|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |
| ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01  Кафедра КБ-4 «Интеллектуальные системы информационной безопасности» | | |
|  |  |  |

Практическая работа 4.2

по дисциплине

«Управление информационной безопасностью»

Группа:

ББМО-02-22

Выполнил:

Шитов А.В.

Проверил:

Пимонов Р.В.

Москва 2023

**Перечень сокращений**

В настоящем документе используются сокращения, приведенные в таблице 1

Таблица 1 – Перечень сокращений

|  |  |
| --- | --- |
| Сокращение | Обозначение |
| АСУ ТП | Автоматизированная система управления технологическим процессом |
| ВПО | Вредоносное программное обеспечение |
| ГосСОПКА | Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации |
| ДИТ | Департамент информационных технологий города Москвы |
| ЗОКИИ | Значимый объект критической информационной инфраструктуры |
| ИБ | Информационная безопасность |
| КА | Компьютерная атака |
| КИ | Компьютерный инцидент |
| КИИ | Критическая информационная инфраструктура Российской Федерации |
| КоАП РФ | Кодекс Российской Федерации об административных правонарушениях |
| Минпромторг России | Министерство промышленности и торговли Российской Федерации |
| Минцифры России | Министерство цифрового развития, связи  и массовых коммуникаций Российской Федерации |
| Минтранс России | Министерство транспорта Российской Федерации |
| Минэнерго России | Министерство энергетики Российской Федерации |
| НКЦКИ | Национальный координационный центр по компьютерным инцидентам |
| НОКИИ | Незначимый объект критической информационной инфраструктуры Российской Федерации |
| ОИВ | Орган исполнительной власти города Москвы |
| Орган (организация) | Органы исполнительной власти города Москвы, подведомственные им государственные учреждения города Москвы, находящиеся в их ведомственном подчинении государственных унитарных предприятий города Москвы |
| ПАК | Программно-аппаратный комплекс |
| План | План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на значимые объекты критической информационной инфраструктуры Российской Федерации |
| Роскомнадзор | Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций |
| РФ | Российская Федерация |

**Нормативные ссылки**

Настоящие Методические рекомендации разработаны с учетом требований законодательства Российской Федерации:

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ;
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
4. Указ Президента Российской Федерации от 01.05.2022 №250

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

1. Постановление Правительства Российской Федерации от 17.02.2018

№ 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

1. Постановление Правительства Российской Федерации от 15.07.2022

№ 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»;

1. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
2. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;
3. Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»
4. Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;
5. Приказ ФСБ России от 13.02.2023 № 77 «Об утверждении Порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных»;
6. Приказ ФСБ России от 11.05.2023 № 213 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими»;
7. Приказ Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных»;
8. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
9. Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;
10. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
11. Постановление Правительства Москвы от 23.12.2021 № 2170-ПП

«Об утверждении Положения о координации деятельности органов исполнительной власти города Москвы и подведомственных им организаций в области обеспечения безопасности информации, обрабатываемой с использованием средств автоматизации, в том числе в информационно- телекоммуникационных сетях»;

1. Распоряжение Департамента информационных технологий города Москвы от 12.09.2022 № 64-16-434/22 «Об утверждении порядка предоставления сведений об инцидентах информационной безопасности»
2. Рекомендации ФСТЭК России по повышению уровня безопасности информационных ресурсов при установлении в Российской Федерации уровней опасности проведения целевых компьютерных атак;
3. Методические рекомендации НКЦКИ по разработке Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации;
4. Методические рекомендации НКЦКИ по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов российской федерации;
5. Инструкция НКЦКИ по формированию электронного письма уведомления о компьютерном инциденте, атаке или уязвимости.
6. Методические рекомендации по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации;
7. ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» утвержден приказом Росстандарта от 29 ноября 2022 года № 1375-ст;
8. ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения» утвержден приказом Росстандарта от 29 ноября 2022 года № 1376-ст;
9. ГОСТ Р 59711-2022 «Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами» утвержден приказом Росстандарта от 29 ноября 2022 года № 1377-ст;
10. ГОСТ Р 59712-2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты» утвержден приказом Росстандарта от 29 ноября 2022 года № 1378-ст.

## План реагирования на КИ и принятия мер по ликвидации последствий КА

**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 | МГТС |
| 3 | Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель) | Взаимодействие с целью оказания услуг |
| 4 | Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия | Проводной |
| **Сведения о программных и программно-аппаратных средствах,**  **используемых на объекте критической информационной инфраструктуры** | | |
| 1 | Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного | * Сервер HPE ProLiant DL380 Gen10, * АРМ 13th Gen Intel Core I5-13600K, 3.5GHz (4 шт) * Cisco C1117-4PLTEEAWA |

|  |  |  |
| --- | --- | --- |
|  | оборудования, средств беспроводного доступа, иных средств) и их количество |  |
| 2 | Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии) | Desktop - Astra Linux Special Edition 1.7.3  Server - Astra Linux Special Edition 1.7.3 |
| 3 | Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав  дистрибутивов операционных систем) | RuBackup, ALD Pro, Rupost, Tantor, Astra Monitoring, Termidesk |
| 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 ФСТЭК, Минцифры, ФСБ. |
| **Иные сведения** | | |
| 1 | Сведения о наличии средств архивирования и резервного копирования данных | RuBackup |
| 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 «ГК Астра»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № 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 | Коммутатор Cisco C1117-4PLTEEAWA | Cisco | МГТС | - | 192.168.14.181 | 10.0.0.1 | tcp, udp, snmp, ssh | Cisco IOS 17.11.1 | - | admin | 7 | 7 | Firewall |
| 2 | Сервер HPE ProLiant DL380 Gen10 | serv | - | - | - | 10.0.0.2 | tcp, udp, ssh | Astra Linux Special Edition 1.7.3 | Tantor | server | 7 | 7 | Встроенные в ядро ОС СЗИ |
| 3 | АРМ | User1 | - | - | - | 10.0.0.3 | tcp, udp | Astra Linux Special Edition 1.7.3 | Libre Office | User1 | 3 | 7 | Встроенные в ядро ОС СЗИ |
| 4 | АРМ | User2 | - | - | - | 10.0.0.4 | tcp, udp | Astra Linux Special Edition 1.7.3 | Libre Office | User2 | 4 | 7 | Встроенные в ядро ОС СЗИ |
| 5 | АРМ | User3 | - | - | - | 10.0.0.5 | tcp, udp | Astra Linux Special Edition 1.7.3 | Libre Office | User3 | 5 | 7 | Встроенные в ядро ОС СЗИ |

5 Операционная система.

6 Прикладное программное обеспечение.

7 Указывается номер строки из Раздела 4 настоящего приложения, в которой содержатся сведения о соответствующем должностном лице.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | АРМ | User4 | - | - | - | 10.0.0.6 | tcp, udp | Astra Linux Special Edition 1.7.3 | Libre Office | User4 | 6 | 7 | Встроенные в ядро СЗИ |

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

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.

## 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.

## 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**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ 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 + Уведомление на рабочую почту | Специалист ИБ | Начальник дежурной смены | Ч + 5 мин. |  | Предоставление доклада и первичной фактуры по КИ |  |
| 1.2. | Заполнение карточки КИ | АРМ (форма в электронной виде) | Специалист ИБ | Начальник дежурной смены | Ч + 10 мин. | После выполнения п. 1.1 | В карточку внесена запись о КИ |  |
| 1.3. | Заполнение журнала  КИ | АРМ (форма в электронном виде) | Специалист ИБ | 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 | Устный доклад | Начальник дежурной смены | Ответственное уполномоченное лицо | Ч + 10 мин. | После выполнения п. 1.3 | Произведено информирование о КИ |  |
| 1.5. | Незамедлительное информирование уполномоченного лица (куратор ИБ) | Устный доклад | Начальник дежурной смены | Куратор ИБ | Ч + 15 мин. | После выполнения п. 1.4 | Произведено информирование о КИ |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| 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 | Произоведено информирование о КИ |  |
| 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 | Произведено информирование о КИ |  |
| 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 | Произведено отправление дежурной бригады на место размещения ЗОКИИ | Служебный транспорт |
| **2. Определение вовлеченных в КИ элементов информационной инфраструктуры** | | | | | | | | |
| 2.1. | Сбор сообщений от технических средств | Общесистемное ПО, Astra Monitoring. | Ответственный  за ИБ участка | Куратор ИБ | Ч + 25 мин. | После выполнения п. 1.6 | Произведён сбор сообщений |  |
| 2.2. | Сбор сообщений от работников, пользователей, | Опрос / получение письменных  объяснений | Куратор ИБ | Заместитель руководителя | Ч + 30 мин. | После выполнения п. 1.7 | Произведён сбор сообщений |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ 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 | Произведён сбор |  |
| 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 | Произведён сбор данных |  |
| **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 | 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 | Произведено направление ответственного за ИБ для диагностики |  |
| 4.2. | Отключение пораженных элементов ЗОКИИ |  | Ответственный  за ИБ участка | Куратор ИБ | Ч + 60 мин. | После выполнения  п 4.1 | Произведено отключение пораженных элементов |  |
| 4.3. | Блокировка скомпрометированн ых учетных записей | АРМ | Ответственный  за ИБ участка | Куратор ИБ | Ч + 1 ч. 05  мин. | После выполнения  п 4.2 | Произведена блокировка скомпроментированных УЗ |  |
| 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 | Произведено изъятие съёмных носителей |  |
| 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 | Произведён визуальный осмотр |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ 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 | Произведён мониторинг и фиксация попыток несанкционнированного доступа |  |
| 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 | Произведена передача данных о произведённых работах по локализации КИ |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ 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 | Диспетчер | Куратор ИБ | Ч + 2 часа 40 мин. | После выполнения  п 4.7 | Произведено протоколирование действий |  |
| **5. Информирование курирующего ОИВ, ДИТ, НКЦКИ, поставщиков услуг (подрядчиков) и внешних организаций** | | | | | | | | |
| 5.1. | Уведомление курирующего ОИВ о КИ | Телефон/ электронная почта | Диспетчер | Куратор ИБ | Ч + 30 мин. | После выполнения п. 1.7 | Произведение уведомление |  |
| 5.2. | Уведомление ДИТ о КИ  (посредством электронной почты: ) | Электронная почта: [dit\_incident@mos.ru](mailto:dit_incident@mos.ru) | Диспетчер | Куратор ИБ | Ч + 40 мин. | После выполнения п. 5.1 | Произведено уведомление |  |
| 5.3. | Информирование внешних организаций о компрометации ключей электронной подписи | Электронная почта, телефон | Диспетчер | Куратор ИБ | Ч + 50 мин. | После выполнения п. 5.2 | Произведено информирование внешних организаций |  |
| 5.4. | Уведомление поставщиков услуг (подрядчиков) | Телефон/ электронная почта | Диспетчер | Куратор ИБ | Ч + 60 мин. | После выполнения п. 5.3 | Произведено уведомление |  |
| 5.5. | Уведомление НКЦКИ о КИ | Электронная почта:  [incident@cert.gov.ru](mailto:incident@cert.gov.ru) или позвоните по телефону:  +7 (916) 515-11-97. | Диспетчер | Куратор ИБ | Ч + 3 ч. | После выполнения п. 4.9 | Произведено уведомление |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ 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 | Диспетчер | Куратор ИБ | Ч + 3 ч. 10  мин. | После  выполнения п. 5.6 | Предоставлены сведения о проведённых мероприятиях |  |
| **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 | Произведено выявление работоспособности |  |
| 6.2. | Протоколирование выявленных последствий | АРМ | 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 | Исполнены меры по восстановлению работоспособности ЗОКИИ |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ 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 | 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 | Диспетчер | Куратор ИБ | Ч + 5 ч. | После выполнения п. 7.2 | Выполнен доклад |  |
| **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 | Диспетчер | Куратор ИБ | Ч + 6 ч. 10  мин. | После выполнения п. 8.1 | Отметка об НКЦКИ внесена в журнал |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ 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) | Диспетчер | Куратор ИБ | Ч + 6 ч. 30  мин. | После выполнения п. 8.2 | Произведено направление дополнительных материалов |  |
| 8.4. | Получение от НКЦКИ  подтверждения о привлечении ФСБ России | Электронная почта, телефон | Диспетчер | Куратор ИБ | Ч + 8 ч. | После выполнения п. 8.3 | Получение подтверждения от НКЦКИ |  |
| 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 | Организовано взаимодействие | 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 организации по  вопросам ИБ | Ч + 30 ч. | После выполнения п. 8.5 | Подготовлен НПА по результатам расследования |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
|  |  | установленном  порядке |  |  |  |  |  |  |
| 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 | Произведено информирование заместителя руководителя организации по вопросам ИБ |  |
| 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) | Диспетчер | Куратор ИБ | Ч + 36 ч. 20  мин. | После выполнения п. 9.4 | Произведено информирование |  |
| 9.6. | Информирование ЦОДД о закрытии КИ | Электронная почта, телефон | Диспетчер | Куратор ИБ | Ч + 36 ч. 50  мин. | После выполнения п. 9.5 | Произведено информирование |  |
| 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) 515-11-97. | Диспетчер | Куратор ИБ | Ч + 48 ч. | После выполнения п. 9.6 | Произведено направление результатов расследования в НКЦКИ |  |
| 9.8. | Внесение журнал КИ  о времени оповещения НКЦКИ о результатах  расследования КИ | Журнал, ручка / АРМ | Диспетчер | Куратор ИБ | Ч + 48 ч. 30  мин. | После выполнения п. 9.7 | Внесено время |  |
| **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 | Рекомендации 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 | Произведено внесение изменений в план реагирования на КИ | 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 | Произведена отправка проекта плана реагирования КИ | 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 | Произведена доработка проекта плана реагирования на КИ | 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 | Произведено утверждение плана реагирования на КИ |  |
| 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 | Направлена копия изменённого плана реагирования на КИ |  |

## 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. | **Дедов Е.М.,**  **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:   * 8 (800) 100-34-50 | dedey@mos.ru | Варшавское ш., 26, Москва | Приказ (распоряжение) от 02.07.2017  № 14 |
| 2. |  | Курирует деятельность по | Телефоны: | pishik78@mos.ru | Варшавское ш., 26, Москва | Приказ |
|  |  | обеспечению ИБ | - 8 (800) 100-34-50 |  | (распоряжение) |
|  |  | ФСТЭК России, ГосСОПКА |  |  | 02.07.2017 |
|  |  | (НКЦКИ), РКН, СМИ, ОИВ, |  |  | № 14 |
|  | **Пищиков Д.А.,**  **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: | pentsova\_12@mos.ru | Варшавское ш., 26, Москва | Приказ |
|  |  | ЗОКИИ от ответственного за ИБ. | - 8 (800) 100-34-50, |  | (распоряжение) |
|  |  | Передаёт поступившую |  |  | 02.07.2017 |
|  |  | информацию заместитель |  |  | № 14 |
|  |  | руководителя организации по |  |  |  |
|  |  | вопросам ИБ. Совместно с |  |  |  |
|  |  | Ответственным за ИБ проводит |  |  |  |
|  | **Пенцов А.С.,** | 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: | pah\_vi9@mos.ru | Варшавское ш., 26, Москва | Приказ |
|  |  | и контроль за действиями | - 8 (800) 100-34-50, |  | (распоряжение) |
|  | **Пахомов В.И.,** | дежурной смены во время её |  |  | от |
|  | **начальник** | дежурства. При потере |  |  | 02.07.2017 |
|  | **дежурной** | автоматизированного управления |  |  | № 14 |
|  | **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: | mumay\_17@mos.ru | Варшавское ш., 26, Москва | Приказ |
|  |  | Диспетчера (оператора АСУ) о | - 8 (800) 100-34-50, |  | (распоряжение) |
|  |  | КИ на ЗОКИИ. Регистрирует КИ в |  |  | от |
|  |  | общем Журнале КИ. Передаёт |  |  | 02.07.2017 |
|  |  | поступившую информацию в |  |  | № 14 |
|  | **Мамаев А.А.,** | НКЦКИ, ДИТ, курирующий ОИВ, |  |  |  |
|  | **диспетчер** | рекомендации и предписания от |  |  |  |
|  |  | НКЦКИ. Передаёт поступившую |  |  |  |
|  |  | информацию от НКЦКИ |  |  |  |
|  |  | Диспетчеру (оператору АСУ). |  |  |  |
|  |  | Вносит данные о КИ в журнал |  |  |  |
|  |  | учёта КИ. Протоколирование |  |  |  |
|  |  | действий. |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ 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. |  |  |  |  |
| 6. |  | Проводит предварительную | Телефоны: | smirna\_98@mos.ru | Варшавское ш., 26, Москва | Приказ |
|  |  | проверку состояния ИБ ЗОКИИ. | - 8 (800) 100-34-50, |  | (распоряжение) |
|  |  | Участвует в мероприятиях по |  |  | от |
|  |  | реагированию КИ ЗОКИИ. |  |  | 02.07.2017 |
|  |  | Передаёт данные о КИ (пункт №4 |  |  | № 14 |
|  |  | Карточки КИ), на бумажном |  |  |  |
|  |  | носителе или посредством |  |  |  |
|  |  | служебной электронной почты |  |  |  |
|  | **Смирнова А.Н.,** | 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. |  |  |  |
| 7. | **Клюев Н.С.,**  **администратор** | Эксплуатирует и администрирует ЗОКИИ. Участвует в мероприятиях по выявлению, реагированию и расследованию КИ ЗОКИИ. | Телефоны:  - 8 (800) 100-34-50, | birdy@mos.ru | Варшавское ш., 26, Москва | Приказ  (распоряжение)  от  02.07.2017  № 14 |

9 Действия проводятся в нерабочее время, выходные и праздничные дни.

## 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:

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).

## Раздел 6. Порядок проведения мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА в отношении ЗОКИИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России

Доклад заместителя руководителя организации по вопросам ИБ Пищикова Д.А. руководству организации Дедов Е.М. о необходимости привлечения подразделений и (или) должностных лиц ФСБ России к проведению мероприятий по реагированию на КИИ и принятию мер по ликвидации последствий КА.

Решение руководителя организации о необходимости привлечения подразделений и должностных лиц ФСБ России.

В течение 30 минут:

Внесение в карточку КИ отметки о привлечении должностных лиц ФСБ России к реагированию на КИ и ликвидации последствий КА (Мамаев А.А., диспетчер). Готовит и направляет в НКЦКИ дополнительные материалы (Мамаев А.А., диспетчер).

Получение от НКЦКИ подтверждения о привлечении ФСБ России.

Заместитель руководителя организации по вопросам ИБ организует взаимодействие с подразделениями и должностными лицами ФСБ России.