

|  |
| --- |
| АДМИНИСТРАЦИЯ  ВАРНЕНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА  ЧЕЛЯБИНСКОЙ ОБЛАСТИ  **РАСПОРЯЖЕНИЕ** |

|  |
| --- |
| От 05.09.2022 г. № 566-р  с. Варна |

Об утверждении Плана мероприятий по противодействию целевым компьютерным атакам на информационно-коммуникационную инфраструктуру

В целях реализации пункта 3.1. Протокола заседания Комиссии по информационной безопасности Челябинской обла­сти:

1. Утвердить План мероприятий по противодействию целевым компьютерным атакам на информационно-коммуникационную инфраструктуру (Приложение № 1).
2. Начальнику отдела информационных технологий и технической защиты ин­формации администрации Варненского муниципального района (Зуев Е.П.) организовать исполнение плана.
3. Контроль за исполнением настоящего распоряжения возложить на управляющего администрацией Варненского муниципального района Маклакова А.В.

**Глава Варненского**

**муниципального района К.Ю.Моисеев**

Приложение № 1

к распоряжению от «\_\_\_»\_\_\_\_ 2022 г. № \_\_\_\_

План мероприятий по противодействию целевым компьютерным атакам на информационно-коммуникационную инфраструктуру

*администрации Варненского муниципального района Челябинской области*

| **№**  **п/п** | **Наименование мероприятия** | **Ответственный** | **Срок выполнения** | **Примечание** |
| --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** |
| При установлении критического («красного») уровня проведения целевых компьютерных атак | | | | |
| 1 | Информирование сотрудников о вероятной компьютерной атаке | Отдел ИТ и ТЗИ | Немедленно |  |
| 2 | 2.1. Формирование перечня мер по блокированию угрозы, которая может способствовать реализации компьютерной атаки | Отдел ИТ и ТЗИ | Немедленно |  |
| 2.2 Информирование сотрудников, поставщиков продуктов и услуг в сфере информационных технологий, подрядных организаций в сфере информационных технологий, иных юридических и физических лиц, имеющих доступ к ИКИ о необходимости принятия мер по блокированию угроз и о необходимости соблюдения требований по безопасности при предоставлении услуг | Отдел ИТ и ТЗИ | Немедленно |  |
| 3 | 3.1. Формирование группы оперативного реагирования на компьютерные инциденты из числа наиболее подготовленных специалистов, назначение руководителя группы | Отдел ИТ и ТЗИ | В течении часа |  |
| 3.2. Организация круглосуточного мониторинга информационной безопасности и круглосуточного дежурства группы оперативного реагирования на компьютерные инциденты из числа наиболее подготовленных специалистов, предусматривающего круглосуточную готовность к реализации мер по обеспечению безопасности | Отдел ИТ и ТЗИ | В течении часа |  |
| 4 | Организация круглосуточного дежурства сотрудников, ответственных за обеспечение функционирования объектов ИКИ | Отдел ИТ и ТЗИ | В течении часа |  |
| 5 | Организация процесса приоритетной обработки информации об аномалиях, обнаруженных в работе объектов ИКИ. Любой сбой рассматривается как результат компьютерной атаки. | Отдел ИТ и ТЗИ | В течении часа |  |
| 6 | Организация экстренного взаимодействия подразделений и сотрудников, проверка установленных способов взаимодействия группы реагирования на компьютерные инциденты и НКЦКИ | Отдел ИТ и ТЗИ | В течении часа |  |
| 7 | Реализация мер обеспечения бесперебойного функционирования | Отдел ИТ и ТЗИ | В течении суток |  |
| 8 | Реализация временного ограничения доступа к объектам ИКИ | Отдел ИТ и ТЗИ | В течении часа |  |
| 9 | Проверка актуальности версий программного обеспечения СЗИ, а также их баз данных (далее проводится ежедневно), при наличии обновлений – незамедлительное применение обновлений | Отдел ИТ и ТЗИ | В течении 7 дней |  |
| 10 | Внеплановый контроль (анализ) защищённости ИКИ:  - выявление возможных точек проникновения внешнего нарушителя ИКИ;  - анализ уязвимостей объектов ИКИ, являющихся точками проникновения внешнего нарушителя | Отдел ИТ и ТЗИ | В течении 3 дней |  |
| 11 | Минимизация состава ПО, установленного на объектах ИКИ | Отдел ИТ и ТЗИ | В течении 7 дней |  |
| 12 | Анализ актуальности учётных записей пользователей, смена аутентификационной информации и анализ их стойкости | Отдел ИТ и ТЗИ | В течении 7 дней |  |
| 13 | Удаление неактуальных учётных записей | Отдел ИТ и ТЗИ | В течении 7 дней |  |
| 14 | Проверка конфигурации системы доменных имён на стороне организации и на стороне регистратора доменов и устранение выявленных в результате такой проверки недостатков обеспечения безопасности |  | В течении 7 дней |  |
| 15 | Проверка настроек средств межсетевого экранирования и активного сетевого оборудования, включая актуальные обновления прошивок, отключение неиспользуемых портов и ограничение на доступ пользователей в сеть «Интернет» | Отдел ИТ и ТЗИ | В течении 3 дней |  |
| 16 | Исключение из состава объектов ИКИ беспроводных сетей | Отдел ИТ и ТЗИ | В течении 7 дней |  |
| 17 | Принятие организационных и технических мер по обеспечению физической защиты | Управляющий делами,  Отдел ИТ и ТЗИ | В течении часа |  |
| 18 | Полное исключение применения съёмных машинных носителей информации (за исключением сертифицированных средств хранения электронных подписей) | Отдел ИТ и ТЗИ | В течении 7 дней |  |
| 19 | Настройка средств антивирусной защиты и других СЗИ, при наличии, на максимально детализированный анализ соответствующих данных | Отдел ИТ и ТЗИ | В течении часа |  |
| 20 | Обеспечение ежедневного резервирования информации и ПО, а также хранения резервных копий, исключающего несанкционированный доступ к ним в результате компьютерных атак | Отдел ИТ и ТЗИ | В течении 7 дней |  |
| 21 | Ограничение до минимально необходимого количества АРМ, на которых реализованы сервисы электронной почты, и обеспечение контроля почтовых вложений на предмет наличия вредоносного ПО | Отдел ИТ и ТЗИ | В течении 7 дней |  |
| 22 | Информирование не менее одного раза в день работников Минцифры ЧО, ответственных за координацию, методическое сопровождение и контроль реализации Плана мероприятий, о принятых мерах по повышению защищённости и о его текущем состоянии. О выявлении признаках компьютерных атак и компьютерных инцидентах незамедлительно осуществляется информирование работников Минцифры ЧО, ФСТЭК России и НКЦКИ | Отдел ИТ и ТЗИ | В течении часа |  |
| При установлении высокого («оранжевого») уровня проведения целевых компьютерных атак | | | | |
| 1 | Информирование сотрудников о вероятной компьютерной атаке | Отдел ИТ и ТЗИ | В течении часа |  |
| 2 | 2.1. Формирование перечня мер по блокированию угрозы, которая может способствовать реализации компьютерной атаки | Отдел ИТ и ТЗИ | В течении суток |  |
| 2.2. Информирование сотрудников, поставщиков продуктов и услуг в сфере информационных технологий, подрядных организаций в сфере информационных технологий, иных юридических и физических лиц, имеющих доступ к ИКИ, о необходимости принятия мер по блокированию угроз и о необходимости соблюдения требований по безопасности при предоставлении услуг | Отдел ИТ и ТЗИ | В течении суток |  |
| 3 | Реализация временного ограничения доступа к объектам ИКИ | Отдел ИТ и ТЗИ | В течении суток |  |
| 4 | 4.1. Организация мониторинга информационной безопасности ИКИ | Отдел ИТ и ТЗИ | В течении 3 дней |  |
| 4.2. Формирование группы оперативного реагирования на компьютерные инциденты из числа наиболее подготовленных специалистов, назначение руководителя группы, организация дежурства группы | Отдел ИТ и ТЗИ | В течении 3 дней |  |
| 4.3. Организация дежурства группы оперативного реагирования на компьютерные инциденты | Отдел ИТ и ТЗИ | В течении суток |  |
| 5 | Организация дежурств сотрудников, ответственных за обеспечение функционирования объектов ИКИ | Отдел ИТ и ТЗИ | В течении суток |  |
| 6 | Изменение графиков регламентных работ на объектах ИКИ в части переноса сроков регламентных работ | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 7 | Внеплановый контроль (анализ) защищённости объектов ИКИ:  - выявление возможных точек проникновения внешнего нарушителя в ИКИ;  - анализ уязвимостей объектов ИКИ, являющихся точками проникновения внешнего нарушителя;  - проверка наличия цифровых сертификатов, выданных нелегитимно на доменные имена;  - проверка источников обновления ПО, используемого на объектах ИКИ. | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 8 | Минимизация состава ПО с учётом технологической необходимости | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 9 | Анализ актуальности учётных записей пользователей и сложности аутентификаторов учётных записей, удаление неактуальных учётных записей | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 10 | При необходимости смена аутентификационной информации | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 11 | Выполнение комплекса специальных технических мер по активному целенаправленному поиску и анализу следов компрометации в ИКИ | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 12 | Проверка соблюдения правил безопасной работы:  - проверка соблюдения ограничения на использование средств и протоколов файлового обмена и правил безопасного использования таких средств;  - проверка правил безопасного использования средств и протоколов удалённого доступа (администрирования);  - проверка соблюдения требований и правил безопасного обращения с корпоративной почтой, средствами аудио- и видеоконференцсвязи;  - проверка соблюдения требований парольной политики;  - контроль невозможности подключения неучтённых съёмных носителей информации и мобильных устройств;  - проверка соблюдения требований и процедур экстренного взаимодействия подразделений и Минцифры ЧО | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 13 | Проверка актуальности версий программного обеспечения СЗИ, а также обновление их баз данных не реже одного раза в 3 дня, при наличии – незамедлительное применение обновлений | Отдел ИТ и ТЗИ | 1 раз в 3 дня |  |
| 14 | Контроль съёмных машинных носителей информации, управление физическим доступом к ним | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 15 | Реализация многофакторной аутентификации для удалённого доступа администраторов к объектам ИКИ | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 16 | Принятие мер по обеспечению физической защиты | Управляющий делами,  Отдел ИТ и ТЗИ | В течении часа |  |
| 17 | Обеспечение возможности оперативного восстановления функционирования объектов ИКИ, и (или) выполнения их функций в случае возникновения нештатных ситуаций | Отдел ИТ и ТЗИ | В течении недели |  |
| 18 | Настройка средств антивирусной защиты и других СЗИ, при наличии, на максимально детализированный анализ соответствующих данных | Отдел ИТ и ТЗИ | В течении недели |  |
| 19 | Обеспечение резервирования информации и ПО, не реже, чем раз в 3 дня, а также хранения резервных копий, исключающего несанкционированный доступ к ним в результате компьютерных атак | Отдел ИТ и ТЗИ | 1 раз в 3 дня |  |
| 20 | Ограничение до минимально необходимого количества АРМ, на которых реализованы сервисы электронной почты, и обеспечение контроля почтовых вложений на предмет наличия вредоносного ПО | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| При установлении повышенного («жёлтого») уровня проведения целевых компьютерных атак | | | | |
| 1 | Информирование сотрудников о вероятной компьютерной атаке | Отдел ИТ и ТЗИ | В течении часа |  |
| 2 | 2.1. Формирование перечня мер по блокированию угрозы, которая может способствовать реализации компьютерной атаки | Отдел ИТ и ТЗИ | В течении суток |  |
| 2.2. Информирование сотрудников, поставщиков продуктов и услуг в сфере информационных технологий, подрядных организаций в сфере информационных технологий, иных юридических и физических лиц, имеющих доступ к ИКИ. о необходимости принятия мер по блокированию угроз и о необходимости соблюдения требований по безопасности при предоставлении услуг | Отдел ИТ и ТЗИ | В течении суток |  |
| 3 | Реализация временного ограничения доступа к объектам ИКИ | Отдел ИТ и ТЗИ | В течении часа |  |
| 4 | 4.1. Организация мониторинга информационной безопасности | Отдел ИТ и ТЗИ | В течении суток |  |
| 4.2. Формирование группы оперативного реагирования на компьютерные инциденты из числа наиболее подготовленных специалистов, назначение руководителя группы, организация дежурства группы | Отдел ИТ и ТЗИ | В течении трёх дней |  |
| 4.3. Организация дежурства группы оперативного реагирования на компьютерные инциденты | Отдел ИТ и ТЗИ | В течении суток |  |
| 5 | Организация дежурств сотрудников, ответственных за обеспечение функционирования объектов ИКИ | Отдел ИТ и ТЗИ | В течении суток |  |
| 6 | Изменение графиков регламентных работ на объектах ИКИ в части переноса сроков регламентных работ | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 7 | Внеплановый контроль (анализ) защищённости объектов ИКИ:  - выявление возможных точек проникновения внешнего нарушителя в ИКИ;  - анализ уязвимостей объектов ИКИ, являющихся точками проникновения внешнего нарушителя;  - проверка наличия цифровых сертификатов, выданных нелегитимно на доменные имена;  - проверка источников обновления ПО, используемого на объектах ИКИ. | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 8 | Минимизация состава ПО с учётом технологической необходимости | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 9 | Анализ актуальности учётных записей пользователей и сложности аутентификаторов учётных записей, удаление неактуальных учётных записей | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 10 | При необходимости смена аутентификационной информации | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 11 | Выполнение комплекса специальных технических мер по активному целенаправленному поиску и анализу следов компрометации в ИКИ | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 12 | Проверка соблюдения правил безопасной работы:  - проверка соблюдения ограничения на использование средств и протоколов файлового обмена и правил безопасного использования таких средств;  - проверка правил безопасного использования средств и протоколов удалённого доступа (администрирования);  - проверка соблюдения требований и правил безопасного обращения с корпоративной почтой, средствами аудио- и видеоконференцсвязи;  - проверка соблюдения требований парольной политики;  - контроль невозможности подключения неучтённых съёмных носителей информации и мобильных устройств;  - проверка соблюдения требований и процедур экстренного взаимодействия подразделений и Минцифры ЧО | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 13 | Проверка актуальности версий программного обеспечения СЗИ, а также обновление их баз данных не реже одного раза в 3 дня, при наличии – незамедлительное применение обновлений | Отдел ИТ и ТЗИ | 1 раз в три дня |  |
| 14 | Контроль съёмных машинных носителей информации, управление физическим доступом к ним | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 15 | Реализация многофакторной аутентификации для удалённого доступа администраторов к объектам ИКИ | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 16 | Принятие мер по обеспечению физической защиты | Управляющий делами,  Отдел ИТ и ТЗИ | В течении суток |  |
| 17 | Обеспечение возможности оперативного восстановления функционирования объектов ИКИ, и (или) выполнения их функций в случае возникновения нештатных ситуаций | Отдел ИТ и ТЗИ | В течении недели |  |
| 18 | Настройка средств антивирусной защиты и других СЗИ, при наличии, на максимально детализированный анализ соответствующих данных | Отдел ИТ и ТЗИ | В течении недели |  |
| 19 | Обеспечение резервирования информации и ПО, не реже, чем раз в 3 дня, а также хранения резервных копий, исключающего несанкционированный доступ к ним в результате компьютерных атак | Отдел ИТ и ТЗИ | 1 раз в три дня |  |
| 20 | Ограничение до минимально необходимого количества АРМ, на которых реализованы сервисы электронной почты, и обеспечение контроля почтовых вложений на предмет наличия вредоносного ПО | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 21 | Проверка знаний и практических навыков по информационной безопасности, полученных в результате обучения, у сотрудников | Отдел ИТ и ТЗИ | В течении 90 дней |  |
| 22 | Проведение отработки выполнения мероприятий, предусмотренных Планом мероприятий, а также по противодействию компьютерным атакам, восстановлению работоспособности и устранению последствий компьютерных инцидентов | Отдел ИТ и ТЗИ | В течении 90 дней |  |
| 23 | Проверка соблюдения ограничений на использование личных средств вычислительной техники, модемов и съёмных носителей информации и правил безопасного использования таких средств | Отдел ИТ и ТЗИ | В течении недели |  |
| 24 | Проверка соблюдения ограничений на применение, наиболее часто используемого при реализации компьютерных атак ПО, в том числе Microsoft Office, Adobe, Autocad, браузеров, средств администрирования командных оболочек (PowerShell, Bash и др.) и правил их безопасного использования | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 25 | Проверка применения ПО, не относящегося к производственной деятельности и не требуемого для выполнения должностных обязанностей | Отдел ИТ и ТЗИ | В течении 30 дней |  |
| 26 | Принятие организационных и технических мер по аутентификации устройств | Отдел ИТ и ТЗИ | В течении 90 дней |  |
| 27 | Реализация многофакторной аутентификации для удалённого доступа всех категорий пользователей | Отдел ИТ и ТЗИ | В течении 90 дней |  |

В Плане были использованы следующие сокращения:

АРМ – автоматизированное рабочее место

ИКИ – информационно-коммуникационная инфраструктура

НКЦКИ – Национальный координационный центр по компьютерным инцидентам

ПО – программное обеспечение

СЗИ – средства защиты информации

Минцифры ЧО – Министерство информационных технологий, связи и цифрового развития Челябинской области

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации

**Примечание:**

1. Мероприятия, при установлении «красного» уровня опасности, предусмотренные пунктами 1-9, 12, 13, 15 реализуются в приоритетном порядке. Все мероприятия необходимо реализовать в течении 7 дней с момента поступления информации об установлении уровня опасности.
2. Мероприятия, при установлении «оранжевого» уровня опасности, предусмотренные пунктами 1-4, 7, 9, 10 и 18 реализуются в приоритетном порядке. Все мероприятия необходимо реализовать в течении 30 дней с момента поступления информации об установлении уровня опасности.
3. Мероприятия, при установлении «жёлтого» уровня опасности, реализуются в течении 90 дней с момента поступления информации об установлении уровня опасности.