

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 №2**

по дисциплине: «Управление информационной безопасностью»   
На тему:

«План реагирования на компьютерные инциденты»

Группа:

ББМО-01-22

Выполнил:

Гребенник Г.С

Проверил:

Пимонов Р.В.

Москва, 2023

**Содержание**

[**Нормативно-правовое обеспечение** 3](#_Toc156670594)

[**План реагирования на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак** 5](#_Toc156670595)

[**1.** **Технические характеристики и состав ЗОКИИ** 5](#_Toc156670596)

[- L3 КОММУТАТОР HPE ARUBA 2930F (1) 5](#_Toc156670597)

[- МЭ CHECK POINT SMART-1 210 (2) 5](#_Toc156670598)

[**1.1Состав значимого объекта КИИ «АО Россети»** 7](#_Toc156670599)

[**2.** **События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий** 10](#_Toc156670600)

[**2.1** **Источники информации о КИ на ЗОКИИ** 10](#_Toc156670601)

[**3.**  **Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию** 12](#_Toc156670602)

[**4. Подразделения и должностные лица, ответственные за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА** 28](#_Toc156670603)

[**5. Условия привлечения подразделений и должностных лиц ФСБ России** 31](#_Toc156670604)

[**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** 31](#_Toc156670605)

# **Нормативно-правовое обеспечение**

Настоящий документ составлен в соответствии с следующими действующими нормативно-правовыми требованиями законодательства Российской Федерации.

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
2. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
3. Федеральный закон от 26.07.2017 года № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".
4. постановление Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
6. 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";
7. 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".
8. 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".
9. 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»;
10. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
11. 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".
12. Постановление Правительства РФ от 17.02.2018 года№162 "Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ".
13. 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".
14. Приказ ФСБ России от 06.05.2019 года №196 "Об утверждении требований к средствам ГосСОПКА.
15. Приказ ФСБ России от 19.06.2019 года№281 "Об утверждении Порядка, технических условий установки и эксплуатации средств ГосСОПКА".

# **План реагирования на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак**

## **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 | Выделенная сеть электросвязи, присоединенная к сети связи общего пользования |
| 2. | Наименование оператора связи и (или) провайдера хостинга | ПАО «Ростелеком» |
| 3. | Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель) | Оказание услуг клиентским организациям. |
| 4. | Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия | Проводной и 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 | - Aquarius PC на базе Intel core i5 12400 3.2 GHz. (2)  - AMD ATHLON 200GE with Radeon Vega Graphics 3.20 GHz (3)  - Коммутатор Cisco CATALYST 2960 (2)  - HP Proliant DL380p Gen8 (4) - L3 КОММУТАТОР HPE ARUBA 2930F (1)- МЭ CHECK POINT SMART-1 210 (2) |
| 2. | Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии) | * Windows 8 pro * AstaLinux * Linux - RouterOS v.X.X.X * SwitchOS v.X.X.X |
| 3. | Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав  дистрибутивов операционных систем) | * FIRE 1 * Adobe Illustrator * КриптоПРО * Континент АП * Соболь |
| 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 | * Kaspersky * МЭ CHECK POINT SMART-1 210 |
| Иные сведения | | |
| 1. | Сведения о наличии средств архивирования и резервного копирования данных | * Сервер резервного копирования, подключенный к выделенному сегменту хранения данных с RAID конфигурацией и дублированием оборудования, резервное копирование состояния систем и данных выполняется каждые 24 часа. |
| 2. | Сведения о подключении ЗОКИИ к корпоративному (ведомственному) центру ГосСОПКА | * Взаимодействует с центром ГосСОПКА |
| 3. | Сведения об установленных на ЗОКИИ средствах ГосСОПКА | * Взаимодействие с ГосСОПКА осуществляется при помощи установленной инфраструктуры |

### **1.1Состав значимого объекта КИИ «АО Россети»**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | 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 |
| 1. | Коммутатор Cisco CATALYST 2960 | Switch\_dmz | ПАО "Ростелеком" | - | 165.124.198.54 | 10.137.1.1 | tcp, udp, snmp, ssh http, https, smtp. Ldap. | Cisco IOS XE | - | dzm | Ведущий сетевой инженер | Ведущий сетевой инженер | Встроенные в общесистемное ПО алгоритмы и средства. Отделение в DMZ.  Межсетевой экран Check Point. |
| 2. | Коммутатор HPE ARUBA 2930F | Switch\_route | - | - | - | 10.137.54.2 | tcp, udp, ssh snmp, Ldap, telnet | ОС  WC.16.08.0019 | - | L3\_mage | Ведущий сетевой инженер | Ведущий сетевой инженер | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point. |
| 3. | Коммутатор Cisco CATALYST 2960 | Switch\_adm | - | - | - | 10.137.24.1 | tcp, udp, snmp, ssh http, https, smtp. Ldap. | Cisco IOS XE | - | Adm | Системный администратор | Системный администратор | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point. |
| 4. | Сервер HP Proliant DL380p Gen8 | Srv\_main | - | - | - | 10.137.198.1 | tcp, udp, ssh, http, https | Windows server 2016 | Active Directory | Adm, user\_1, user\_2 | Системный администратор | Системный администратор | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point.  Kaspersky |
| 5. | Сервер HP Proliant DL380p Gen8 | Srv\_prox | - | - | - | 10.137.198.2 | tcp, udp, ssh, http, https | Windows server 2016 | - | Adm, user\_1, user\_2 | Системный администратор | Системный администратор | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point.  Kaspersky |
| 6. | Сервер HP Proliant DL380p Gen8 | Srv\_backup | - | - | - | 10.137.198.252 | tcp, udp, ssh, http, https | Windows server 2016 | - | Adm, user\_1, user\_2 | Системный администратор | Системный администратор | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point.  Kaspersky |
| 7. | Сервер HP Proliant DL380p Gen8 | Srv\_1 | - | - | - | 10.137.198.4 | tcp, udp, ssh, http, https | Windows server 2016 | - | Adm, user\_1, user\_2 | Системный администратор | Системный администратор | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point.  Kaspersky |
| 8. | Aquarius PC на базе Intel core i5 12400 3.2 GHz. | User\_arm1 | - | - | - | 10.140.165.1 | tcp, udp, ssh | Windows 8 PRO | - | Admin, user | Системный администратор | Системный администратор | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point.  -Kaspersky |
| 9. | Aquarius PC на базе Intel core i5 12400 3.2 GHz. | User\_arm2 | - | - | - | 10.140.165.2 | tcp, udp, ssh, rdp | Windows 8 PRO | - | Admin, user | Системный администратор | Системный администратор | В-строенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point.  Kaspersky |
| 10. | AMD ATHLON 200GE with Radeon Vega Graphics 3.20 GHz | Adm\_arm1 | - | - | - | 10.140.65.1 | tcp, udp, ssh, rdp | Windows 8 PRO | - | Admin, user | Системный администратор | Системный администратор | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point.  Kaspersky |
| 11. | AMD ATHLON 200GE with Radeon Vega Graphics 3.20 GHz | Adm\_arm2 | - | - | - | 10.140.65.2 | tcp, udp, ssh, rdp | Windows 8 PRO | - | Admin, user | Системный администратор | Системный администратор | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point.  Kaspersky |
| 12. | AMD ATHLON 200GE with Radeon Vega Graphics 3.20 GHz | Adm\_arm3 | - | - | - | 10.140.65.3 | tcp, udp, ssh, rdp | Windows 8 PRO | - | Admin, user | Системный администратор | Системный администратор | Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Check Point.  Kaspersky |

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

* Замедление, временный сбой или прекращение работы АРМ, сервисов и иных компонентов ЗОКИИ (нарушение доступности);
* Нарушение установленного в организации режима доступа к информации или компонентам ЗОКИИ (нарушение конфиденциальности);
* Внедрение ВПО при помощи съемных носителей или путем загрузки из внешней сети (нарушение конфиденциальности, целостности и доступности);
* Несанкционированное изменение информации на элементах хранения данных ЗОКИИ (нарушение целостности);
* Приведение компонентов ЗОКИИ к состоянию «отказ в обслуживании» (нарушение доступности);
* Нарушение штатного функционирования системного и прикладного ПО в результате направленной реализации угроз или в результате ошибок персонала (нарушение доступности);
* Предупреждение системы обряжения вторжений (IDS/IPS);
* Ошибки в результате загрузки и применении обновлений ПО (нарушение доступности)
* Иные виды нарушения в работе ЗОКИИ, приводящих к прекращению выполнения его функций.

### **Источники информации о КИ на ЗОКИИ**

**Информация, поступающая от средств защиты информации:**

* Оповещения центра антивирусного ПО и внутрисистемных компонентов межсетевого экранирования (брандмауэр);
* Данные журналов событий ПО операционных систем серверов и автоматизированных рабочих мест, систем резервного копирования и других систем;
* Оповещения систем мониторинга состояния сетевых ресурсов;
* Оповещения средств автоматического или автоматизированного мониторинга информационной безопасности учреждения;

Отчет результатов резервного копирования средств ЗОКИИ.

**2.2Пользовательские, административные и внешние источники информации:**

* Сотрудники учреждения, ответственные за ИБ: Администратор ИБ, Главный администратор ИБ, диспетчер, старший диспетчер, системный администратор, дежурный, начальник дежурной смены, пользователи;
* Уведомления или информирование ДИТ; Уведомления или информирование ФСТЭК России или НКЦКИ о наличии угроз ИБ.

## **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. | Немедленное уведомление начальнику дежурной смены о возникшем инциденте, о КИ | Устный доклад | Диспетчер поддержи | Начальник дежурной смены | Ч + 5 мин. |  | Доклад озвучен | |  |
| 1.2. | Заполнение карточки КИ | Карточка, распечатанная на бумаге, ручка / АРМ (форма в электронной форме) | Диспетчер поддержи | 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/электронный вид | Старший диспетчер поддержки | Начальник дежурной смены | Ч + 15 мин. | После  выполнения п. 1.2 | В журнал  внесена запись о КИ | |  |
| 1.4. | Немедленное 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 | Ч + 10 мин. | После выполнения п. 1.3 | Информация передана ответственному лицу | |  |
| 1.5. | Незамедлительное информирование ответственного за ИБ участка о КИ | Устный доклад | Начальник дежурной смены | Руководитель ИБ по участку№1 | Ч + 15 мин. | После выполнения п. 1.4 | Информация передана ответственному ИБ участка | |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ 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 | Старший инженер ИБ | Руководитель ИБ | Ч + 20 мин. | После  выполнения п. 1.5 | Информация передана заместителю главного адм. управления ИБ |  |
| 1.7. | Незамедлительное информирование заместителя руководителя  организации по вопросам ИБ о произошедшем КИ | Устный доклад | Ведущий инженер ИБ | Руководитель ИБ | Ч + 25 мин. | После  выполнения п. 1.6 | Информация передана заместителю главного адм. управления ИБ |  |
| 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 | Руководитель ИБ | Ч + 25 мин. | После выполнения п. 1.7 | Выполнено отправление на место размещения ЗОКИИ | Служебный транспорт |
| **2. Определение вовлеченных в КИ элементов информационной инфраструктуры** | | | | | | | | |
| 2.1. | Сбор сообщений от технических средств | Общесистемное ПО, АВЗ. | Старший инженер ИБ | Руководитель ИБ | Ч + 25 мин. | После выполнения п. 1.6 | Информация передана заместителю главного адм. управления ИБ |  |
| 2.2. | Сбор сообщений от работников, пользователей, привилегированных пользователей | Опрос / получение письменных объяснений | Ведущий инженер ИБ | Руководитель ИБ | Ч + 30 мин. | После выполнения п. 1.7 | Информация передана заместителю главного адм. управления ИБ |  |
| 2.3. | 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 | Информация передана главному администратору управления ИБ |  |
| 2.4. | Сбор сведений об уязвимостях, посредством которых были реализованы угрозы ИБ | Сканер уязвимостей | Администратор ИБ | Руководитель ИБ | Ч + 30 мин. | После выполнения п 2.1 | Зафиксирован ное свидетельство |  |
| 2.5. | Сбор данных, зафиксированных системами контроля доступа и видеонаблюдения |  | Администратор ИБ | Руководитель ИБ | Ч + 40 мин. | После выполнения п 2.4 | Собраны сданные о системах контроля доступа и видеонаблюдения |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| **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 | Администратор ИБ | Руководитель ИБ | Ч + 50 мин. | После выполнения п 2.3 | Решение заместителя руководителя последовател ьности мероприятий по результатам определения |  |
| 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 | Администратор ИБ | Руководитель ИБ | Ч + 50 мин. | После выполнения п 2.3 | Решение заместителя руководителя последовател ьности мероприятий по результатам определения очередности реагирования |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| **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. | Администратор ИБ | Руководитель ИБ | Ч + 60 мин. | После  выполнения п 2.5 | Направлен ответственный для проведения диагностики |  |
| 4.2. | Отключение пораженных  элементов ЗОКИИ |  | Администратор ИБ | Руководитель ИБ | Ч + 60 мин. | После  выполнения п 4.1 | Отключены пораженные элементы ЗОКИИ |  |
| 4.3. | Блокировка скомпрометированн ых учетных записей | АРМ | Администратор ИБ | Руководитель ИБ | Ч + 1 ч. 05  мин. | После  выполнения п 4.2 | Заблокированы скомпрометированные УЗ |  |
| 4.4. | Изъятие съемных носителей | Жесткий диск, флеш-накопитель | Администратор ИБ | Руководитель ИБ | Ч + 60 мин. | После выполнения п 3.1 | Изъяты съемные носители |  |
| 4.5. | Визуальный осмотр мест размещения ЗОКИИ на предмет выявления и фиксации попыток несанкционированн ой 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 п 4.3 | Визуальный осмотр зоны размещения ЗОКИИ, выполнен |  |
| 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 | Администратор ИБ | Руководитель ИБ | Ч + 1 ч. 50  мин. | После  выполнения п 4.5 | Осуществлен мониторинг и фиксация попыток несанкционированной установки ПО |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| 4.7. | Передача данных о проведенных работах по локализации КИ, диспетчеру (оператору АСУ) для дальнейшего информирования старшего диспетчера, куратора ИБ и заместителя руководителя организации по вопросам ИБ | Устный доклад/ телефон/  электронная почта | Администратор ИБ | Руководитель ИБ | Ч + 2 ч. 30  мин. | После  выполнения п 4.6 | Осуществлена передача данных о проведенных работах по локализации |  |
| 4.8. | Протоколирование действий по локализации | АРМ | Диспетчер ИБ | Руководитель ИБ | Ч + 2 часа 40 мин. | После  выполнения п 4.7 | Осуществлена передача данных о проведенных работах по локализации |  |
| **5. Информирование курирующего ОИВ, ДИТ, НКЦКИ, поставщиков услуг (подрядчиков) и внешних организаций** | | | | | | | | |
| 5.1. | Уведомление курирующего ОИВ о КИ | +7-916-715-75-74 | Руководитель ИБ | - | Ч + 30 мин. | После  выполнения п. 1.7 | Уведомление передано с помощью телефона и продублировано на корпоративную почту |  |
| 5.2. | Уведомление ДИТ о КИ (посредством электронной почты:) | Электронная почта: [dit\_incident@mos.ru](mailto:dit_incident@mos.ru) | Руководитель ИБ | - | Ч + 40 мин. | После  выполнения п. 5.1 | Уведомление передано с помощью телефона и продублировано на корпоративную почту |  |
| 5.3. | Информирование внешних организаций о компрометации ключей электронной подписи | Электронная почта, телефон  +7-916-715-75-74 | Руководитель ИБ | - | Ч + 50 мин. | После  выполнения п. 5.2 | Осуществлено информирование внешних организаций |  |
| 5.4. | Уведомление поставщиков услуг (подрядчиков) | Lanta@mail.ru | Руководитель ИБ | - | Ч + 60 мин. | После  выполнения п. 5.3 | Уведомление передано НКЦКИ |  |
| 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. | Руководитель ИБ | - | Ч + 3 ч. | После  выполнения п. 4.9 | Уведомление руководителя ИБ |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ъ** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| **6. Выявление последствий КИ** | | | | | | | | |
| 6.1. | Выявление  работоспособности СВТ |  | Ведущий инженер ИБ | Руководитель ИБ | Ч + 3 ч. 30  мин. | После  выполнения п. 4.7 | Выявлена работоспособность |  |
| 6.2. | Протоколирование выявленных последствий | АРМ | Инженер ИБ | Руководитель 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 скомпрометированных паролей, восстановление данных из резервных копий, удаление вредоносного кода, восстановление настройки технических средств, Связанности элементов ЗОКИИ, Проведение нагрузочного тестирования т.д. | Ведущий инженер ИБ | Руководитель ИБ | Ч + 4 ч. 30  мин. | После  выполнения п. 6.1 | Загрузка антивируса,  обновление ПО |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| 7.2. | Протоколирование действий по ликвидации последствий КИ | АРМ | Инженер ИБ | Руководитель 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 | Руководитель ИБ | Ч + 5 ч. | После  выполнения п. 7.2 | Доклад озвучен |  |
| **8. Привлечение ФСБ России к ликвидации последствий КИ** | | | | | | | | |
| 8.1. | Решение о привлечении ФСБ России, если работоспособность ЗОКИИ не восстановлена | Устное решение | Руководитель ИБ | - | Ч + 6 ч. | После  выполнения п. 7.3 | Устное решение |  |
| 8.2. | Внесение в журнал отметки об информировании НКЦКИ о | Журнал, ручка | Руководитель ИБ | - | Ч + 6 ч. 10  мин. | После  выполнения п. 8.1 | Принято решение |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ 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) | Руководитель ИБ | - | Ч + 6 ч. 30  мин. | После  выполнения п. 8.2 | Переданы дополнительные материалы |  |
| 8.4. | Получение от НКЦКИ подтверждения о привлечении ФСБ России | Электронная почта, телефон | Руководитель ИБ | - | Ч + 8 ч. | После  выполнения п. 8.3 | Получено подтверждение о НКЦКИ |  |
| 8.5. | 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 с подразделениями должностными лицами ФСБ России | 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 Установленном порядке | Руководитель ИБ |  | Ч + 30 ч. | После  выполнения п. 8.5 | Приказ создан и издан |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| 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 | Администратор | Руководитель ИБ | Ч + 30 ч. 30  мин. | После  выполнения п. 9.1 | Проект акта по результатам проведённого расследовании я КИ, причины возникновения, условия и обстоятельства КИ |  |
| 9.3. | Информирование заместителя руководителя организации по вопросам ИБ о проведенном расследовании | Устный доклад | Администратор ИБ | - | Ч + 35 ч. 30 мин. | После выполнения п. 9.2 | Информация передана |  |
| 9.4. | Подписание акта по результатам Проведённого расследования КИ | Оформленный акт | Руководитель ИБ | Заместитель руководителя организации по вопросам ИБ | Ч + 36 ч. | После выполнения п. 9.3 | Подписанный акт по результатам Проведённого расследовани я КИ |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| 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) | Руководитель ИБ | - | Ч + 36 ч. 20  мин. | После  выполнения п. 9.4 | Подписанный акт |  |
| 9.6. | Информирование ЦОДД о закрытии КИ | Электронная почта, телефон | Руководитель ИБ | - | Ч + 36 ч. 50  мин. | После выполнения п. 9.5 | Информация передана ДИТ и ОИВ |  |
| 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. | Руководитель ИБ | - | Ч + 48 ч. | После выполнения п. 9.6 | Информация передана ЦОДД |  |
| 9.8. | Внесение журнал КИ о времени оповещения НКЦКИ о результатах расследования КИ | Журнал, ручка / АРМ | Руководитель ИБ | - | Ч + 48 ч. 30  мин. | После  выполнения п. 9.7 | Информация внесена в журнал |  |
| **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 | Руководитель ИБ, Администратор ИБ, Старший системный администратор | 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 воздействия на информационные ресурсы. |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п\п** | **Мероприятие** | **Средства реагирования** | **Силы реагирования** | **Куратор** | **Время выполнения** | **Последоват ельность** | **Результат** | **Примечание** |
| 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 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 | - | 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** |
| 10.3. | 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 | Осуществлено внесение изменений в план реагирования | 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 | Руководитель ИБ | - | Ч + 16 дней | После  выполнения п. 10.3 | Отправлен проект плана реагирования на КИ | Если в Плане задействован ы силы ФСБ России |
| 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 | Руководитель ИБ | - | Ч + 20 дней | После выполнения п. 10.4 | Осуществлена доработка проекта плана реагирования на КИ и приняты меры по ликвидации последствий КА | Если требуется внести изменения по результатам согласования |
| 10.6. | Утверждение Плана реагирования на КИ и принятия мер по ликвидации последствий КА | План | Руководитель ИБ | - | Ч + 25 дней | После  выполнения п. 10.5 | Утвержден план |  |
| 10.7. | Направление копии измененного Плана реагирования на КИ и принятия мер по ликвидации последствий КА в НКЦКИ | Копия утвержденного Плана | Руководитель ИБ | - | Ч + 32 дня | После  выполнения п. 10.6 | Отправлена копия плана с добавленными пунктами |  |

## **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. | **Гребенник Георгий Сергеевич,**  **Руководитель организации** | Делегирует заместителю руководителя организации ответственность за обеспечение информационной безопасности. Формирует структурное подразделение по вопросам информационной безопасности. Принимает решение о привлечении подразделений и должностных лиц ФСБ России для проведения мероприятий по реагированию на инциденты информационной безопасности. | Рабочий Код 5515  Телефон:  88005672654 | greb@rosset.gov.ru |  | Приказ (распоряжение) от 18.01.2024  № 745 |
| 2. | **Защитный Дмитрий Афанасьевич,**  **Главный администратор управления ИБ** | Курирует мероприятия по обеспечению информационной безопасности и взаимодействует с рядом организаций, включая ФСБ России, ФСТЭК России, ГосСОПКА (НКЦКИ), РКН, СМИ, органы внутренних дел (ОИВ), внешних и отраслевых регуляторов, Департамент информационных технологий (ДИТ), поставщиков услуг (подрядчиков), лицензиатов и субъектов контроля и управления информационной безопасностью (КИИ) в ходе реагирования на инциденты информационной безопасности. Регулярно информирует руководство об инцидентах. Осуществляет руководство структурным подразделением по информационной безопасности и получает от начальника этого подразделения информацию о произошедших инцидентах на объекте контроля и управления (ЗОКИИ/ОКИИ). | Телефон:  896745612432 | zash@rosset.gov.ru |  | Приказ (распоряжение) от 18.01.2024  № 745 |
| 3 | **Панкевич Эдуард Евгеньевич,**  **Администратор управления ИБ** | Получает от лица, ответственного за информационную безопасность, информацию о инциденте на объекте контроля и управления (ЗОКИИ). Передает полученные данные главному администратору управления ИБ организации по вопросам информационной безопасности. Совместно с руководителем ИБ по участку №1 проводит расследование случившегося инцидента на ЗОКИИ. Координирует действия всех участников процесса и разрабатывает рекомендации или осуществляет мероприятия для предотвращения подобных инцидентов в будущем. | Телефон:  89153457895 | pank@rosset.gov.ru |  | Приказ (распоряжение) от 18.01.2024  № 745 |
| 4 | **Смотрящий Анатолий Вячеслалович,**  **Старший диспетчер** | Принимает от диспетчера поддержки информацию об инциденте информационной безопасности на объекте контроля и управления (ЗОКИИ). Осуществляет регистрацию инцидента в общем Журнале инцидентов. Передает полученные данные в Национальный киберцентр по компьютерной безопасности и координирующие структуры, такие как Департамент информационных технологий, ответственный за объекты информационно-вычислительной инфраструктуры, и Центр обработки данных и диспетчеризации. Получает сообщения, рекомендации и предписания от НКЦКИ и передает полученную информацию обратно в Журнал учёта инцидентов. Ведет протоколирование совершенных действий. | Телефон:  89997899090 | smotr@rosset.gov.ru |  | Приказ (распоряжение) от 18.01.2024  № 745 |
| 5 | **Трубин Иван Иванович,**  **Системный администратор** | Протоколирует действия выполняемые для устранения проблем, фиксирует проблему, фиксирует невозможность управления автоматизированного контроля и мониторинга параметров ЗОКИИ. Заполняет карту КИ | Телефон:  89541234323 | trub@rosset.gov.ru |  | Приказ (распоряжение) от 18.01.2024  № 745 |
| 6 | **Ехиднов Олег Маратович,**  **Начальник дежурной смены** | Осуществляет общий контроль и руководство над действиями дежурной смены в период ее дежурства. В случае утраты автоматизированного управления и мониторинга параметров объекта контроля и управления ЗОКИИ, направляет дежурную бригаду для активации управления в ручном режиме | Телефон:  8775670990 | exid@rosset.gov.ru |  | Приказ (распоряжение) от 18.01.2024  № 745 |

## **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).
* Инцидент привел к серьезным отклонениям и последствиям покрывающей свою сферу оказания услуг, будь то социальные, экономические, технические и т.д.

В каждом случае для ЗОКИИ/НОКИИ могут быть установлены иные условия, при которых осуществляется привлечение подразделений и должностных лиц ФСБ России.

# **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 главного администратора управления ИБ (Защитный Д.А.) руководителю организации (Гребеннику Г.С.) 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 (Абрамов К.С. Старший системный администратор). Подготовка и направление в НКЦКИ дополнительных материалов (Андреев А.С., Руководитель ИБ).

Получение от НКЦКИ подтверждения о привлечении ФСБ России.

Руководитель ИБ организует взаимодействие с подразделениями и должностными лицами ФСБ России с целью ликвидации последствий КА.