|  |
| --- |
|  |
| МИНОБРНаУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

Институт кибербезопасности и цифровых технологий

КБ-4 «Интеллектуальные системы информационной безопасности»

**Отчет** по практической работе №4.2 на тему: План Реагирования на компьютерные инциденты

**по дисциплине:** «Интеллектуальные системы информационной

безопасности в промышленных системах»

**Выполнил:**

Студент группы ББМО-02-22

ФИО: Исаев А.М.

**Проверил:**

С. А. Петренко

Для разработки Плана реагирования на компьютерные инциденты выбранной на предыдущих занятиях Организации.4 необходимо ознакомиться с Требованиями к разработке Плана:

При разработке Плана учитывать организационную структуру субъекта КИИ, назначение и архитектуру ЗОКИИ, применяемые программные и программно-аппаратные средства, взаимосвязь с другими объектами КИИ, наличие и характеристики доступа к сетям связи [201 ]. План включает следующие разделы:

1. Технические характеристики и состав ЗОКИИ;

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

3. Мероприятия, проводимые в ходе реагирования на КИ и принятия мер по ликвидации последствий КА, а также время, отводимое на их реализацию;

4. Описание состава подразделений и должностных лиц субъекта КИИ, ответственных за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА.

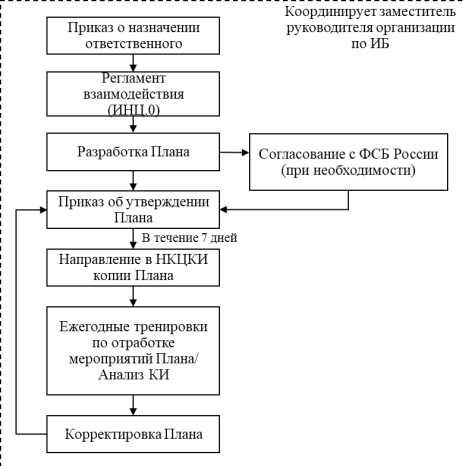


Рисунок 1 – Общие меры по планированию мероприятий реагирования на КИ и принятию мер по ликвидации последствий КА

План должен содержать перечень и состав конкретных мероприятий, проводимых субъектом КИИ на этапах «Обнаружение и регистрация КИ» и «Реагирование на КИ» в рабочее время, а также в выходные и праздничные дни, с учетом организационной структуры организации, особенностей ее информационной инфраструктуры, применяемых программных и программнотехнических средств, типов КИ, их приоритетов и уровней влияния. Пример оформления Плана приведен в приложении 3 к настоящим Методическим рекомендациям.

По структуре План содержит:

1.1. **Раздел 1.** Технические характеристики и состав ЗОКИИ. В данном разделе указываются: 1. Актуальные сведения о результатах категорирования ЗОКИИ (сведения о взаимодействии ЗОКИИ и сетей электросвязи, сведения о программных и программно-аппаратных средствах, используемых на ЗОКИИ) [15].

2. Сведения о наличии средств архивирования и резервного копирования данных.

3. Сведения о подключении ЗОКИИ к корпоративному (ведомственному) центру ГосСОПКА. 4. Сведения об установленных на ЗОКИИ средствах ГосСОПКА.

**1.2. Раздел 2.** События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий. В данном разделе могут указываться источники информации о КИ на ЗОКИИ (программные и программно-технические средства, пользователи, администраторы, внешние источники и т.д.). Реализация Плана начинается с момента выявления КИ на ЗОКИИ.

Источниками таких сведений могут выступать: − сотрудники структурного подразделения субъекта КИИ, ответственного за обеспечение безопасности ЗОКИИ; − сотрудники структурного подразделения субъекта КИИ, ответственного за эксплуатацию и (или) обеспечение функционирования ЗОКИИ, или сотрудники иной организации, выполняющие функции по эксплуатации и (или) обеспечению функционирования ЗОКИИ в силу заключенного с субъектом КИИ договора; − сотрудники структурного подразделения субъекта КИИ, ответственного за эксплуатацию средств, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, и (или) за осуществление анализа результатов функционирования этих средств, или сотрудники иной организации, выполняющие указанные функции в силу заключенного с субъектом КИИ договора; − сотрудники подрядных организаций, ответственные за эксплуатацию и (или) обеспечение функционирования ЗОКИИ в части заключенных договоров; − ДИТ;

Приказом об утверждении Плана должны быть назначены должностные лица субъекта КИИ, уполномоченные на принятие решений о реализации мероприятий Плана, информирование задействованных сил (ДИТ, ОИВ, НКЦКИ и Роскомнадзор) и организацию взаимодействия с подразделениями и должностными лицами ФСБ России.

Рекомендуемая форма приказа о возложении обязанностей по реагированию на КИ и принятию мер ликвидации последствий КА на значимом объекте КИИ и об утверждении Плана приведена в приложении 4. На рисунке 3 представлен общий подход к обнаружению и регистрации КИ, реагированию на них и информированию организации, осуществляющей координацию деятельности в части управления КИ.

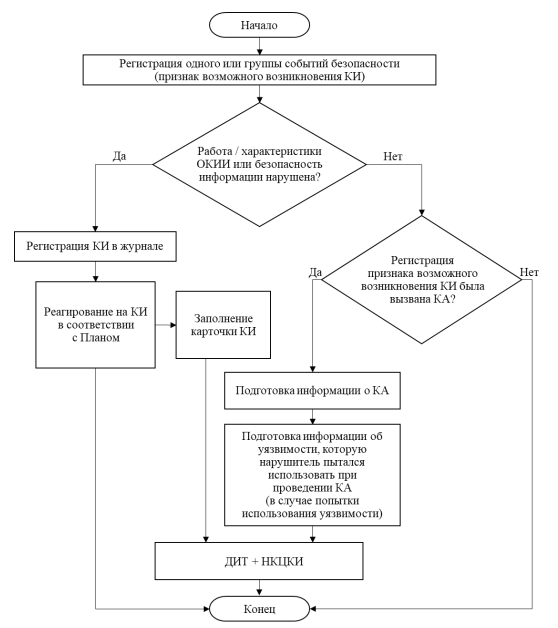


Рисунок 2 – Алгоритм реагирования на КИ

**1.3. Раздел 3. Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию**.

Перечень и состав конкретных мероприятий, проводимых субъектом КИИ в ходе реагирования на КИ и принятия мер по ликвидации последствий КА, разрабатывается с указанием времени, необходимых для реализации указанных мероприятий, исходя из: − порядка предоставления сведений об инцидентах информационной безопасности [18]; − состава и особенностей функционирования элементов ЗОКИИ; − типа выявленного компьютерного инцидента; − состава имеющихся у субъекта КИИ сил и средств, выделенных для проведения необходимых мероприятий; − наличия или отсутствия взаимодействия субъекта КИИ с ведомственным (корпоративным) центром ГосСОПКА; − необходимости привлечения сил ФСБ России; − положений документов, регламентирующих порядок эксплуатации ЗОКИИ и меры по обеспечению его безопасности; − положений иных нормативных правовых актов и методических документов. К обязательным мероприятиям реагирования относятся: 1. Обнаружение и регистрация (рекомендуемая форма карточки КИ приведена в приложении 5 к настоящим Методическим рекомендациям, рекомендуемая форма журнала учета КИ приведена в приложении 6 к настоящим Методическим рекомендациям) [10], [25], [26], [27]. 2. Информирование о КИ: − Курирующий ОИВ, ДИТ, (при необходимости поставщиков услуг (подрядчиков), ЦОД, и внешних организаций и т.д.) в установленном Порядке [18]. − НКЦКИ о КИ, связанных с ЗОКИИ, включая КИ с ПДн не позднее 3 часов с момента его обнаружения [7], [10], [11]. − НКЦКИ о КИ, связанных с НОКИИ, включая КИ с ПДн не позднее 24 часов с момента его обнаружения [7], [10], [11]. − Роскомнадзор о КИ с ПДн не позднее 24 часов с момента его обнаружения (первичное уведомление) [13]. 3. Реагирование на КИ: 4. Определение вовлеченных в КИ элементов информационной инфраструктуры [10], [25], [26], [27]. 5. Определение очередности реагирования на КИ, исходя из оценки уровня влияния КИ и приоритета [10], [25], [26], [27]. 6. Локализация КИ [10], [25], [26], [27]. 7. Выявление последствий КИ [10], [25], [26], [27]. 8. Ликвидация последствий КИ [10], [25], [26], [27].

**1.4. Раздел 4. Подразделения и должностные лица, ответственные за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА**.

Субъектом КИИ определяются подразделения и (или) должностные лица (должностное лицо), ответственные за проведение мероприятий по реагированию на КИ, связанные с функционированием ЗОКИИ. Разрабатывается соответствующий локальный нормативный акт об определении (назначении) указанных подразделений и (или) должностных лиц (должностного лица) субъекта КИИ ответственными за данные мероприятия (приложение 4 к настоящим Методическим рекомендациям). В Плане указываются реквизиты акта, в соответствии с которым определены (назначены) подразделения и (или) должностные лица субъекта КИИ. При описании подразделений и должностных лиц, ответственных за проведение мероприятий Плана указываются: − наименования подразделений субъекта КИИ, ответственных за проведение указанных мероприятий; − ФИО, должности, контактные данные, места размещения сотрудников субъекта КИИ и возложенные на них функции по Плану. Описание структуры сил реагирования субъекта КИИ приведено в таблице 2 [6].

**5.5. Раздел 5. Условия привлечения подразделений и должностных лиц ФСБ России.**

Условиями привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА являются следующие: 1. КИ привёл к прекращению функционирования ЗОКИИ. 2. Выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ, связанного с функционированием ЗОКИИ (восстановить штатное функционирование ЗОКИИ). 3. В НКЦКИ направлено сообщение о КИ, связанном с функционированием ЗОКИИ с указанием в нем необходимости привлечения подразделений и должностных лиц ФСБ России и причин, по которым выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ. Алгоритм оценки возможности привлечения подразделений и (или) должностных лиц ФСБ России приведена на рисунке 5

Согласно приведенным разделам необходимо создать План реагирования на компьютерные инциденты для ГК ИННО

# Раздел 1. Технические характеристики и состав ЗОКИИ

|  |  |  |
| --- | --- | --- |
| **Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи** | | |
| 1. | Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или  сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи | Отсутствует взаимодействие ЗОКИИ с сетью связи общего пользования, а также наложенными или  выделенными сетями. Объект расположен локально в пределах инженерного сооружения. |
| 2. | Наименование оператора связи и (или) провайдера хостинга | Отсутствует |
| 3. | Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель) | Отсутствует |
| 4. | Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия | Беспроводной |
| **Сведения о программных и программно-аппаратных средствах,**  **используемых на объекте критической информационной инфраструктуры** | | |
| 1. | Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество | * CA-7200, DIU-N4, СА-ШУЗ, * АРМ 11th Gen Intel(R) Core(TM)   i5-1135G7, 2.40GHz, 1.38 GHz (16 шт.) |
| 2. | Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии) | * Linux, CentOS |
| 3. | Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав  дистрибутивов операционных систем) | * FIRE 1 |
| 4. | Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных  документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты  информации | * Встроенные общесистемные прикладные средства, сертификация и экспертиза средств информации не производилась. |
| * Иные сведения | | |
| 1. | Сведения о наличии средств архивирования и резервного копирования данных | * Бэкап-Сервер |
| 2. | Сведения о подключении ЗОКИИ к корпоративному (ведомственному) центру ГосСОПКА | * С центрами ГосСОПКА не взаимодействует |
| 3. | Сведения об установленных на ЗОКИИ средствах ГосСОПКА | * Средства ГосСОПКА отсутствуют |

## Состав значимого объекта КИИ «Наименование системы»

**«ГК ИННО»**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименовани е элемента значимого объекта КИИ | Сетево е имя | Провайд ер | Доменн ое имя | Внешни й IP-  адрес | Внутренни й IP-адрес | Используем ые протоколы | ОС**5** | ППО6 | Название учетных записей | Лицо, ответствен ное за  эксплуатац ию7 | Лицо,  ответственн ое  за  администри рование | Средства защиты |
| 1. | Сервер №1 | server1 | ISP A | example.com | 203.0.113.10 | 192.168.1.10 | TCP/IP, SSH, HTTP | Linux CentOS 8 | Apache, OpenSSH | admin, user1, user2 | Иван Иванов | Анна Петрова | Firewall, IDS |
| 2. | Рабочая станция отдела маркетинга | marketing-pc | ISP B | marketing.local | 198.51.100.5 | 192.168.0.25 | TCP/IP, SMB | Windows 10 | Microsoft Office | marketing\_user, admin | Елена Сидорова | Павел Николаев | Antivirus, VPN |
| 3. | Маршрутизатор | router | ISP C | - | 192.0.2.1 | 192.168.0.1 | TCP/IP, ICMP | Cisco IOS | - | admin | Алексей Козлов | Ольга Смирнова | ACLs, VPN |
| 4. | Бэкап-сервер | backup | ISP D | backup.local | 198.51.100.20 | 192.168.2.15 | TCP/IP, SSH, FTP | Ubuntu 20.04 LTS | Bacula, OpenSSH | backup\_admin, backup\_user | Мария Попова | Дмитрий Иванов | Backup software, Firewall |
| 5. | Шлюз безопасности | security-gw | ISP E | securenet.local | 203.0.113.50 | 192.168.3.1 | TCP/IP, VPN | pfSense | - | admin | Наталья Кузнецова | Андрей Зайцев | IDS, Firewall, Proxy |

# Раздел 2. События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий

Обнаружение угрозы безопасности.

Обнаружение вторжения в сеть.

Аномальная активность на сетевых устройствах.

Зарегистрированные попытки несанкционированного доступа.

Изменения в системных ресурсах:

Превышение нормативов использования процессора, памяти или сети.

Системные ошибки, приводящие к сбоям в работе.

Обновления и патчи:

Необходимость внедрения критических исправлений для предотвращения известных уязвимостей.

Сигналы от систем мониторинга:

Предупреждения от систем обнаружения вторжений (IDS/IPS).

Алерты от систем мониторинга безопасности и сетевого трафика.

Информация от сотрудников и специалистов:

Сообщения от администраторов о возможных проблемах или инцидентах безопасности.

Отчеты о необычной активности от пользователей.

Достижение предельных значений ресурсов.

Изменения в законодательстве.

Сбои в работе системы.

Обновления и исправления.

Запланированные технические работы.

Изменения в бизнес-процессах.

Замедление, временный сбой или прекращение работы АРМ, сервисов и иных компонентов ЗОКИИ;

Нарушение установленного в организации режима доступа к информации или компонентам ЗОКИИ;

Функционирование ВПО;

Несанкционированное изменение информации на элементах ЗОКИИ;

Превышение допустимой нагрузки на вычислительные ресурсы элементов ЗОКИИ;

Отказ функционирующего на элементах ЗОКИИ программного и аппаратного обеспечения;

Иные нарушения в работе элементов ЗОКИИ, вызывающих прекращение выполнения его целевых функций.

## 2.1 Источники информации о КИ на ЗОКИИ

СЗИ:

Оповещения антивирусного ПО и внутрисистемных компонентов межсетевого экранирования (брандмауэр);

Данные журналов событий ПО АСУ ТП, операционных систем серверов и автоматизированных рабочих мест, систем резервного копирования и других систем;

Оповещения средств автоматического или автоматизированного мониторинга информационной безопасности учреждения;

Оповещения и уведомления СЗИ ЗОКИИ/ОКИИ.

Пользовательские, административные и внешние источники информации:

Сотрудники учреждения, ответственные за ИБ: куратор ИБ, ответственный за ИБ участка, администратор, старший диспетчер, диспетчер (оператор АСУ), начальник дежурной смены, пользователи;

Уведомления или информирование ДИТ;

Уведомления или информирование ФСТЭК России или НКЦКИ о наличии угроз ИБ;

СМИ.

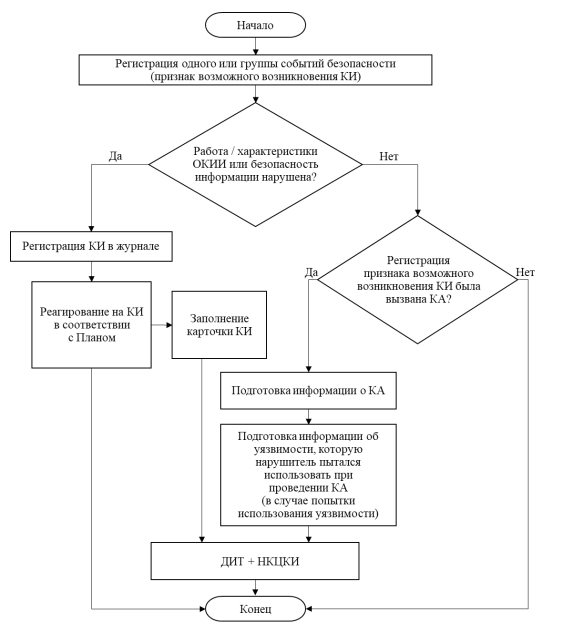


Рисунок 3 – Алгоритм реагирования

# Раздел 3. Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| **1. Обнаружение и регистрация КИ** | | | | | | | | |
| 1.1. | Незамедлительный доклад начальнику дежурной смены о  произошедшем КИ | Устный доклад | Диспетчер (оператор АСУ) | Начальник дежурной смены | Ч + 5 мин. |  |  |  |
| 1.2. | Заполнение карточки КИ | Карточка, распечатанная на бумаге, ручка / АРМ (форма в электронной форме) | Диспетчер (оператор АСУ) | Начальник дежурной смены | Ч + 10 мин. | После выполнения п. 1.1 | В карточку внесена запись о КИ |  |
| 1.3. | Заполнение журнала КИ | Оформленный по  форме журнал, ручка | Диспетчер (оператор АСУ) | Начальник дежурной смены | Ч + 15 мин. | После  выполнения п. 1.2 | В журнал  внесена запись о КИ |  |
| 1.4. | Незамедлительное информирование ответственного лица, уполномоченного предоставлять  сведения о КИ в ДИТ, НКЦКИ о  произошедшем КИ (старшего диспетчера) | Устный доклад | Начальник дежурной смены | Ответственное лицо, уполномоченное предоставлять сведения о КИ в ДИТ, НКЦКИ о  произошедшем КИ Старший  диспетчер службы ИТС | Ч + 10 мин. | После выполнения п. 1.3 |  |  |
| 1.5. | Незамедлительное информирование ответственного за ИБ участка и | Устный доклад | Начальник дежурной смены | Старший диспетчер службы ИТС | Ч + 15 мин. | После выполнения п. 1.4 |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  | администратора о  произошедшем КИ |  |  |  |  |  |  |  |
| 1.6. | Незамедлительное информирование куратора ИБ участка о произошедшем КИ | Устный доклад | Ответственный за ИБ участка | Куратор ИБ | Ч + 20 мин. | После выполнения п. 1.5 |  |  |
| 1.7. | Незамедлительное информирование заместителя руководителя организации по вопросам ИБ о произошедшем КИ | Устный доклад | Куратор ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 25 мин. | После выполнения п. 1.6 |  |  |
| 1.8. | Направление дежурной бригады на место размещения ЗОКИИ для выяснения обстоятельств, приведших к  ошибке/сбою | Служебный транспорт, необходимый инструмент (отвертки, гаечные ключи и т.д.),  дистрибутивы СЗИ, запасное имущество и принадлежности (ЗИП) | Начальник дежурной смены | Куратор ИБ | Ч + 25 мин. | После выполнения п. 1.7 |  | Служебный транспорт |
| **2. Определение вовлеченных в КИ элементов информационной инфраструктуры** | | | | | | | | |
| 2.1. | Сбор сообщений от технических средств | Общесистемное ПО, АВЗ. | Ответственный за ИБ участка | Куратор ИБ | Ч + 25 мин. | После выполнения п. 1.6 |  |  |
| 2.2. | Сбор сообщений от работников, пользователей, | Опрос / получение письменных  объяснений | Куратор ИБ | Заместитель руководителя | Ч + 30 мин. | После выполнения п. 1.7 |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  | привилегированных  пользователей |  |  | организации по  вопросам ИБ |  |  |  |  |
| 2.3. | Сбор доказательств | Журналы регистрации событий, копий жестких дисков и других данных, собранных на предшествующих  этапах и т.п. | Куратор ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 35 мин. | После выполнения п 2.2 |  |  |
| 2.4. | Сбор сведений об уязвимостях, посредством которых были реализованы угрозы ИБ | Сканер уязвимостей | Ответственный за ИБ участка | Куратор ИБ | Ч + 30 мин. | После выполнения п 2.1 | Зафиксирован ное  свидетельство |  |
| 2.5. | Сбор данных,  зафиксированных системами контроля доступа и  видеонаблюдения |  | Ответственный за ИБ участка | Куратор ИБ | Ч + 40 мин. | После выполнения п 2.4 |  |  |
| **3. Определение очередности реагирования на КИ** | | | | | | | | |
| 3.1. | Определение очередности  реагирования на КИ, исходя из оценки уровня влияния КИ и приоритета | Сбор информации по последствиям КИ, определение уровня влияния и приоритетов (по масштабу и по значимости вовлеченных СВТ | Куратор ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 50 мин. | После выполнения п 2.3 | Решение  заместителя руководителя последовател ьности мероприятий по  результатам определения |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  |  |  |  |  |  |  | очередности  реагирования |  |
| **4. Локализация КИ** | | | | | | | | |
| 4.1. | Направление ответственного за ИБ для проведения диагностических  работ по выявлению и локализации КИ | Служебный транспорт,  флеш-накопитель, дистрибутивы СЗИ, образы ПО и т.д. | Ответственный за ИБ участка | Куратор ИБ | Ч + 60 мин. | После выполнения п 2.5 |  |  |
| 4.2. | Отключение пораженных элементов ЗОКИИ |  | Ответственный за ИБ участка | Куратор ИБ | Ч + 60 мин. | После выполнения п 4.1 |  |  |
| 4.3. | Блокировка скомпрометированн ых учетных записей | АРМ | Ответственный за ИБ участка | Куратор ИБ | Ч + 1 ч. 05  мин. | После выполнения п 4.2 |  |  |
| 4.4. | Изъятие съемных носителей | Жесткий диск,  флеш-накопитель | Куратор ИБ | Заместитель руководителя  организации по вопросам ИБ | Ч + 60 мин. | После  выполнения п 3.1 |  |  |
| 4.5. | Визуальный осмотр мест размещения  ЗОКИИ на предмет выявления и фиксации попыток несанкционированн ой установки ПО, установки внешних носителей информации, нарушения  опломбирования, нарушения | ПАК СЗИ для выявления КИ | Ответственный за ИБ участка | Куратор ИБ | Ч + 1 ч. 20  мин. | После выполнения п 4.3 |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  | целостности  кабельной инфраструктуры и иных нарушений информационной безопасности ЗОКИИ/ОКИИ и его  компонентов |  |  |  |  |  |  |  |
| 4.6. | Мониторинг и фиксация попыток несанкционированн ой установки ПО, установки внешних носителей информации и иных действий,  проводимых на оборудовании, АРМ и серверах, входящих в периметр ЗОКИИ/ОКИИ. | ПАК СЗИ для выявления КИ | Ответственный за ИБ участка | Куратор ИБ | Ч + 1 ч. 50  мин. | После выполнения п 4.5 |  |  |
| 4.7. | Передача данных о проведенных  работах по локализации КИ, диспетчеру (оператору АСУ) для дальнейшего информирования  старшего диспетчера, | Устный доклад/ телефон/ электронная почта | Ответственный за ИБ участка | Куратор ИБ | Ч + 2 ч. 30  мин. | После выполнения п 4.6 |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  | куратора ИБ и  заместителя руководителя организации по вопросам ИБ |  |  |  |  |  |  |  |
| 4.8. | Протоколирование действий по  локализации | АРМ | Старший диспетчер | Куратор ИБ | Ч + 2 часа 40 мин. | После выполнения  п 4.7 |  |  |
| **5. Информирование курирующего ОИВ, ДИТ, НКЦКИ, поставщиков услуг (подрядчиков) и внешних организаций** | | | | | | | | |
| 5.1. | Уведомление курирующего ОИВ о КИ | Телефон/ электронная почта | Старший диспетчер | Куратор ИБ | Ч + 30 мин. | После выполнения п. 1.7 |  |  |
| 5.2. | Уведомление ДИТ о КИ  (посредством электронной почты:) | Электронная почта: [dit\_incident@mos.ru](mailto:dit_incident@mos.ru) | Старший диспетчер | Куратор ИБ | Ч + 40 мин. | После выполнения п. 5.1 |  |  |
| 5.3. | Информирование внешних организаций о компрометации ключей электронной подписи | Электронная почта, телефон | Старший диспетчер | Куратор ИБ | Ч + 50 мин. | После выполнения п. 5.2 |  |  |
| 5.4. | Уведомление поставщиков услуг (подрядчиков) | Телефон/ электронная почта | Старший диспетчер | Куратор ИБ | Ч + 60 мин. | После выполнения п. 5.3 |  |  |
| 5.5. | Уведомление НКЦКИ о КИ | Электронная почта:  [incident@cert.gov.ru](mailto:incident@cert.gov.ru) или позвоните по телефону:  +7 (916) 901-07-42. | Старший диспетчер | Куратор ИБ | Ч + 3 ч. | После выполнения п. 4.9 |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| 5.6. | Доведение сведений  о проведенных мероприятиях по информированию куратора ИБ и заместителя руководителя организации по  вопросам ИБ | Личный доклад | Старший  диспетчер | Куратор ИБ | Ч + 3 ч. 10  мин. | После  выполнения п. 5.6 |  |  |
| **6. Выявление последствий КИ** | | | | | | | | |
| 6.1. | Выявление  работоспособности СВТ |  | Ответственный за ИБ участка | Куратор ИБ | Ч + 3 ч. 30  мин. | После выполнения п. 4.7 |  |  |
| 6.2. | Протоколирование выявленных последствий | АРМ | Старший диспетчер | Куратор ИБ | Ч + 4 ч. | После выполнения п. 6.1 | Внесение данных в протокол |  |
| **7. Ликвидация последствий КИ** | | | | | | | | |
| 7.1. | Использование всех возможных мер по восстановлению работоспособности ЗОКИИ | АРМ, загрузка антивируса, обновление ПО и смена скомпрометирован ных паролей, восстановление  данных из резервных копий, удаление  вредоносного кода, восстановление настройки технических  средств, | Ответственный за ИБ участка | Куратор ИБ | Ч + 4 ч. 30  мин. | После выполнения п. 6.1 |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  |  | связанности  элементов ЗОКИИ, Проведение нагрузочного тестирования т.д. |  |  |  |  |  |  |
| 7.2. | Протоколирование действий по ликвидации  последствий КИ | АРМ | Старший диспетчер | Куратор ИБ | Ч + 4 ч. 45  мин. | После выполнения п. 7.1 | Внесение данных в протокол |  |
| 7.3. | Доклад о произведенных работах по ликвидации последствий КИ старшему диспетчеру, куратору ИБ и заместителю руководителя организации по  вопросам ИБ | Личный доклад | Старший диспетчер | Куратор ИБ | Ч + 5 ч. | После выполнения п. 7.2 |  |  |
| **8. Привлечение ФСБ России к ликвидации последствий КИ** | | | | | | | | |
| 8.1. | Решение о привлечении ФСБ России, если  работоспособность ЗОКИИ не  восстановлена | Устное решение | Заместитель руководителя организации по вопросам ИБ |  | Ч + 6 ч. | После выполнения п. 7.3 | Устное решение |  |
| 8.2. | Внесение в журнал отметки об  информировании НКЦКИ о | Журнал, ручка | Старший диспетчер | Куратор ИБ | Ч + 6 ч. 10  мин. | После выполнения п. 8.1 |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  | необходимости  привлечения  должностных лиц ФСБ России |  |  |  |  |  |  |  |
| 8.3. | Направление в НКЦКИ  дополнительных материалов | АРМ, Электронная почта: [incident@cert.gov.ru](mailto:incident@cert.gov.ru) | Старший диспетчер | Куратор ИБ | Ч + 6 ч. 30  мин. | После выполнения п. 8.2 |  |  |
| 8.4. | Получение от НКЦКИ  подтверждения о привлечении ФСБ России | Электронная почта, телефон | Старший диспетчер | Куратор ИБ | Ч + 8 ч. | После выполнения п. 8.3 |  |  |
| 8.5. | Организация взаимодействия с подразделениями и должностными лицами ФСБ России | Пропуск к  ЗОКИИ, АРМ | Куратор ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 10 ч. | После выполнения п. 8.4 |  | Обеспечение прохода на территорию, предоставлен ие  должностным лицам ФСБ России АРМов, и точек входа  для подключения к ЗОКИИ со  служебного ноутбука |
| **9. Закрытие КИ** | | | | | | | | |
| 9.1. | Издание приказа о проведении расследования | Приказ, согласованный и подписанный в | Куратор ИБ | Заместитель руководителя | Ч + 30 ч. | После выполнения п. 8.5 |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  |  | установленном  порядке |  | организации по  вопросам ИБ |  |  |  |  |
| 9.2. | Проведение расследования КИ, выявление причин возникновения и оценивание нанесённого ущерба КИ ЗОКИИ | Просмотр и обработка лог- файлов АРМ, записей видеокамер внутреннего наблюдения, данных СКУД и других имеющихся технических и административных возможностей учреждения, не противоречащих действующему законодательству, изучение объяснительных, служебных записок  от персонала | Ответственный за ИБ участка | Куратор ИБ | Ч + 30 ч. 30  мин. | После выполнения п. 9.1 | Проект акта по результатам проведённого расследовани я КИ,  причины возникновени я, условия и обстоятельст ва КИ |  |
| 9.3. | Информирование заместителя руководителя организации по вопросам ИБ о  проведенном расследовании | Устный доклад | Куратор ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 35 ч. 30  мин. | После выполнения п. 9.2 |  |  |
| 9.4. | Подписание акта по результатам | Оформленный акт | Куратор ИБ | Заместитель руководителя | Ч + 36 ч. | После выполнения п. 9.3 | Подписанный акт по результатам |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  | проведённого  расследования КИ |  |  | организации по  вопросам ИБ |  |  | проведённого  расследовани я КИ |  |
| 9.5. | Информирование ДИТ, ОИВ о  результатах расследования КИ и о нанесенном  ущербе КИ | Электронная почта: [dit\_incident@mos.ru](mailto:dit_incident@mos.ru) | Старший диспетчер | Куратор ИБ | Ч + 36 ч. 20  мин. | После выполнения п. 9.4 |  |  |
| 9.6. | Информирование ЦОДД о закрытии КИ | Электронная почта, телефон | Старший диспетчер | Куратор ИБ | Ч + 36 ч. 50  мин. | После выполнения п. 9.5 |  |  |
| 9.7. | Направление в НКЦКИ результатов расследования КИ | Электронная почта:  [incident@cert.gov.ru](mailto:incident@cert.gov.ru) или позвоните по телефону:  +7 (916) 901-07-42. | Старший диспетчер | Куратор ИБ | Ч + 48 ч. | После выполнения п. 9.6 |  |  |
| 9.8. | Внесение журнал КИ о времени оповещения НКЦКИ о результатах  расследования КИ | Журнал, ручка / АРМ | Диспетчер (оператор АСУ) | Куратор ИБ | Ч + 48 ч. 30  мин. | После выполнения п. 9.7 |  |  |
| **10. Анализ результатов деятельности по управлению КИ [23], [27]** | | | | | | | | |
| 10.1. | Разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения КИ | Рекомендации по принятию  дополнительных мер защиты  информации в соответствии с нормативными правовыми актами | Куратор ИБ, ответственный за ИБ участка / администратор, старший диспетчер,  начальник дежурной смены | Заместитель руководителя организации по вопросам ИБ | Ч + 7 дней | После выполнения п. 9.8 | Рекомендаци и доложены руководителю | При необходимост и по решению руководства |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  |  | и методическими  документами уполномоченных федеральных органов исполнительной власти (ФСБ России и ФСТЭК России), в том числе доработку (актуализацию) и/или разработку документации,  регламентирующей вопросы обеспечения  безопасности организации; рекомендации по повышению защищенности информационных ресурсов от компьютерных атак;  рекомендации по устранению технических причин и условий, способствующих проведению  деструктивного |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  |  | воздействия на  информационные ресурсы. |  |  |  |  |  |  |
| 10.2. | Оценка результатов и эффективности реагирования на КИ, предусмотренная Планом | Оценка  достаточности и эффективности процессов и процедур реагирования на компьютерные инциденты, изложенных в Плане;  предложения по включению в План дополнительных процессов и процедур, которые могли бы повысить эффективность  действий, выполняемых на стадиях  «обнаружение и регистрация КИ» и  «реагирование на КИ»;  предложения по использованию дополнительных  инструментальных средств с целью | Куратор ИБ, ответственный за ИБ участка / администратор, старший диспетчер, начальник дежурной смены | Заместитель руководителя организации по вопросам ИБ | Ч + 10 дней | После выполнения п. 10.1 | Рабочее совещание проведено | При необходимост и по решению руководства |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  |  | повышения  эффективности реагирования и установления причин и условий возникновения КИ; оценка  эффективности обмена  информацией о КИ между всеми сторонами, принимающими участие на стадиях  «обнаружение и регистрация КИ» и  «реагирование на КИ». |  |  |  |  |  |  |
| 10.3. | Внесение изменений в План реагирования на КИ  и принятия мер по ликвидации последствий КА и его утверждение | АРМ, План | Куратор ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 14 дней | После выполнения п. 10.2 |  | При необходимост и по решению руководства |
| 10.4. | Отправка проекта Плана реагирования на КИ и принятия мер по ликвидации последствий КА  на согласование в ФСБ России | Проект Плана, письмо в ФСБ | Куратор ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 16 дней | После выполнения п. 10.3 |  | Если в Плане задействован ы силы ФСБ России |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| 10.5. | Доработка проекта  Плана реагирования на КИ и принятия мер по ликвидации последствий КА с учетом мнения ФСБ России | Проект Плана,  письмо в ФСБ | Куратор ИБ | Заместитель  руководителя организации по вопросам ИБ | Ч + 20 дней | После  выполнения п. 10.4 |  | Если  требуется внести изменения по результатам согласования |
| 10.6. | Утверждение Плана реагирования на КИ и принятия мер по ликвидации  последствий КА | План | Куратор ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 25 дней | После выполнения п. 10.5 |  |  |
| 10.7. | Направление копии измененного Плана реагирования на КИ и принятия мер по ликвидации  последствий КА в НКЦКИ | Копия утвержденного Плана | Куратор ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 32 дня | После выполнения п. 10.6 |  |  |

# Раздел 4. Подразделения и должностные лица, ответственные за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Ответственное лицо (ФИО) / должность** | **Роль** | **Контактные данные** | **Адрес электронной почты** | **Адрес и место размещения (номер кабинета)** | **Реквизиты приказа (распоряжения)** |
| 1. | **Иванов Иван Иванович,**  **руководитель организации** | Возлагает на заместителя руководителя организации полномочия по ИБ  Создает подразделение по ИБ Принимает решение о привлечении подразделений и  должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ | Телефоны:   * рабочий, * мобильный | ххх@mos.ru |  | Приказ (распоряжение) от ХХ.ХХ.ХХХХ  № ХХХ |
| 2. |  | Курирует деятельность по | Телефоны: | ххх@mos.ru |  | Приказ |
|  |  | обеспечению ИБ | - рабочий, |  | (распоряжение) |
|  |  | Взаимодействует с ФСБ России, | - мобильный |  | от |
|  |  | ФСТЭК России, ГосСОПКА |  |  | ХХ.ХХ.ХХХХ |
|  |  | (НКЦКИ), РКН, СМИ, ОИВ, |  |  | № ХХХ |
|  | **Петров Петр Петрович,**  **заместитель руководителя организации по вопросам ИБ** | внешними и отраслевыми регуляторами, ДИТ, поставщиками услуг (подрядчиками), лицензиатами, субъектами КИИ при проведении мероприятий по реагированию на КИ  Информирует руководство о КИ |  |  |  |
|  |  | Руководит структурным |  |  |  |
|  |  | подразделением по ИБ |  |  |  |
|  |  | Получает информацию о КИ на |  |  |  |
|  |  | ЗОКИИ/ОКИИ от начальника |  |  |  |
|  |  | структурного подразделения по ИБ |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Ответственное лицо (ФИО) / должность** | **Роль** | **Контактные данные** | **Адрес электронной почты** | **Адрес и место размещения (номер кабинета)** | **Реквизиты приказа (распоряжения)** |
| 3. |  | Получает информацию о КИ на | Телефоны: | ххх@mos.ru |  | Приказ |
|  |  | ЗОКИИ от ответственного за ИБ. | - рабочий, |  | (распоряжение) |
|  |  | Передаёт поступившую | - мобильный |  | от |
|  |  | информацию заместитель |  |  | ХХ.ХХ.ХХХХ |
|  |  | руководителя организации по |  |  | № ХХХ |
|  |  | вопросам ИБ. Совместно с |  |  |  |
|  |  | Ответственным за ИБ проводит |  |  |  |
|  | **ФИО,** | расследование произошедшего |  |  |  |
|  | **куратор ИБ** | КИ на ЗОКИИ. |  |  |  |
|  |  | Координирует работу и действия |  |  |  |
|  |  | Участников процесса. |  |  |  |
|  |  | Осуществляет выработку |  |  |  |
|  |  | рекомендаций/проведение |  |  |  |
|  |  | мероприятий (совместно с |  |  |  |
|  |  | Ответственным за ИБ) по |  |  |  |
|  |  | недопущении КИ на ЗОКИИ в |  |  |  |
|  |  | будущем. |  |  |  |
| 4. |  | Осуществляет общее руководство | Телефоны: | ххх@mos.ru |  | Приказ |
|  |  | и контроль за действиями | - рабочий, |  | (распоряжение) |
|  | **ФИО,** | дежурной смены во время её | - мобильный |  | от |
|  | **начальник** | дежурства. При потере |  |  | ХХ.ХХ.ХХХХ |
|  | **дежурной** | автоматизированного управления |  |  | № ХХХ |
|  | **смены** | и мониторинга параметров |  |  |  |
|  |  | ЗОКИИ/ОКИИ, направляет |  |  |  |
|  |  | дежурную бригаду для включения |  |  |  |
|  |  | управления в «ручном/местном». |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Ответственное лицо (ФИО) / должность** | **Роль** | **Контактные данные** | **Адрес электронной почты** | **Адрес и место размещения (номер кабинета)** | **Реквизиты приказа (распоряжения)** |
| 5. |  | Получает информацию от | Телефоны: | ххх@mos.ru |  | Приказ |
|  |  | Диспетчера (оператора АСУ) о | - рабочий, |  | (распоряжение) |
|  |  | КИ на ЗОКИИ. Регистрирует КИ в | - мобильный |  | от |
|  |  | общем Журнале КИ. Передаёт |  |  | ХХ.ХХ.ХХХХ |
|  |  | поступившую информацию в |  |  | № ХХХ |
|  | **ФИО,** | НКЦКИ, ДИТ, курирующий ОИВ, |  |  |  |
|  | **старший** | ЦОДД. Получает сообщения, |  |  |  |
|  | **диспетчер** | рекомендации и предписания от |  |  |  |
|  |  | НКЦКИ. Передаёт поступившую |  |  |  |
|  |  | информацию от НКЦКИ |  |  |  |
|  |  | Диспетчеру (оператору АСУ). |  |  |  |
|  |  | Вносит данные о КИ в журнал |  |  |  |
|  |  | учёта КИ. Протоколирование |  |  |  |
|  |  | действий. |  |  |  |
| 6. |  | Фиксирует невозможность | Телефоны: | ххх@mos.ru |  | Приказ |
|  |  | автоматизированного управления, | - рабочий, |  | (распоряжение) |
|  |  | контроля и мониторинга | - мобильный |  | от |
|  |  | параметров ЗОКИИ, в результате |  |  | ХХ.ХХ.ХХХХ |
|  |  | сбоя/неисправности в работе |  |  | № ХХХ |
|  | **ФИО,**  **диспетчер (оператор АСУ)** | ЗОКИИ.  Докладывает о произошедшем начальнику дежурной смены. Заполняет карточку КИ.  Направляет регистрационную |  |  |  |
|  |  | форму КИ Старшему диспетчеру. |  |  |  |
|  |  | Регистрирует КИ в Журнале учёта |  |  |  |
|  |  | КИ. Получает уведомления и |  |  |  |
|  |  | инструкции НКЦКИ от старшего |  |  |  |
|  |  | диспетчера. |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Ответственное лицо (ФИО) / должность** | **Роль** | **Контактные данные** | **Адрес электронной почты** | **Адрес и место размещения (номер кабинета)** | **Реквизиты приказа (распоряжения)** |
|  |  | Участвует в мероприятиях по выявлению и реагированию на КИ ЗОКИИ9. |  |  |  |  |
| 7. |  | Проводит предварительную | Телефоны: | ххх@mos.ru |  | Приказ |
|  |  | проверку состояния ИБ ЗОКИИ. | - рабочий, |  | (распоряжение) |
|  |  | Участвует в мероприятиях по | - мобильный |  | от |
|  |  | реагированию КИ ЗОКИИ. |  |  | ХХ.ХХ.ХХХХ |
|  |  | Передаёт данные о КИ (пункт №4 |  |  | № ХХХ |
|  |  | Карточки КИ), на бумажном |  |  |  |
|  |  | носителе или посредством |  |  |  |
|  |  | служебной электронной почты |  |  |  |
|  | **ФИО,** | Диспетчеру (оператору АСУ). |  |  |  |
|  | **ответственный** | Передаёт информацию о |  |  |  |
|  | **за ИБ участка** | произошедшем КИ старшему |  |  |  |
|  |  | дежурному смены и куратору ИБ. |  |  |  |
|  |  | Выполняет полученные |  |  |  |
|  |  | рекомендации и предписания от |  |  |  |
|  |  | НКЦКИ. Проводит расследование |  |  |  |
|  |  | КИ ЗОКИИ и информирует |  |  |  |
|  |  | куратора ИБ и старшего |  |  |  |
|  |  | диспетчера о результатах |  |  |  |
|  |  | проведённого расследования. |  |  |  |
| 8. | **ФИО,**  **администратор** | Эксплуатирует и администрирует ЗОКИИ. Участвует в мероприятиях по выявлению, реагированию и расследованию КИ ЗОКИИ. | Телефоны:   * рабочий, * мобильный | ххх@mos.ru |  | Приказ (распоряжение) от ХХ.ХХ.ХХХХ  № ХХХ |

# Раздел 5. Условия привлечения подразделений и должностных лиц ФСБ России

Условиями привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА являются следующие: 1. КИ привёл к прекращению функционирования ЗОКИИ. 2. Выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ, связанного с функционированием ЗОКИИ (восстановить штатное функционирование ЗОКИИ). 3. В НКЦКИ направлено сообщение о КИ, связанном с функционированием ЗОКИИ с указанием в нем необходимости привлечения подразделений и должностных лиц ФСБ России и причин, по которым выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ.

Для каждого ЗОКИИ/НОКИИ могут быть добавлены и другие условия, при которых могут привлекаться подразделения и должностные лица ФСБ России. Условиями привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА являются следующие: КИ привёл к прекращению функционирования ЗОКИИ. Выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ, связанного с функционированием ЗОКИИ (восстановить штатное функционирование ЗОКИИ).