСТЭК России по ПФО, ответственных за координацию, методическое сопровождение и контроль реализации Плана мероприятий, о принятых мерах по повышению защищённости объектов информационной инфраструктуры и о текущем состоянии безопасности этих объектов. О выявленных признаках проведения компьютерных атак в отношении объектов информационной инфраструктуры и компьютерных инцидентах в них незамедлительно осуществляется информирование работников Управления ФСТЭК России по Приволжскому федеральному округу, работников НКЦКИ, ответственных за координацию деятельности по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 7 суток | Ежедневно в течение действия критического («красного») уровня опасности. Целесообразно осуществлять информирование через головные подразделения по технической защите информации не отнесенной к государственной тайне |
| 1. При установлении высокого («оранжевого») уровня опасности проведения целевых компьютерных атак
 |
| 2.1 | Информирование руководителя об установленном высоком («оранжевом») уровне опасности проведения компьютерной атаки | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 1 час | В соответствии с нормативным правовым актом, определяющим порядок получения и оперативного доведения решения об установлении уровня опасности проведения целевых компьютерных атак, а также информации о необходимости принятия дополнительных мер по повышению защищённости объектов информационной инфраструктуры, утвержденным высшим должностным лицом субъекта Российской Федерации |
| 2.2 | Информирование работников, имеющих доступ к объектам информационной инфраструктуры, в отношении которых установлен уровень опасности, о вероятной компьютерной атаке | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 12 часов |  |
| 2.3 | Информирование работников, поставщиков продуктов и услуг в сфере информационных технологий, подрядных организаций в сфере информационных технологий, иных юридических и физических лиц, имеющихдоступ к объектам информационной инфраструктуры, о необходимости принятия мер по блокированию угроз и о необходимости соблюдения требований по безопасности при предоставлении услуг | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 24 часа | Способ уведомления определяется с учетом того, что не должны быть раскрыты уровень проведения целевых компьютерных атак и подробности реализации мероприятий |
| 2.4 | Реализация временного ограничения доступа к объектам информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 15 суток | В течение действия высокого («оранжевого») уровня опасности |
| 2.5 | Организация мониторинга информационной безопасности объектов информационной инфраструктуры и дежурства групп оперативного реагирования на компьютерные инциденты из числа наиболее подготовленных специалистов Учреждения, предусматривающего готовность к реализации мер по обеспечению безопасности объектов информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 15 суток | По графику, утвержденному руководителем (минимально в течение рабочего времени) |
| 2.6 | Организация дежурств инженеров и иного технического персонала, ответственных за обеспечение функционирования объектов информационной инфраструктуры, в отношении которых установлен уровень опасности | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток | По графику, утвержденному руководителем (минимально в течение рабочего времени) |
| 2.7 | Изменение графика регламентных работ на объектах информационной инфраструктуры в части переноса сроков регламентных работ | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток |  |
| 2.8 | Внеплановый контроль (анализ) защищенности объектов информационной инфраструктуры, включающий:а) выявление возможных точек проникновения внешнего нарушителя на объекты информационной инфраструктуры (каналы удаленного доступа, подключения к сети «Интернет», через взаимодействие с иными информационными (автоматизированными)системами, через беспроводные сети и другие способы);б) анализ уязвимостей узлов объектов информационной инфраструктуры, являющихся точками проникновения внешнего нарушителя на объекты информационной инфраструктуры, в том числе контроль состава программного обеспечения, установленного на этих узлах,уязвимостей архитектуры, конфигурации и кода программного обеспеченияузлов включая прикладное и системное программное обеспечение, прошивкиоборудования и микропрограммы процессоров;в) проверку наличия цифровых сертификатов, выданных нелегитимно на доменные имена Учреждения;г) проверку источников обновления программного обеспечения,используемого на объектах информационной инфраструктуры; | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 15 суток |  |
| 2.9 | Минимизация состава программного обеспечения, установленного на соответствующих узлах сети, с учетом технологической необходимости | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток |  |
| 2.10 | Анализ актуальности учетных записей пользователей программного обеспечения и сложности аутентификаторов учетных записей, удаление неактуальных учётных записей пользователей программного обеспечения, установленного на соответствующих узлах сети | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 15 суток |  |
| 2.11 | Смена аутентификаторов учетных записей пользователей программного обеспечения, установленного на соответствующих узлах сети(при необходимости); | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 15 суток | В первую очередь учетных записей с повышенными привилегиями и сервисных учетных записей |
| 2.12 | Выполнение комплекса специальных технических мер по активному целенаправленному поиску и анализу следов компрометации на объектах информационной инфраструктуры (сроки ретроспективного исследования информации баз данных, журналоврегистрации событий, внешних источников (последовательно) - 1 месяц, 6 месяцев, 12 месяцев) | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток |  |
| 2.13 | проверка соблюдения правил безопасной работы на объектах информационной инфраструктуры, включающая:а) проверку соблюдения ограничений на использование средств и протоколов файлового обмена и правил безопасного использования таких средств на объектах информационной инфраструктуры;б) проверку соблюдения ограничений на использование средств и протоколов удалённого доступа (администрирования) и правил безопасного использования таких средств в отношении объектов информационной инфраструктуры;в) проверку соблюдения требований и правил разграничения прав доступа в объектах информационной инфраструктуры;г) проверку соблюдения ограничений и правил безопасного обращения скорпоративной почтой, средствами аудио- и видеоконференц-связи;д) проверку соблюдения требований парольной политики на объектах информационной инфраструктуры;е) контроль невозможности подключения неучтенных съемных машинных носителей информации и мобильных устройств;ж) проверку соблюдения ограничений на доступ ко внешним ресурсам со средств, входящих в состав объектов информационной инфраструктуры;з) проверку соблюдения требований и процедур экстренного взаимодействия подразделений и работников Учреждения; | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток |  |
| 2.14 | Проверка актуальности версий программного обеспечения СЗИ, применяемых для обеспечения безопасности объектов информационной инфраструктуры, а также их баз данных, осуществляемая не реже, чем раз в 3 дня, при наличии их обновлений -незамедлительное применение этих обновлений | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток | Не реже 1 раза в 3 дня. При наличии обновлений – незамедлительное их применение  |
| 2.15 | Контроль съемных машинных носителей информации, подключаемых к объектам информационной инфраструктуры, управление физическим доступом к ним, контроль ихподключения к иным информационным (автоматизированным) системам | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток | Постоянно в течение действия высокого («оранжевого») уровня опасности |
| 2.16 | Реализация многофакторной аутентификации для удаленного доступа администраторов к объектам информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток |  |
| 2.17 | Принятие мер по обеспечению физической защиты объекта информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток | Усиление контроля физического доступа к объектам информационной инфраструктуры |
| 2.18 | Обеспечение возможности оперативного восстановленияфункционирования объектов информационной инфраструктуры и (или) выполнения их функций в случае возникновения нештатных ситуаций | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток |  |
| 2.19 | Настройка средств антивирусной защиты, средств предотвращения утечек данных, систем обнаружения вторжений и систем управления событиями информационной безопасности, применяемых для обеспечениябезопасности объектов информационной инфраструктуры, на максимально детализированный анализсоответствующих данных и установка актуальных баз данных средств антивирусной защиты и решающих правил | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 15 суток |  |
| 2.20 | Обеспечение резервного копирования информации, обрабатываемой в объектах информационной инфраструктуры, не реже, чем раз в 3 дня, а также хранения резервных копий, исключающих несанкционированный доступ к ним в результате компьютерныхатак | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток |  |
| 2.21 | Ограничение до минимально необходимого количестваавтоматизированных рабочих мест, на которых реализованы сервисы электронной почты, и обеспечение контроля почтовых вложений на предмет наличия вредоносного программного обеспечения | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 30 суток | Постоянно в течение действия высокого («оранжевого») уровня опасности |
| 1. При установлении повышенного («желтого») уровня опасности проведения целевых компьютерных атак
 |
| 3.1 | Информирование руководителя об установленном повышенном («жёлтом») уровне опасности проведения компьютерной атаки | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 1 час | В соответствии с нормативным правовым актом, определяющим порядок получения и оперативного доведения решения об установлении уровня опасности проведения целевых компьютерных атак, а также информации о необходимости принятия дополнительных мер по повышению защищённости объектов информационной инфраструктуры, утвержденным высшим должностным лицом субъекта Российской Федерации |
| 3.2 | Информирование работников, имеющих доступ к объектам информационной инфраструктуры, в отношении которых установлен уровень опасности, о вероятной компьютерной атаке | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 12 часов |  |
| 3.3 | Информирование работников, поставщиков продуктов и услуг в сфере информационных технологий, подрядных организаций в сфере информационных технологий, иных юридических и физических лиц, имеющихдоступ к объектам информационной инфраструктуры, о необходимости принятия мер по блокированию угроз и о необходимости соблюдения требований по безопасности при предоставлении услуг | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 24 часа | Способ уведомления определяется с учетом того, что не должны быть раскрыты уровень проведения целевых компьютерных атак и подробности реализации мероприятий |
| 3.4 | Реализация временного ограничения доступа к объектам информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 45 суток | В течение действия повышенного («жёлтого») уровня опасности |
| 3.5 | Организация мониторинга информационной безопасности объектов информационной инфраструктуры и дежурства групп оперативного реагирования на компьютерные инциденты из числа наиболее подготовленных специалистов Учреждения, предусматривающего готовность к реализации мер по обеспечению безопасности объектов информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 45 суток | По графику, утвержденному руководителем (минимально в течение рабочего времени) |
| 3.6 | Организация дежурств инженеров и иного технического персонала, ответственных за обеспечение функционирования объектов информационной инфраструктуры, в отношении которых установлен уровень опасности | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток | По графику, утвержденному руководителем (минимально в течение рабочего времени) |
| 3.7 | Изменение графика регламентных работ на объектах информационной инфраструктуры в части переноса сроков регламентных работ | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.8 | Внеплановый контроль (анализ) защищенности объектов информационной инфраструктуры, включающий:а) выявление возможных точек проникновения внешнего нарушителя на объекты информационной инфраструктуры (каналы удаленного доступа, подключения к сети «Интернет», через взаимодействие с иными информационными (автоматизированными)системами, через беспроводные сети и другие способы);б) анализ уязвимостей узлов объектов информационной инфраструктуры, являющихся точками проникновения внешнего нарушителя на объекты информационной инфраструктуры, в том числе контроль состава программного обеспечения, установленного на этих узлах,уязвимостей архитектуры, конфигурации и кода программного обеспеченияузлов включая прикладное и системное программное обеспечение, прошивкиоборудования и микропрограммы процессоров;в) проверку наличия цифровых сертификатов, выданных нелегитимно на доменные имена Учреждения ;г) проверку источников обновления программного обеспечения,используемого на объектах информационной инфраструктуры; | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 45 суток |  |
| 3.9 | Минимизация состава программного обеспечения, установленного на соответствующих узлах сети, с учетом технологической необходимости | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.10 | Анализ актуальности учетных записей пользователей программного обеспечения и сложности аутентификаторов учетных записей, удаление неактуальных учётных записей пользователей программного обеспечения, установленного на соответствующих узлах сети | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 45 суток |  |
| 3.11 | Смена аутентификаторов учетных записей пользователей программного обеспечения, установленного на соответствующих узлах сети(при необходимости); | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 45 суток | В первую очередь учетных записей с повышенными привилегиями и сервисных учетных записей |
| 3.12 | Выполнение комплекса специальных технических мер по активному целенаправленному поиску и анализу следов компрометации на объектах информационной инфраструктуры (сроки ретроспективного исследования информации баз данных, журналоврегистрации событий, внешних источников (последовательно) - 1 месяц, 6 месяцев, 12 месяцев) | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.13 | проверка соблюдения правил безопасной работы на объектах информационной инфраструктуры, включающая:а) проверку соблюдения ограничений на использование средств и протоколов файлового обмена и правил безопасного использования таких средств на объектах информационной инфраструктуры;б) проверку соблюдения ограничений на использование средств и протоколов удалённого доступа (администрирования) и правил безопасного использования таких средств в отношении объектов информационной инфраструктуры;в) проверку соблюдения требований и правил разграничения прав доступа в объектах информационной инфраструктуры;г) проверку соблюдения ограничений и правил безопасного обращения скорпоративной почтой, средствами аудио- и видеоконференц-связи;д) проверку соблюдения требований парольной политики на объектах информационной инфраструктуры;е) контроль невозможности подключения неучтенных съемных машинных носителей информации и мобильных устройств;ж) проверку соблюдения ограничений на доступ ко внешним ресурсам со средств, входящих в состав объектов информационной инфраструктуры;з) проверку соблюдения требований и процедур экстренного взаимодействия подразделений и работников Учреждения ; | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.14 | Проверка актуальности версий программного обеспечения СЗИ, применяемых для обеспечения безопасности объектов информационной инфраструктуры, а также их баз данных, осуществляемая не реже, чем раз в 3 дня, при наличии их обновлений -незамедлительное применение этих обновлений | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток | Не реже 1 раза в 3 дня. При наличии обновлений – незамедлительное их применение  |
| 3.15 | Контроль съемных машинных носителей информации, подключаемых к объектам информационной инфраструктуры, управление физическим доступом к ним, контроль ихподключения к иным информационным (автоматизированным) системам | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток | Постоянно в течение действия повышенного («жёлтого») уровня опасности |
| 3.16 | Реализация многофакторной аутентификации для удаленного доступа администраторов к объектам информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.17 | Принятие мер по обеспечению физической защиты объекта информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток | Усиление контроля физического доступа к объектам информационной инфраструктуры |
| 3.18 | Обеспечение возможности оперативного восстановленияфункционирования объектов информационной инфраструктуры и (или) выполнения их функций в случае возникновения нештатных ситуаций | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.19 | Настройка средств антивирусной защиты, средств предотвращения утечек данных, систем обнаружения вторжений и систем управления событиями информационной безопасности, применяемых для обеспечениябезопасности объектов информационной инфраструктуры, на максимально детализированный анализсоответствующих данных и установка актуальных баз данных средств антивирусной защиты и решающих правил | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 45 суток |  |
| 3.20 | Обеспечение резервного копирования информации, обрабатываемой в объектах информационной инфраструктуры, не реже, чем раз в 3 дня, а также хранения резервных копий, исключающих несанкционированный доступ к ним в результате компьютерныхатак | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.21 | Ограничение до минимально необходимого количестваавтоматизированных рабочих мест, на которых реализованы сервисы электронной почты, и обеспечение контроля почтовых вложений на предмет наличия вредоносного программного обеспечения | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток | Постоянно в течение действия повышенного («жёлтого») уровня опасности |
| 3.22 | Проверка знаний и практических навыков, полученных в результатеобучения, у работников Учреждения | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.23 | Проведение (при возможности) отработки выполнения мероприятий,предусмотренных планом мероприятий, а также по противодействиюкомпьютерным атакам на объекты информационной инфраструктуры, восстановлению их работоспособности и устранению последствий компьютерных инцидентов | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.24 | Проверка соблюдения ограничений на использование на объектах информационной инфраструктуры личных средств вычислительной техники (ноутбуков, планшетов, смартфонов), модемов и съемных машинных носителей информации и правил безопасногоиспользования таких средств | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.25 | Проверка соблюдения ограничений на применение на объектах информационной инфраструктуры наиболее часто используемого при реализации компьютерных атак программного обеспечения, в том числе Microsoft Office, Adobe, браузеров, средств администрирования командных оболочек (например, PowerShell, Bash и другие) и правил их безопасного использования | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.26 | Проверка на объектах информационной инфраструктуры соблюдения ограничений наиспользование программного обеспечения, не относящегося к производственной деятельности и не требуемого для выполнения должностныхобязанностей работников Учреждения | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.27 | Принятие организационных и технических мер по аутентификации устройств при их подключении ко всем объектам информационной инфраструктуры | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |
| 3.28 | Реализация многофактороной аутентификации для удаленного доступа к объектам информационной инфраструктуры для всех пользователей | Руководитель учреждения / Заместитель руководителя учреждения | Ч + ≤ 90 суток |  |

*1 Дата и время получения информации об установлении уровня опасности проведения целевых компьютерных атак. Информация может быть получена от работников ФСТЭК России, ответственных за координацию, методическое сопровождение и контроль реализации настоящего Плана мероприятий, а также иных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (центр ГосСОПКА).*

Перечень ключевых объектов информационной инфраструктуры:

* Информационно-телекоммуникационная сеть ГБУЗ НО «НАИМЕНОВАНИЕ УЧРЕЖДЕНИЯ»

Подписи должностных лиц, ответственных за разработку Плана мероприятий:

 Руководитель ГБУЗ НО «НАИМЕНОВАНИЕ УЧРЕЖДЕНИЯ»

Иванов Иван Иванович \\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (дата, подпись)

С планом ознакомлены:

Заместитель руководителя ГБУЗ НО «НАИМЕНОВАНИЕ УЧРЕЖДЕНИЯ»

Иванов Иван Иванович \\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (дата, подпись)