|  |  |
| --- | --- |
|  | УТВЕРЖДЕНАприказом ГКУ НСО ЦСПН Коченевского районаот «28» декабря 2024 г. № 114  |

**Инструкция** **по выявлению компьютерных инцидентов**

**и реагированию на них**

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по выявлению компьютерных инцидентов и реагирование на них, которые должны обеспечивать обнаружение в информационных системах (далее – ИС) ГКУ НСО ЦСПН Коченевского района.

1.2. Контроль за исполнением настоящей Инструкции осуществляет администратор безопасности ИС.

1.3. Серверный сегмент государственных информационных систем Новосибирской области, размещенных в центре обработки данных Новосибирской области, относится к зоне ответственности государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области» (ГБУ НСО «ЦЗИ НСО») и государственного бюджетного учреждения Новосибирской области «Центр информационных технологий Новосибирской области» (ГБУ НСО «ЦИТ НСО») каждого в своей зоне ответственного согласно определенных их функциональных обязанностей. В случае выявления инцидентов на стороне ГКУ НСО ЦСПН Коченевского района вышеуказанные организации обязуются уведомить ГКУ НСО ЦСПН Коченевского района и при необходимости принять участие в проведении расследований по результатам.

1.4. Анализ инцидентов в ГКУ НСО ЦСПН Коченевского района производится с применением следующих средств:

* Система обнаружения и предотвращения вторжений и журналы Dallas Lock;
* Система обнаружения вторжений ViPNet EndPoint Protection;
* Журналы ОС Альт 8 СП;
* Журналы Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Linux.

2. Категории инцидентов информационной безопасности

К инцидентам информационной безопасности в ИС (далее – инциденты ИБ) относятся:

* заражение вредоносным программным обеспечением;
* распространение вредоносного программного обеспечения;
* нарушение или замедление работы ИС;
* несанкционированный доступ в систему;
* нарушение целостности информации, обрабатываемой в ИС.

Инциденты ИБ подразделяются на категории, определенные в таблице 1.

Таблица 1 – Сведения о категориях инцидента ИБ

| **№** | **Наименование категории**  | **Описание категории** |
| --- | --- | --- |
|  | Атаки на веб-сервисы | Сценарии, связанные с атаками на веб-сервисы |
|  | Контроль активности процессов\служб | Сценарии, связанные с работой служб\сервисов\приложений и т.д. |
|  | Контроль антивирусной защиты | Сценарии, связанные с обнаружением вирусов средствами антивирусной защиты и их работоспособности |
|  | Контроль утечек | Сценарии, связанные с фактами утечек информации |
|  | Контроль изменений - конфигурация | Сценарии, связанные с фактами изменения конфигурации систем и сервисов |
|  | Контроль изменений - критичные файлы | Сценарии, связанные с фактами изменения и доступа к файлам\каталогам  |
|  | Контроль сетевого доступа | Сценарии, связанные с сетевыми средствами защиты информации (межсетевые экраны, системы обнаружения вторжений и т.д.) |
|  | Контроль удаленного доступа (VPN) | Сценарии, связанные с работой VPN-решений |
|  | Сетевые атаки | Сценарии, связанные с различными сетевыми атаками на инфраструктуру  |
|  | Контроль идентификации и аутентификации | Сценарии, связанные с идентификацией и аутентификацией пользователей в системах |
|  | Контроль управления доступа  | Сценарии, связанные с фактами изменения\удаления\создания учетных записей |
|  | Контроль уязвимостей | Сценарии, связанные с попытками эксплуатации уязвимостей |
|  | Другое | Все, что не предусмотрено предыдущими категориями |

3. Правила и процедуры мониторинга инцидентов ИБ

3.1. В рамках мониторинга событий администратор безопасности ИС должен осуществлять:

1. наблюдение за событиями ИБ, в т.ч. наблюдение и оценка статистической информации:
	* возникновение событий ИБ с высокой важностью;
	* возникновение определенных категорий/типов событий ИБ;
	* возникновение событий ИБ на определенных сегментах ИС;
	* возникновение событий ИБ в определенные промежутки времени;
	* отсутствие событий ИБ от источников событий ИБ.
2. выявление отклонений как в большую, так и в меньшую сторону (аномалий), а также достижений пороговых значений и/или возникновений отдельно взятых событий ИБ;
3. формирование уведомлений.

3.2. Должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

3.3. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

* предупреждение (сигнализация, индикация) администратора безопасности ИС о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
* реагирование на сбои при регистрации событий безопасности путем изменения администратором безопасности ИС параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов систем, запись поверх устаревших хранимых записей событий безопасности.

3.4. Защита информации о событиях безопасности должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования и в том числе включает защиту средств ведения регистрации и настроек механизмов регистрации событий.

3.5. Доступ к записям аудита и функциям управления механизмами регистрации предоставляться только администратору безопасности ИС.

4. Порядок реагирования на инциденты ИБ

4.1. Выявление инцидентов ИБ

Выявление инцидента ИБ возможно получением информации из следующих источников:

* события ИБ, поступившие с используемых средств защиты информации;
* иная информация о состоянии защищенности;
* обращения работников ГКУ НСО ЦСПН Коченевского района;
* обращения представителей сторонней организации или лица.

После получения информации об инциденте должен зарегистрировать ее в формате карточки инцидента ИБ, включающей:

* уникальный идентификатор;
* название (имя) инцидента ИБ;
* дату и время регистрации инцидента ИБ;
* сведения о том, каким образом обнаружен инцидент ИБ (обращение работника, обращение другая информация о состоянии или техническим средством);
* дополнительную информацию (если она доступна на данный момент (примечания/комментарии)).

Допускается ведение карточки инцидента ИБ в электронном виде.

Далее администратор безопасности ИС должен получить сведения об источнике активности и ее цели (узле, системе, сегменте сети и т.п.), путем анализа событий ИБ, связанных с указанным инцидентом ИБ, и иной информации о состоянии защищенности на предмет наличия в них соответствующих идентификаторов (IP-адрес, имя учетной записи и т.п.) и сопоставления их со справочными данными (диапазоны подсетей, группы пользователей и т.п.). На данном этапе должно происходить дополнение карточки инцидента ИБ сведениями об источнике активности (IP-адрес, сведения о пользователе и т.п.) и сведениями о цели (IP-адрес (диапазон IP-адресов) и т.п.).

Далее должен производиться анализ событий ИБ, действий, произошедших на источнике активности и цели в течение ближайшего времени, поиск признаков, подтверждающих несанкционированность действий, проверка отсутствия отказов/сбоев при регистрации событий ИБ, связанных с указанным инцидентом ИБ, и иной информации о состоянии защищенности. В случае принятия решения о ложном срабатывании должно происходить закрытие инцидента ИБ со статусом «Ложное срабатывание». В ином случае идет процесс реагирование на инцидент ИБ.

4.2. Реагирование на инцидент ИБ

Администратор безопасности ИС обязан принять меры, сдерживающие дальнейшее распространение инцидента. В числе таких мер может быть изоляция скомпрометированных устройств.

Также в ходе сдерживания дальнейшего развития инцидента ИБ необходимо принять меры по фиксированию возможных доказательств для дальнейшего расследования.

4.3. Устранение последствий инцидента ИБ

Обязанности по устранению последствий инцидента ИБ возлагаются на администратора безопасности ИС. Не позднее одного дня с момента наступления инцидента ИБ администратора безопасности ИС должен составить план устранения последствий инцидента ИБ. В данный план необходимо включить:

* общую информацию о произошедшем инциденте ИБ;
* анализ ситуации, оперативные контрмеры, примененные для локализации инцидента ИБ;
* меры, которые необходимо применить для устранения последствий инцидента и восстановления штатной работы ИС;
* определение лиц, ответственных за расследование и установление причин, по которым стало возможным наступление инцидента ИБ;
* определение лиц, ответственных за проведение профилактических мероприятий, разработку и внедрение мер по недопущению повторного наступления инцидента ИБ.

Ответственность за реализацию плана устранения последствий и причин наступления инцидента ИБ лежит на администраторе безопасности ИС. В ходе реализации Плана должны быть приняты меры по устранению последствий инцидента ИБ и восстановление ИС до исходного состояния способами, определяемыми в Плане.

К реализации плана могут привлекаться специалисты ГКУ НСО ЦСПН Коченевского района, ответственные за поддержание технических средств и систем в рабочем состоянии (системные администраторы).

4.4. Проведение расследования инцидента ИБ

Разбирательство и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов:

* нарушение конфиденциальности, целостности и доступности информации;
* халатность и несоблюдение требований по обеспечению безопасности информации;
* несоблюдение условий хранения носителей информации.

Расследование инцидента ИБ может производиться работниками ГКУ НСО ЦСПН Коченевского района (внутреннее расследование) или с привлечением независимых организаций (Лицензиатов ФСТЭК) на основании оформленных договоров.

Задачами расследования являются:

* установление обстоятельств нарушений, приведших к возникновению инцидента ИБ, в том числе времени, места и способа их совершения;
* установление лиц, непосредственно виновных в данных нарушениях;
* выявление причин и условий, способствовавших развитию инцидента.

Обязанность проведения внутреннего расследования возлагается на администратора безопасности ИС. Администратор безопасности ИС должен приступить к работе по расследованию инцидента ИБ не позднее следующего дня после даты выявления инцидента ИБ.

Общая продолжительность внутреннего расследования не должна превышать одного месяца.

Расследование инцидента ИБ должны включать в себя:

* восстановление хронологии событий при инциденте;
* выявление задействованного оборудования, программного обеспечения и инструментов, которые могли использоваться для реализации инцидента ИБ;
* сбор доказательной базы по инциденту;
* установление источника инцидента;
* оценку последствий инцидента ИБ;
* выдачу рекомендаций по предотвращению аналогичных инцидентов ИБ.

Все полученные в ходе расследования материалы подлежат письменному оформлению.

По окончании расследования администратор безопасности ИС должен предоставить директору ГКУ НСО ЦСПН Коченевского района заключение, в котором излагаются:

* основания и время проведения расследования;
* проделанная работа (кратко);
* выявленные нарушения, приведшие к реализации инцидента;
* причины и условия совершения нарушений;
* виновные лица и степень их вины;
* наличие умысла в действиях виновных лиц;
* предложения по возмещению ущерба;
* рекомендации по предотвращению повторного возникновения инцидентов;
* другие вопросы (об актуальности конфиденциальной информации, о размерах ущерба и т.д.).

Материалы расследования подлежат хранению не менее 1 года.

5. Информирование о компьютерных инцидентах уполномоченных органов

5.1. Уведомление о компьютерных атаках на информационные ресурсы Российской Федерации, являющиеся ИС.

5.1.1. Уведомление о компьютерных атаках на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных (далее – инцидент) производится в соответствии с пунктом 12 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

5.1.2. Руководствуясь положениями пункта 3 статьи 21 Федерального закона № 152-ФЗ в случае выявления такого инцидента предпринимаются следующие действия:

5.1.2.1. В течение 24 часов уведомляется уполномоченный орган по защите прав субъектов персональных данных через сервис https://pd.rkn.gov.ru/incidents/form/ с передачей следующих сведений:

* произошедший инцидент,
* предполагаемые причины, повлекшие нарушение прав субъектов персональных данных;
* предполагаемый вред, нанесенный правам субъектов персональных данных;
* о принятых мерах по устранению последствий соответствующего инцидента;
* сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом.

5.1.2.2. В течение 72 часов направляется посредством сервиса https://pd.rkn.gov.ru/incidents/form/ информация о результатах внутреннего расследования выявленного инцидента, а также предоставляются сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5.1.2.3. Направление сведений о расследовании производится с указанием полученного номера и ключа уведомления при регистрации инцидента.

5.1.2.4. Проверить состояние своего уведомления об инциденте можно посредством сервиса https://pd.rkn.gov.ru/incidents/notification\_check/.

6. Ответственность при организации мероприятий по выявлению компьютерных инцидентов и реагированию на них

6.1. Ответственность за организацию мероприятий по выявлению компьютерных инцидентов и реагированию на них в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

6.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_