

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

----------------------------------------------------------------------------------------------------

Институт кибербезопасности и цифровых технологий

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

----------------------------------------------------------------------------------------------------

**Отчёт по практической работе № 4.2**

По дисциплине

«Управление информационной безопасностью»

Тема: «Управление инцидентами информационной безопасности»

Задание: «Разработка плана реагирования на компьютерные инциденты»

Студент Кузькин Павел Александрович

Группа ББМО-01-22

Работу проверил

Пимонов Р.В.

Москва, 2024

**Список терминов, сокращений и определений**

**Безопасность информации** – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при их обработке в информационных системах.

**Безопасность критической информационной инфраструктуры** – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

**Государственная ликвидации последствий компьютерных атак (ГосСОПКА)** – единый территориально распределенный комплекс, включающий силы и средства, предназначенные последствий инциденты.

**Значимый объект критической инфраструктуры (ЗОКИИ)** – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр информационной инфраструктуры.

**Информация** – сведения (сообщения, данные) независимо от формы их представления.

**Информационная система (ИС)** – совокупность содержащейся в базах данных информации и обеспечивающих её информационных технологий, и технических средств.

**Информационные ресурсы** – информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.

**Категорирование объекта критической информационной инфраструктуры** – установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверка сведений о результатах ее присвоения.

**Компьютерная атака** – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

**Компьютерный инцидент** – факт нарушения и (или) прекращения функционирования объекта инфраструктуры, сети электросвязи, взаимодействия таких объектов, обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

**Критический процесс** – управленческий, производственный, финансово-экономический и (или) иной процесс в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которого может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения безопасности государства и правопорядка.

**Критическая информационная инфраструктура (КИИ)** – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

**Нарушитель безопасности информации** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при их обработке техническими средствами в информационных системах.

**Объекты критической информационной инфраструктуры (ОКИИ)** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

**Субъекты КИИ (субъект КИИ)** – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

**1 Общие положения**

**1.1 Назначение Плана**

Настоящий План реагирования на компьютерные инциденты в ФГПУ «ПИЯФ» НИЦ «Курчатовский институт» предназначен для формирования обоснованных организационных требований к составу и содержанию мероприятий по обеспечению реагирования на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак.

**1.2 Нормативно-правовые акты, методические документы, используемые для оценки угроз безопасности информации и разработки Плана**

1. Положение о Национальном координационном центре по компьютерным инцидентам, утвержденное приказом ФСБ России от 24 июля 2018 г. № 366 "О Национальном координационном центре по компьютерным инцидентам".

2. Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСТЭК России от 6 декабря 2017 г. № 227 "Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации".

3. Приказ ФСБ России от 19.06.2019 № 282 "Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации".

4. Приказ ФСТЭК России от 21.12.2017 года №235 (ред. от 27.03.2019) "Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования".

5. Приказ ФСТЭК России от 22.12.2017 года №236 (ред. от 21.03.2019) "Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий".

6. Приказ ФСТЭК России от 25.12.2017 года №239 (ред. 09.08.2018) (ред. 26.03.2019) "Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ".

7. Базовая модель угроз безопасности персональных данных при обработке, в информационных системах персональных данных (утверждена 15.02.2008 года заместителем директора ФСТЭК России).

8. Информационное сообщение ФСТЭК России от 04.05.2018 года №240/22/2339 "О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ".

9. Информационное сообщение ФСТЭК России от 24.08.2018 года№240/25/3752 "По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий".

10. Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14.02.2008 года заместителем директора ФСТЭК России).

11. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности информации персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 центра ФСБ России 31.03.2015 года № 149/7/2/6-432).

12. Методический документ ФСТЭК России "Методика определения угроз безопасности информации в информационных системах" (проект).

13. Методический документ ФСТЭК России от 11.02.2014 года "Меры защиты информации в государственных информационных системах".

14. Нормативно-методический документ ФСТЭК России от 30.08.2002 года "Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)", Гостехкомиссия России, 2002 год.

15. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 09.02.2005 года № 66 (зарегистрирован Минюстом России 03.03.2005, регистрационный № 6382).

16. Постановление Правительства РФ "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" от 01.11.2012 года № 1119.

17. Постановление Правительства РФ от 17.02.2018 года№162 "Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ".

18. Постановление Правительства РФ от 13.04.2019 года №452 "О внесении изменений в постановление ПП-127 от 08.02.2018".

19. Постановление Правительства РФ от 08.06.2019 года №743 "Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ РФ".

20. Приказ ФСБ России от 06.05.2019 года №196 "Об утверждении требований к средствам ГосСОПКА.

21. Приказ ФСБ России от 19.06.2019 года№281 "Об утверждении Порядка, технических условий установки и эксплуатации средств ГосСОПКА".

22. Федеральный закон от 27.06.2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

23. Федеральный закон от 26.07.2017 года № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

**2 Технические характеристики и состав ЗОКИИ**

Сведенья в данном разделе содержат информацию о текущем состоянии и технических характеристиках инфраструктуры организации ФГПУ «ПИЯФ» НИЦ «Курчатовский институт». В данном разделе указываются следующие сведения: сведения о результатах категорирования ЗОКИИ (сведения о взаимодействии ЗОКИИ и сетей электросвязи, сведения о программных и программно-аппаратных средствах, используемых на ЗОКИИ), сведения о наличии средств архивирования и резервного копирования данных, сведения о подключении ЗОКИИ к корпоративному (ведомственному) центру ГосСОПКА, сведения об установленных на ЗОКИИ средствах ГосСОПКА, сведения о составе ЗОКИИ (см. табл. 1 и 2).

Таблица 1 - Технические характеристики ЗОКИИ ФГПУ «ПИЯФ» НИЦ «Курчатовский институт»

|  |  |
| --- | --- |
| Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи | |
| 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 | Подключение к сети общего пользования для взаимодействия с сетью Интернет и клиентами Организации, также выделенная и локальная сети для организации внутренней инфраструктуры. |
| Наименование оператора связи и (или)  провайдера хостинга | ПАО “Ростелеком” |
| Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель) | Контроль за технологическим, производственным оборудованием |
| 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 | |
| Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество | - [[DELL T630 16SFF 2xE5-2603v3 32GB](https://market.yandex.ru/product--server-dell-t630-16sff-2xe5-2603v3-32gb-h730/37974673?show-uid=17048817085029766219416011&context=search&uniqueId=37240046&resale_goods=resale_resale&resale_goods_condition=resale_excellent&sku=102571551451&cpc=8DklTICcZZsItNUk8Cok9pX4Qt4wSChp7hCTsBJE75FoW3wveBuSKDRYMbJZsydEuG0wRvGc2fGhwj8B8AZDPdAmsZnlmJAztdeUnKFeRUfulP7-huyW-68oHzAWQvlx6YGdAQDDLNHlOdt3oNTfIvBCrX15AhklWT_WopxGVB8Yc9JtoS5KYx4Xukzk6hQHuayMarJjlfvsIAcI9YQU3NVblnmKWdTuKYb4GU0sYDqLbIazSr2ncp5FIilRCjgoTEMbiIJC8EpGqZCatpE1Bw%2C%2C&do-waremd5=HG6P5D_JsRJ2wNXt2jG1vQ&rs=eJwdUD1rAkEUvDNVyC8QETatjWgXPWGxCtiovXCVlYW9RRYTJCBY2dmstRG0sFFD1kL_wGEhFi5-YGmKiNjlZpphmHlv5u2mmw9Fd-k6opoL0ZSzIcqTB2U_AwaZEG2Hyi9cO4Qu38DFArrzCVSxOZQit85Q_BG4moLbBN0ulTW4KgBNCb3imfkfcM0KXE6I9ZcQ9Z18DNR_vKHxA36EK1LUK0wYMPkVmf6Ntz2Cy3eg9uBqF9xJ8s420vwWJs2VdwbM4Rt1j738AfVFfcOZLbbMgVuCevwbM3nOR9j4xPY-56P8nx3areKW5G9c0GJr2X_EO4ie)](https://market.yandex.ru/product--server-hp-dl80-gen9-8lff-2xe5-2609v3-32gb-b140i/37979013?show-uid=17048817085029766219416009&context=search&uniqueId=37240046&resale_goods=resale_resale&resale_goods_condition=resale_excellent&sku=102571552019&cpc=8DklTICcZZud_s4DBeFXdLR2iTH2b8vmpi0zHEPmRe2zD4_YGxV5yCe83q75hpslNNqOhkdL5h9OPCqTsUFXHknNjTbWACVmLjHDliGCSk8n7xm6f4uKw-3Mbm9RNimud2ay_aXewltxBhiVvdi5bYWxhWs9oXnfIIuPhelhugxEts5_nS03UcTUNvWzf4yHz6xMAmAn3fIKJ5wnjVVJY2LAtcpdVZFdB3wC3OTq4VC-Rjb5RaMnWGbPWGFjSQ_q04Ds4qXOfO48ZAZDAWRMNQ%2C%2C&do-waremd5=DenQSNyZI3YTbP1FpTAf1w&rs=eJwdUD1rAkEUvDNVyC8QETatjWgXPWGxCtiovXCVlYW9RRYTJCBY2dmstRG0sFFD1kL_wGEhFi5-YGmKiNjlZpphmHlv5u2mmw9Fd-k6opoL0ZSzIcqTB2U_AwaZEG2Hyi9cO4Qu38DFArrzCVSxOZQit85Q_BG4moLbBN0ulTW4KgBNCb3imfkfcM0KXE6I9ZcQ9Z18DNR_vKHxA36EK1LUK0wYMPkVmf6Ntz2Cy3eg9uBqF9xJ8s420vwWJs2VdwbM4Rt1j738AfVFfcOZLbbMgVuCevwbM3nOR9j4xPY-56P8nx3areKW5G9c0GJr2X_EO4ie) (1 шт.)  - [HP DL80 Gen9 8LFF 2xE5-2609v3 32GB, B140i](https://market.yandex.ru/product--server-hp-dl80-gen9-8lff-2xe5-2609v3-32gb-b140i/37979013?show-uid=17048817085029766219416009&context=search&uniqueId=37240046&resale_goods=resale_resale&resale_goods_condition=resale_excellent&sku=102571552019&cpc=8DklTICcZZud_s4DBeFXdLR2iTH2b8vmpi0zHEPmRe2zD4_YGxV5yCe83q75hpslNNqOhkdL5h9OPCqTsUFXHknNjTbWACVmLjHDliGCSk8n7xm6f4uKw-3Mbm9RNimud2ay_aXewltxBhiVvdi5bYWxhWs9oXnfIIuPhelhugxEts5_nS03UcTUNvWzf4yHz6xMAmAn3fIKJ5wnjVVJY2LAtcpdVZFdB3wC3OTq4VC-Rjb5RaMnWGbPWGFjSQ_q04Ds4qXOfO48ZAZDAWRMNQ%2C%2C&do-waremd5=DenQSNyZI3YTbP1FpTAf1w&rs=eJwdUD1rAkEUvDNVyC8QETatjWgXPWGxCtiovXCVlYW9RRYTJCBY2dmstRG0sFFD1kL_wGEhFi5-YGmKiNjlZpphmHlv5u2mmw9Fd-k6opoL0ZSzIcqTB2U_AwaZEG2Hyi9cO4Qu38DFArrzCVSxOZQit85Q_BG4moLbBN0ulTW4KgBNCb3imfkfcM0KXE6I9ZcQ9Z18DNR_vKHxA36EK1LUK0wYMPkVmf6Ntz2Cy3eg9uBqF9xJ8s420vwWJs2VdwbM4Rt1j738AfVFfcOZLbbMgVuCevwbM3nOR9j4xPY-56P8nx3areKW5G9c0GJr2X_EO4ie) (1 шт.)  - Intel Core i5 10400, LGA 1200, OEM (3 шт.) |
| Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии) | Windows 11 Pro |
| Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем) | MS Office, Google Chrome |
| 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 | |
| Сведения о наличии средств архивирования и резервного копирования данных | Отсутствуют |
| Сведения о подключении ЗОКИИ к корпоративному (ведомственному) центру ГосСОПКА | С центрами ГосСОПКА не взаимодействует |
| Сведения об установленных на ЗОКИИ средствах ГосСОПКА | Средства ГосСОПКА отсутствуют |

Таблица 2 - Состав ЗОКИИ ФГПУ «ПИЯФ» НИЦ «Курчатовский институт»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование элемента значимого объекта КИИ** | **Сетевое имя** | **Провайдер** | **Доменное имя** | **Внешний IP-адрес** | **Внутренний IP-адрес** | **Используемые протоколы** | **ОС** | **ППО** | **Название учетных записей** | **Лицо, ответственное за эксплуатацию** | **Лицо, ответственное за администрирование** | **Средства защиты** |
|  | Коммутатор  HP DL80 Gen9 8LFF | Switch | - | - | - | 172.16.16.1 | tcp, udp, snmp, ssh | - | - | admin | Администратор | Администратор | - |
|  | Сервер [DELL T630 16SFF 2xE5-2603v3 32GB](https://market.yandex.ru/product--server-dell-t630-16sff-2xe5-2603v3-32gb-h730/37974673?show-uid=17048817085029766219416011&context=search&uniqueId=37240046&resale_goods=resale_resale&resale_goods_condition=resale_excellent&sku=102571551451&cpc=8DklTICcZZsItNUk8Cok9pX4Qt4wSChp7hCTsBJE75FoW3wveBuSKDRYMbJZsydEuG0wRvGc2fGhwj8B8AZDPdAmsZnlmJAztdeUnKFeRUfulP7-huyW-68oHzAWQvlx6YGdAQDDLNHlOdt3oNTfIvBCrX15AhklWT_WopxGVB8Yc9JtoS5KYx4Xukzk6hQHuayMarJjlfvsIAcI9YQU3NVblnmKWdTuKYb4GU0sYDqLbIazSr2ncp5FIilRCjgoTEMbiIJC8EpGqZCatpE1Bw%2C%2C&do-waremd5=HG6P5D_JsRJ2wNXt2jG1vQ&rs=eJwdUD1rAkEUvDNVyC8QETatjWgXPWGxCtiovXCVlYW9RRYTJCBY2dmstRG0sFFD1kL_wGEhFi5-YGmKiNjlZpphmHlv5u2mmw9Fd-k6opoL0ZSzIcqTB2U_AwaZEG2Hyi9cO4Qu38DFArrzCVSxOZQit85Q_BG4moLbBN0ulTW4KgBNCb3imfkfcM0KXE6I9ZcQ9Z18DNR_vKHxA36EK1LUK0wYMPkVmf6Ntz2Cy3eg9uBqF9xJ8s420vwWJs2VdwbM4Rt1j738AfVFfcOZLbbMgVuCevwbM3nOR9j4xPY-56P8nx3areKW5G9c0GJr2X_EO4ie) | Server | ПАО “Ростелеком” | - | 192.168.88.26 | 172.16.16.2 | tcp, udp, ssh | - | - | admin | Администратор | Администратор | - |
|  | АРМ | PC1 | - | - | - | 172.16.16.3 | tcp, udp, ssh | Windows 11 Pro | MS Office, Google Chrome | Arm 1 | Пользователь | Администратор | Kaspersky lab |
|  | АРМ | PC2 | - | - | - | 172.16.16.4 | tcp, udp, ssh | Windows 11 Pro | MS Office, Google Chrome | Arm 2 | Пользователь | Администратор | Kaspersky lab |
|  | АРМ | PC3 | - | - | - | 172.16.16.5 | tcp, udp, ssh | Windows 11 Pro | MS Office, Google Chrome | Arm 3 | Пользователь | Администратор | Kaspersky lab |

**3 События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий**

В данном разделе указываются источники информации о КИ на ЗОКИИ (программные и программно-технические средства, пользователи, администраторы, внешние источники).

Среди событий и условий, предусмотренных настоящим стандартом, представлены следующие:

* 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;
* 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, операционных систем серверов и автоматизированных рабочих мест и других систем;
* оповещения средств автоматического или автоматизированного мониторинга информационной безопасности учреждения;
* оповещения и уведомления СЗИ Kaspersky Security Center 3.15.

Пользовательские, административные и внешние источники информации:

* сотрудники учреждения, ответственные за ИБ: администратор ИБ, начальник дежурной смены, диспетчер ИБ, руководитель ИБ, пользователи;
* уведомления или информирование ДИТ;
* уведомления или информирование ФСТЭК России, или НКЦКИ о наличии угроз ИБ.

**4 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** | **Последовательность** | **Результат** | **Примечание** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Обнаружение и регистрация КИ** | | | | | | | | |
|  | Доклад начальнику дежурной смены о КИ | Устный доклад | Диспетчер ИБ | Начальник дежурной смены | Ч + 5 мин. |  | Выполнен доклад |  |
|  | Заполнение карточки КИ | Карточка КИ в электронном виде на АРМ | Диспетчер ИБ | Начальник дежурной смены | Ч + 10 мин. | После выполнения п. 1.1. | Карточка КИ заполнена |  |
|  | Заполнение журнала КИ | Журнал в электронном виде | Диспетчер ИБ | Начальник дежурной смены | Ч + 15 мин. | После выполнения п. 1.2. | Журнал КИ заполнен |  |
|  | Информирование  ответственного лица,  уполномоченного  предоставлять  сведения о КИ в  ДИТ, НКЦКИ | Устный доклад | Начальник дежурной смены | Уполномоченное лицо | Ч + 10 мин. | После выполнения п. 1.3. | Выполнено информирование |  |
|  | Информирование администратора ИБ о КИ | Устный доклад | Начальник дежурной смены | Руководитель ИБ | Ч + 15 мин. | После выполнения п. 1.4. | Выполнено информирование |  |
|  | Информирование руководителя ИБ о КИ | Устный доклад | Администратор ИБ | Начальник дежурной смены | Ч + 20 мин. | После выполнения п. 1.5. | Выполнено информирование |  |
|  | Направление дежурной бригады на место размещения ЗОКИИ для выяснения обстоятельств, приведших к ошибке/сбою | Необходимый инструмент (отвертки, гаечные ключи и т.д.), дистрибутивы СЗИ, запасное имущество и принадлежности (ЗИП) | Начальник дежурной смены | Руководитель ИБ | Ч + 25 мин. | После выполнения п. 1.6. | Выполнено направление на место размещения ЗОКИИ |  |
| 1. **Определение вовлеченных в КИ элементов информационной инфраструктуры** | | | | | | | | |
|  | Сбор сообщений от технических средств | Общесистемное ПО, KSC. | Администратор ИБ | Руководитель ИБ | Ч + 25 мин. | После выполнения п. 1.6. | Выполнен сбор сообщений |  |
|  | Сбор сообщений от работников, пользователей, привилегированных пользователей | Опрос или получение  письменных  объяснений | Администратор ИБ | Руководитель ИБ | Ч + 30 мин. | После выполнения п. 1.7. | Выполнен сбор сообщений |  |
|  | Сбор доказательств | Журналы регистрации событий, копий жестких дисков и других данных, собранных на предшествующих этапах и т.п. | Администратор ИБ | Руководитель ИБ | Ч + 35 мин. | После выполнения п. 2.2. | Выполнен сбор доказательств |  |
|  | Сбор сведений об уязвимостях, посредством которых были реализованы угрозы ИБ | Сканер уязвимостей | Администратор ИБ | Руководитель ИБ | Ч + 30 мин. | После выполнения п. 2.1. | Выполнен сбор сведений об уязвимостях |  |
|  | Сбор данных, зафиксированных системами контроля доступа и видеонаблюдения | Получение данных их хранилища СКУД и видеонаблюдения | Администратор ИБ | Руководитель ИБ | Ч + 40 мин. | После выполнения п. 2.4. | Выполнен сбор данных |  |
| 1. **Определение очередности реагирования на КИ** | | | | | | | | |
|  | Определение очередности реагирования на КИ, исходя из оценки уровня влияния КИ и приоритета | Сбор информации по последствиям КИ, определение уровня влияния и приоритетов | Администратор ИБ | Руководитель ИБ | Ч + 50 мин. | После выполнения п. 2.5. | Выполнено решение последовательности мероприятий реагирования |  |
| 1. **Локализация КИ** | | | | | | | | |
|  | Направление ответственного за ИБ для проведения диагностических работ по выявлению и локализации КИ | Флеш-накопитель, дистрибутивы СЗИ, образы ПО, средства диагностики, и т.д. | Администратор ИБ | Руководитель ИБ | Ч + 60 мин. | После выполнения 2.5. | Выполнено направление для проведения диагностики |  |
|  | Отключение пораженных элементов ЗОКИИ | - | Администратор ИБ | Руководитель ИБ | Ч + 60 мин. | После выполнения 4.1. | Выполнено отключение элементов |  |
|  | Блокировка скомпрометированных учетных записей | АРМ со средством контроля пользователей | Администратор ИБ | Руководитель ИБ | Ч + 1 ч. 05 мин. | После выполнения 4.2. | Выполнена блокировка УЗ |  |
|  | Изъятие съемных носителей | Жесткий диск, флеш-накопитель | Администратор ИБ | Руководитель ИБ | Ч + 60 мин. | После выполнения 4.3. | Выполнено изъятие накопителей |  |
|  | Визуальный осмотр мест размещения ЗОКИИ на предмет выявления и фиксации попыток несанкционированной установки ПО, установки внешних носителей информации, нарушения опломбирования, нарушения целостности кабельной инфраструктуры и иных нарушений информационной безопасности ЗОКИИ/ОКИИ и его компонентов | ПАК СЗИ для выявления КИ | Администратор ИБ | Руководитель ИБ | Ч + 1 ч. 20  мин. | После выполнения 4.4. | Выполнен осмотр |  |
|  | Мониторинг и фиксация попыток несанкционированной 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 | Администратор ИБ | Руководитель ИБ | Ч + 1 ч. 50  мин. | После выполнения 4.5. | Выполнен мониторинг |  |
|  | Передача данных о проведенных работах по локализации КИ | Устный доклад или телефон или электронная почта | Администратор ИБ | Руководитель ИБ | Ч + 2 ч. 30  мин. | После выполнения 4.6. | Выполнена передача данных |  |
|  | Протоколирование действий по локализации | АРМ | Диспетчер ИБ | Руководитель ИБ | Ч + 2 часа 40 мин. | После выполнения 4.7. | Выполнено протоколирование |  |
| 1. **Информирование курирующего ОИВ, ДИТ, НКЦКИ и внешних организаций** | | | | | | | | |
|  | Уведомление курирующего ОИВ о КИ | Телефон или электронная почта | Диспетчер ИБ | Руководитель ИБ | Ч + 30 мин. | После выполнения 1.6. | Выполнено уведомление |  |
|  | Уведомление ДИТ о КИ | Электронная почта: dit\_incident@mos.ru | Диспетчер ИБ | Руководитель ИБ | Ч + 40 мин. | После выполнения 5.1. | Выполнено уведомление |  |
|  | Информирование внешних организаций о компрометации ключей электронной подписи | Электронная почта, телефон | Диспетчер ИБ | Руководитель ИБ | Ч + 50 мин. | После выполнения 5.2. | Выполнено информирование |  |
|  | Уведомление НКЦКИ о КИ | Электронная почта: incident@cert.gov.ru или по телефону: +7 (916) 901-07-42. | Диспетчер ИБ | Руководитель ИБ | Ч + 60 мин. | После выполнения 5.3. | Выполнено уведомление |  |
|  | Доведение сведений о проведенных мероприятиях по информированию до руководителя ИБ | Личный доклад | Диспетчер ИБ | Руководитель ИБ | Ч + 3 ч. | После выполнения п. 5.4. | Сведения предоставлены |  |
| 1. **Выявление последствий КИ** | | | | | | | | |
|  | Выявление работоспособности СВТ |  | Администратор ИБ | Руководитель ИБ | Ч + 3 ч. 30  мин. | После выполнения п. 4.7. | Выявлена работоспособность |  |
|  | Протоколирование выявленных последствий | АРМ | Диспетчер ИБ | Руководитель ИБ | Ч + 4 ч. | После выполнения п. 6.1. | Выполнено протоколирование |  |
| 1. **Ликвидация последствий КИ** | | | | | | | | |
|  | 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, связанности элементов ЗОКИИ, Проведение нагрузочного тестирования т.д | Администратор ИБ | Руководитель ИБ | Ч + 4 ч. 30  мин. | После выполнения п. 6.1. | Выполнены меры по восстановлению |  |
|  | Протоколирование действий по ликвидации последствий КИ | АРМ | Диспетчер ИБ | Руководитель ИБ | Ч + 4 ч. 45  мин. | После выполнения п. 7.1. | Выполнено протоколирование |  |
|  | Доклад о произведенных работах по ликвидации последствий КИ ответственным лицам | Личный доклад | Диспетчер ИБ | Руководитель ИБ | Ч + 5 ч. | После выполнения п. 7.2. | Выполнен доклад |  |
| 1. **Привлечение ФСБ России к ликвидации последствий КИ** | | | | | | | | |
|  | Решение о привлечении ФСБ России, если работоспособность ЗОКИИ не восстановлена | Устное решение | Руководитель ИБ |  | Ч + 6 ч. | После выполнения п. 7.3. | Принято решение |  |
|  | Внесение в журнал отметки об информировании НКЦКИ о необходимости привлечения должностных лиц ФСБ России | Журнал, ручка | Диспетчер ИБ | Руководитель ИБ | Ч + 6 ч. 10  мин. | После выполнения п. 8.1. | Выполнено внесение отметки в журнал |  |
|  | Направление в НКЦКИ дополнительных материалов | АРМ, Электронная почта: incident@cert.gov.ru | Диспетчер ИБ | Руководитель ИБ | Ч + 6 ч. 30  мин. | После выполнения п. 8.2. | Направлены дополнительные материалы |  |
|  | Получение от НКЦКИ подтверждения о привлечении ФСБ России | Электронная почта, телефон | Диспетчер ИБ | Руководитель ИБ | Ч + 8 ч. | После выполнения п. 8.3. | Получено подтверждение |  |
|  | Организация взаимодействия с подразделениями и должностными лицами ФСБ России | Пропуск к ЗОКИИ, АРМ | Руководитель ИБ |  | Ч + 10 ч. | После выполнения п. 8.4. | Организовано взаимодействие |  |
| 1. **Закрытие КИ** | | | | | | | | |
|  | Издание приказа о проведении расследования | Приказ, согласованный и подписанный в установленном порядке | Руководитель ИБ |  | Ч + 30 ч. | После выполнения п. 8.5. | Приказ издан |  |
|  | Проведение расследования КИ, выявление причин возникновения и оценивание нанесённого ущерба КИ ЗОКИИ | Просмотр и обработка логфайлов АРМ, записей видеокамер внутреннего наблюдения, данных СКУД и других имеющихся технических и административных возможностей учреждения, не противоречащих действующему законодательств, изучение объяснительных, служебных записок от персонала | Администратор ИБ | Руководитель ИБ | Ч + 30 ч. 30  мин. | После выполнения п. 9.1. | Проведено расследование и подготовлен акт по его результатам |  |
|  | Информирование руководителя ИБ о проведенном расследовании | Устный доклад | Администратор ИБ | Руководитель ИБ | Ч + 35 ч. 30  мин. | После выполнения п. 9.2. | Выполнено информирование |  |
|  | Подписание акта по результатам проведённого расследования КИ | Оформленный акт | Администратор ИБ | Руководитель ИБ | Ч + 36 ч. | После выполнения п. 9.3. | Подписан акт |  |
|  | Информирование ДИТ, ОИВ о результатах расследования КИ и о нанесенном ущербе КИ | Электронная почта: dit\_incident@mos.ru | Диспетчер ИБ | Руководитель ИБ | Ч + 36 ч. 20  мин. | После выполнения п. 9.4. | Выполнено информирование |  |
|  | Информирование ЦОДД о закрытии КИ | Электронная почта, телефон | Диспетчер ИБ | Руководитель ИБ | Ч + 36 ч. 50  мин. | После выполнения п. 9.5. | Выполнено информирование |  |
|  | Направление в НКЦКИ результатов расследования КИ | Электронная почта: incident@cert.gov.ru или по телефону: +7 (916) 901-07-42 | Диспетчер ИБ | Руководитель ИБ | Ч + 48 ч. | После выполнения п. 9.6. | Выполнено направление результатов |  |
|  | Внесение журнал КИ о времени оповещения НКЦКИ о результатах расследования КИ | АРМ | Диспетчер ИБ | Руководитель ИБ | Ч + 48 ч. 30  мин. | После выполнения п. 9.7. | Время внесено в журнал |  |
| 1. **Анализ результатов деятельности по управлению КИ** | | | | | | | | |
|  | 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 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 воздействия на информационные ресурсы. | Руководитель ИБ, Администратор ИБ, Диспетчер ИБ, Начальник дежурной смены | Руководитель ИБ | Ч + 7 дней | После выполнения п. 9.8. | Рекомендации |  |
|  | 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 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» | Руководитель ИБ, Администратор ИБ, Диспетчер ИБ, Начальник дежурной смены | Руководитель ИБ | Ч + 10 дней | После выполнения п. 10.1. | Выполнена оценка результатов |  |
|  | Внесение изменений в План реагирования на КИ и принятия мер по ликвидации последствий КА и его утверждение | АРМ, План | Руководитель ИБ |  | Ч + 14 дней | После выполнения п. 10.2. | Выполнено внесение изменений | При необходимости |
|  | Отправка проекта Плана реагирования на КИ и принятия мер по ликвидации последствий КА на согласование в ФСБ России | Проект Плана, письмо в ФСБ | Руководитель ИБ |  | Ч + 16 дней | После выполнения п. 10.3. | План отправлен | При задействовании сил ФСБ |
|  | Доработка проекта Плана реагирования на КИ и принятия мер по ликвидации последствий КА с учетом мнения ФСБ России | Проект Плана, письмо в ФСБ | Руководитель ИБ |  | Ч + 20 дней | После выполнения п. 10.4. | Выполнена доработка | При необходимости внесения изменений |
|  | Утверждение Плана реагирования на КИ и принятия мер по ликвидации последствий КА | План | Руководитель ИБ |  | Ч + 25 дней | После выполнения п. 10.5. | План утвержден |  |

**5 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) |
|  | Ответственный\_1, руководитель организации | Создает подразделение по ИБ;  Принимает решение о привлечении подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ | Телефоны:  89XXXXXXXX1 | otv\_1@mos.ru | Адрес и место размещения (номер кабинета) № 1 | Приказ (распоряжение) от XX.XX.XXXX № 1 |
|  | Ответственный\_2, Руководитель ИБ | Курирует деятельность по обеспечению ИБ;  Взаимодействует с ФСБ России, ФСТЭК России, ГосСОПКА (НКЦКИ), РКН, СМИ, ОИВ, 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;  Координирует работу и действия Участников процесса. Осуществляет выработку рекомендаций/проведение мероприятий по недопущении КИ на ЗОКИИ в будущем. | Телефоны:  89XXXXXXXX2 | otv\_2@mos.ru | Адрес и место размещения (номер кабинета) № 2 | Приказ (распоряжение) от XX.XX.XXXX № 2 |
|  | Ответственный\_3, начальник дежурной смены | Осуществляет общее руководство и контроль за действиями дежурной смены во время её дежурства. При потере автоматизированного управления и мониторинга параметров ЗОКИИ/ОКИИ, направляет дежурную бригаду для включения управления в «ручном/местном» | Телефоны:  89XXXXXXXX3 | otv\_3@mos.ru | Адрес и место размещения (номер кабинета) № 3 | Приказ (распоряжение) от XX.XX.XXXX № 3 |
|  | Ответственный\_4, диспетчер ИБ | Регистрирует КИ в общем Журнале КИ;  Передаёт поступившую информацию в НКЦКИ, ДИТ, курирующий ОИВ, ЦОДД;  Получает сообщения, рекомендации и предписания от НКЦКИ;  Вносит данные о КИ в журнал учёта КИ;  Протоколирование действий;  Фиксирует невозможность автоматизированного управления, контроля и мониторинга параметров ЗОКИИ, в результате сбоя/неисправности в работе ЗОКИИ;  Докладывает о произошедшем начальнику дежурной смены;  Заполняет карточку КИ. | Телефоны:  89XXXXXXXX4 | otv\_4@mos.ru | Адрес и место размещения (номер кабинета) № 4 | Приказ (распоряжение) от XX.XX.XXXX № 4 |
|  | Ответственный\_5, администратор ИБ | Проводит предварительную проверку состояния ИБ ЗОКИИ;  Участвует в мероприятиях по реагированию КИ ЗОКИИ;  Передаёт данные о КИ (пункт №4 Карточки КИ), на бумажном носителе или посредством служебной электронной почты Диспетчеру ИБ; Передаёт информацию о произошедшем КИ старшему дежурному смены и куратору ИБ;  Выполняет полученные рекомендации и предписания от НКЦКИ;  Проводит расследование КИ ЗОКИИ; | Телефоны:  89XXXXXXXX5 | otv\_5@mos.ru | Адрес и место размещения (номер кабинета) № 5 | Приказ (распоряжение) от XX.XX.XXXX № 5 |
|  | Ответственный\_6, системный администратор | Эксплуатирует и администрирует ЗОКИИ;  Участвует в мероприятиях по выявлению, реагированию и расследованию КИ ЗОКИИ. | Телефоны:  89XXXXXXXX6 | otv\_6@mos.ru | Адрес и место размещения (номер кабинета) № 6 | Приказ (распоряжение) от XX.XX.XXXX № 6 |

**6 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).

**7 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 руководителя ИБ (Ответственный\_2) руководству организации (Ответственный\_1) 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 (Ответственный\_4, диспетчер ИБ).
* готовит и направляет в НКЦКИ дополнительные материалы (Ответственный\_4, диспетчер ИБ).
* получение от НКЦКИ подтверждения о привлечении ФСБ России.
* руководитель ИБ организует взаимодействие с подразделениями и должностными лицами ФСБ России.