|  |  |
| --- | --- |
|  | Приложение 21  УТВЕРЖДЕНО  приказом Контрольно-счетной палаты Республики Карелия  от 27.06.2025 № 61 од |

|  |  |  |
| --- | --- | --- |
|  | **ПОЛОЖЕНИЕ**  **по работе с инцидентами информационной безопасности**  **в** **Контрольно-счетной палате Республики Карелия** |  |

1. Общие положения

Настоящее положение по работе с инцидентами безопасности в Контрольно-счетной палате Республики Карелия (далее – Положение) разработано в целях организации работы с инцидентами информационной безопасности в Контрольно-счетной палате Республики Карелия (далее – Контрольно-счетная палата).

Инцидент – одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации, в том числе персональных данных.

Настоящее Положение разработано в соответствии с:

1) Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

2) Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3) Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

4) Требованиями по реализации мер, предусмотренных составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18.02. 2013 № 21;

5) локальными правовыми актами, определяющими политику обработки персональных данных субъектов персональных данных в Контрольно-счетной палате Республики Карелия.

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов и информационных систем.

Работа с инцидентами включает в себя следующие направления:

1) определение лиц, ответственных за выявление инцидентов и реагирование на них;

2) обнаружение, идентификация и регистрация инцидентов;

3) своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе;

4) анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

5) принятие мер по устранению последствий инцидентов;

6) планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий, планирования и принятия мер по предотвращению повторного возникновения инцидентов, приказом Контрольно-счетной палаты назначаются ответственные за выявление инцидентов и реагирование на них.

2. Ответственные за выявление инцидентов и реагирование на них

2.1. В информационных системах.

Ответственными за выявление инцидентов в информационных системах являются:

1) лица, имеющие право доступа к информационным системам;

2) ответственный за техническое обслуживание информационных систем.

Ответственными за реагирование на инциденты в информационных системах являются:

1) лица, имеющих право доступа к информационным системам;

2) ответственный за техническое обслуживание информационных систем;

3) ответственный за организацию обработки персональных данных в Контрольно-счетной палате.

2.2. Вне информационных систем.

Ответственными за выявление инцидентов вне информационных систем являются все должностные лица и иные штатные работники Контрольно-счетной палаты.

Ответственными за реагирование на инциденты вне информационных систем являются:

1) должностные лица и иные штатные работники Контрольно-счетной палаты, обнаружившие инцидент;

2) ответственный за обработку персональных данных в Контрольно-счетной палате, обнаруживший инцидент;

3) ответственный за организацию обработки персональных данных в Контрольно-счетной палате.

3. Обнаружение, идентификация и регистрация инцидентов

3.1. Работа по обнаружению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

1) выявление инцидентов в области информационной безопасности с помощью технических средств;

2) выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

3) выявление инцидентов с помощью должностных лиц и иных штатных работников Контрольно-счетной палаты.

3.2. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до должностных лиц и иных штатных работников Контрольно-счетной палаты информации, позволяющей идентифицировать инциденты.

3.3. Регистрацию инцидентов осуществляет ответственный за техническое обслуживание информационных систем в журнале регистрации инцидентов информационной безопасности. Форма журнала приведена в приложении к настоящему Положению.

Хранение журнала должно осуществляется в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за хранение журнала – ответственный за техническое обслуживание информационных систем.

4. Информирование о возникновении инцидентов

Должностное лицо или иной штатный работник Контрольно-счетной палаты, обнаруживший инцидент в информационной системе, должен незамедлительно, любым доступным способом сообщить об инциденте ответственному за техническое обслуживание информационных систем, ответственному за обработку персональных данных в Контрольно-счетной палате, Председателю Контрольно-счетной палаты.

Ответственный за техническое обслуживание информационных систем, в случае необходимости, информирует пользователей информационных систем о возникновении инцидента и даёт указания по дальнейшим действиям.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъекта персональных данных, ответственный за обработку персональных данных в Контрольно-счетной палате уведомляет уполномоченный орган по защите прав субъектов персональных данных:

1) в течение 24-х часов – о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет контактные сведения для взаимодействия с комиссией по инцидентам;

2) в течение 72-х часов – о результатах внутреннего расследования выявленного инцидента, а также сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5. Анализ инцидентов, а также оценка их последствий

Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий осуществляет ответственный за техническое обслуживание информационных систем.

5.1. Источниками и причинами возникновения инцидентов в области информационной безопасности являются:

1) действия организаций и отдельных лиц враждебные интересам Контрольно-счетной палаты;

2) недостаточная работа по обеспечению необходимого режима соблюдения конфиденциальности, в том числе персональных данных;

3) отсутствие дисциплинарной мотивации соблюдения правил и требований информационной безопасности;

4) совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;

5) наличие привилегированных бесконтрольных пользователей в информационной системе;

6) пренебрежение правилами и требованиями информационной безопасности должностными лицами и иными штатными работниками Контрольно-счетной палаты;

7) и другие причины.

5.2. Оценка последствий инцидента производится на основании потенциально возможного или фактического ущерба.

6. Принятие мер по устранению последствий инцидентов

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

1) определение границ инцидента и ущерба от реализации угроз информационной безопасности;

2) ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. Планирование и принятие мер по предотвращению инцидентов

7.1. Планирование и принятие мер по предотвращению возникновения инцидентов осуществляют ответственный за техническое обслуживание информационных систем Контрольно-счетной палаты и ответственный за обработку персональных данных в Контрольно-счетной палате, основываясь на:

1) планомерной деятельности по повышению уровня осознания информационной безопасности должностными лицами и иными штатными работниками Контрольно-счетной палаты;

2) проведении мероприятий по обучению должностных лиц и иных штатных работников Контрольно-счетной палаты правилам и способам работы со средствами защиты информационных систем;

3) доведении до должностных лиц и иных штатных работников Контрольно-счетной палаты норм законодательства, локальных правовых актов Контрольно-счетной палаты, устанавливающих ответственность за нарушение требований информационной безопасности;

4) разъяснительной работе с увольняющимися и принимаемыми на работу должностными лицами и иными штатными работниками Контрольно-счетной палаты;

5) своевременной модернизации системы обеспечения информационной безопасности с учётом возникновения новых угроз информационной безопасности, либо в случае изменения требований руководящих документов по организации обеспечения информационной безопасности;

6) своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом.

Как правило, самым слабым звеном в любой системе безопасности является человек. Поэтому работа с персоналом является основным направлением деятельности по обеспечению требований информационной безопасности.

Должностные лица и иные штатные работники Контрольно-счетной палаты являются важным источником сведений об инцидентах информационной безопасности, поэтому необходимо донести до них информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности могут являться основанием для смягчения либо отмены наказания за нарушение требований информационной безопасности.

|  |  |
| --- | --- |
|  | Приложение  к Положению по работе с инцидентами информационной безопасности в Контрольно-счетной палате Республики Карелия |

|  |
| --- |
| **Контрольно-счетная палата Республики Карелия** |

|  |  |  |
| --- | --- | --- |
|  | **ЖУРНАЛ**  **регистрации инцидентов информационной безопасности**  **Контрольно-счетной палаты Республики Карелия** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Начат «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года |  | Окончен «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года |  |
|  |  |  |  |
| (должность) |  | (должность) |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | / |  | / |  |  | / |  | / |  |
| (подпись) |  | (И.О. Фамилия) |  |  | (подпись) |  | (И.О. Фамилия) |  |  |

На \_\_\_\_\_ листах

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | ФИО, должность служащего, обнаружившего инцидент | Дата выявления инцидента | Описание инцидента | Принятые меры по устранению последствий инцидента | Причины возникновения инцидента | Размер потенциально- возможного ущерба | Размер фактичес-  кого ущерба | Принятые меры по предотвращению повторного возникновения инцидента |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |