Приложение 1.

УТВЕРЖДЕНО
Распоряжением Администрации
Качканарского городского округа
Свердловской области
от 29.09.2023 № 83
«Об информационной безопасности
(защите информации) в
Администрации Качканарского
городского округа Свердловской
области»

Формы отчета о событиях и инцидентах информационной безопасности

Отчеты о событиях и инцидентах информационной безопасности

Рекомендации по заполнению

Назначением данной формы (формы отчета о событиях и инцидентах ИБ) является обеспечение информацией о событии информационной безопасности (далее - ИБ), а затем, если оно определено как инцидент ИБ, то и об инциденте ИБ, для определенных лиц.

Если подозревается, что событие ИБ развивается или уже свершилось, особенно событие, которое может привести к существенным потерям или ущербу собственности или репутации организации, то необходимо немедленно заполнить и передать форму отчета о событии ИБ в соответствии с процедурами, описанными в системе менеджмента инцидентов ИБ организации.

Представленная информация будет использована для инициирования соответствующего процесса оценки, которая определит, должно ли это событие категорироваться как инцидент ИБ и (в случае положительного ответа), какие корректирующие меры, необходимые для предотвращения или ограничения потерь или ущерба, следует предпринять. Поскольку процесс оценки по своему характеру является краткосрочным, то в данный момент необязательно заполнять все поля формы отчета.

Если сотрудник является членом группы обеспечения эксплуатации, анализирующим полностью/частично заполненные формы отчета, то он должен принять решение, надо ли отнести данное событие к категории инцидента ИБ. При положительном решении сотрудник должен внести в форму отчета об инциденте ИБ как можно больше информации и передать формы отчетов о событии и инциденте ИБ в группе реагирования на инциденты информационной безопасности (далее - ГРИИБ). Независимо от того, будет ли событие ИБ отнесено к категории инцидента ИБ, база данных событий/инцидентов ИБ должна быть обновлена.

Если сотрудник является сотрудником ГРИИБ, анализирующим формы отчетов о событиях и инцидентах ИБ, переданные членом группы обеспечения эксплуатации, то форма отчета об инциденте ИБ должна обновляться по ходу расследования и, соответственно, должна обновляться база данных событий/инцидентов ИБ.

При заполнении форм следует соблюдать следующие рекомендации:

- по возможности формы отчета должны заполняться и передаваться в электронном виде <1>. В случае, если существуют проблемы или считается, что существуют проблемы с принятыми по умолчанию механизмами электронного оповещения (например электронная почта), включая случаи, когда система может подвергаться атаке и формы отчета могут быть

прочитаны несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть телефон или текстовые сообщения, а также использование курьеров;

- следует представить информацию, основанную на фактах, в которой сотрудник уверен, не следует что-либо придумывать для того, чтобы заполнить все формы. Если сотрудник считает уместным включить иную информацию, которую не может подтвердить, следует указать, что это неподтвержденная информация, и причину убежденности в ее недостоверности;

- следует подробно указать, как можно связаться с сотрудником. Немедленно или спустя некоторое время может возникнуть необходимость контакта с ним для получения дальнейшей информации, касающейся Вашего отчета.

<1> Если возможно, то формы отчетов должны быть, например, на безопасной web-странице с привязкой к электронной базе данных событий инцидентов ИБ. В настоящее время основанная на бумажной технологии система является слишком медленно действующей и далеко не самой эффективной в эксплуатации.

Если позднее сотрудник обнаружит, что какая-либо представленная им информация неточна, неполна или ошибочна, то следует внести поправки в отчет и представить его повторно.

Отчет о событии информационной безопасности

Дата события
Номер события <1> _____ Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сообщающем лице

Фамилия _____ Адрес _____
Организация _____ _____
Телефон _____ Электронная почта _____
_____

Описание события ИБ

Описание события:
Что произошло
Как произошло
Почему произошло
Пораженные компоненты
Негативное воздействие на бизнес
Любые идентифицированные уязвимости

Подробности о событии ИБ

Дата и время наступления события
Дата и время обнаружения события
Дата и время сообщения о событии
Закончилось ли событие? (отметить в квадрате) Да ☐ Нет ☐
Если "да", то уточнить длительность события в днях/часах/минутах

<1> Номера событий назначаются руководителем ГРИИБ организации.

Отчет об инциденте информационной безопасности

Дата инцидента
Номер инцидента <1>: _____ Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сотруднике группы обеспечения эксплуатации

Фамилия _____ Адрес _____
Телефон _____ Электронная почта _____

Информация о сотруднике ГРИИБ

Фамилия _____ Адрес _____
Телефон _____ Электронная почта _____
_____

Описание инцидента ИБ

Дополнительное описание инцидента:
Что произошло
Как произошло
Почему произошло
Пораженные компоненты
Негативное воздействие на бизнес
Любые идентифицированные уязвимости

Подробности об инциденте ИБ

Дата и время возникновения инцидента
Дата и время обнаружения инцидента
Дата и время сообщения об инциденте
Закончился ли инцидент? (отметить в квадрате) Да ☐ Нет ☐
Если "Да", то уточнить длительность инцидента в днях/часах/минутах. Если "Нет", то уточнить, как долго он уже длится

<1> Номера инцидентов назначаются руководителем ГРИИБ организации и привязываются к номеру(ам) соответствующих событий.

Отчет об инциденте информационной безопасности

Тип инцидента ИБ

(Сделать отметку в одном из квадратов, затем заполнить ниже соответствующие поля)

Действительный ☐ Попытка ☐ Предполагаемый ☐

(Один из) Намеренная ☐ (указать типы угрозы)

- Хищение (TH) ☐
- Мошенничество (FR) ☐
- Саботаж/физический ущерб (SA) ☐
- Вредоносная программа (MC) ☐
- Хакерство/логическое проникновение (HA) ☐
- Неправильное использование ресурсов (MI) ☐
- Другой ущерб (OD) ☐

Определить:

(Один из) Случайная ☐ (указать типы угрозы)

- Отказ аппаратуры (HF) ☐
- Отказ ПО (SF) ☐
- Отказ системы связи (CF) ☐
- Пожар (HE) ☐
- Наводнение (FL) ☐
- Другие природные события (NE) ☐
- потеря значимых сервисов (LE) ☐
- недостаточное кадровое обеспечение (SS) ☐
- Другие случаи (OA) ☐

Определить:

(Один из) Ошибка ☐ (указать типы угрозы)

- Операционная ошибка (OE) ☐
- Ошибка в эксплуатации аппаратных средств (HE) ☐
- Ошибка в эксплуатации ПО (SE) ☐
- Ошибка пользователя (UE) ☐
- Ошибка проектирования (DE) ☐
- Другие случаи (включая ненамеренные ошибки) (OA) ☐

Определить:

Неизвестно ☐ (Если еще не установлен тип инцидента ИБ (намеренный, случайный, ошибка), то следует сделать отметку в квадрате "неизвестно" и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)

Определить:

Отчет об инциденте информационной безопасности

Пораженные активы

Пораженные активы (при наличии) — (Дать описания активов, пораженных инцидентами ИБ или связанных с ним, включая (где требуются) серийные, лицензионные номера и номера версий)

Информация/данные _____
Аппаратные средства _____
Программное обеспечение _____
Средства связи _____
Документация _____

Негативное воздействие/влияние инцидента на бизнес

Сделать отметку в соответствующих квадратах для указанных ниже нарушений, затем в колонке "значимость" указать степень негативного воздействия на бизнес по шкале 1 - 10, используя следующие сокращения (указатели категорий): (FD) - финансовые убытки/разрушение бизнес-операций, (CE) - коммерческие и экономические интересы, (PI) - информация, содержащая персональные данные, (LR) - правовые и нормативные обязательства (это необходимо сравнить с английским оригиналом), (MO) - менеджмент и бизнес-операции, (LG) - потеря престижа (см. примеры в Приложении). Записать кодовые буквы в колонке "указатели", а если известны действительные издержки, - указать их в колонке "стоимость".

	Значимость	Указатели	Издержки
Нарушение конфиденциальности (то есть несанкционированное раскрытие)	☐		
Нарушение целостности (то есть несанкционированная модификация)	☐		
Нарушение доступности (то есть недоступность)	☐		
Нарушение неотказуемости	☐		
Уничтожение	☐		

Общие расходы на восстановление после инцидента ИБ

	Значимость	Указатели	Издержки
(Там, где возможно, необходимо указать общие расходы на восстановление после инцидента ИБ в целом по шкале 1 - 10 для "значимости" и в деньгах для "стоимости")			

Отчет об инциденте информационной безопасности

Разрешение инцидента

Дата начала расследования инцидента ИБ _____
Фамилия(ии) лица (лиц), проводившего(их) расследование инцидента _____
Дата завершения инцидента ИБ _____
Дата окончания воздействия _____
Дата завершения расследования инцидента ИБ _____
Место хранения отчета о расследовании _____

Причастные к инциденту лица/нарушители

(Один из) Лицо (PE) ☐ Легально учрежденная организация/учреждение (OI) ☐

Организованная группа (GR) ☐ Случайность (AC) ☐

Отсутствие нарушителя (NP)
Например, природные факторы, отказ оборудования, человеческий фактор ☐

Описание нарушителя
Действительная или предполагаемая мотивация

(Один из)
Криминальная/финансовая выгода (CG) ☐
Развлечение/хакерство (PH) ☐
Политика/терроризм (PT) ☐
Месть (RE) ☐
Другие мотивы (OM) ☐
Определить:

Действия, используемые для разрешения инцидента ИБ

(например, "никаких действий", "подручными средствами", "внутреннее расследование", "внешнее расследование с привлечением ...")

Действия, запланированные для разрешения инцидента

(включая возможные приведенные выше действия)

Прочие действия

(например, по-прежнему требуется проведение расследования, но другим персоналом)

Отчет об инциденте ИБ
Заключение

(Сделать отметку в одном из квадратов, является ли инцидент значительным или нет, и приложить краткое изложение обоснования этого заключения)

Значительный ☐ Незначительный ☐

(Указать любые другие заключения)

Оповещенные лица/субъекты

(Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия. Обычно этим лицом является руководитель ИБ организации)

Руководитель службы ИБ ☐

Местный руководитель (уточнить, какого подразделения) ☐

Автор отчета ☐

Полиция ☐

Руководитель ГРИИБ ☐

Руководитель информационных систем ☐

Руководитель автора отчета ☐

Другие лица (например, справочная служба, отдел кадров, руководство, служба внутреннего аудита, регулятивный орган, сторонняя КСБР) ☐

Определить:

Привлеченные лица

Инициатор		Аналитик		Аналитик	
Подпись	_____	Подпись	_____	Подпись	_____
Фамилия	_____	Фамилия	_____	Фамилия	_____
Должность	_____	Должность	_____	Должность	_____
Дата	_____	Дата	_____	Дата	_____

Аналитик		Аналитик		Аналитик	
Подпись	_____	Подпись	_____	Подпись	_____
Фамилия	_____	Фамилия	_____	Фамилия	_____
Должность	_____	Должность	_____	Должность	_____
Дата	_____	Дата	_____	Дата	_____

Приложение
(справочное)

ПРИМЕРЫ ОБЩИХ РЕКОМЕНДАЦИЙ ПО ОЦЕНКЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.1. Введение

В настоящем приложении представлены примерные рекомендации по оценке и категорированию негативных последствий инцидентов ИБ, где каждая рекомендация имеет шкалу от 1 до 10 (1 - низкий, 10 - высокий). (На практике могут использоваться другие шкалы, например, с градацией от 1 до 5. Каждая организация должна использовать шкалу, наиболее подходящую для ее условий).

Перед изучением рекомендаций необходимо ознакомиться со следующими пояснениями:

- в некоторых из рекомендаций, представленных ниже, содержится примечание "Нет записи", для негативных последствий, приведенных для каждой градации инцидента ИБ (от 1 до 10) и идентичных для других шкал (например, с градацией от 1 до 5). Однако на некоторых градациях (по шкале от 1 до 10) для конкретных инцидентов ИБ считается, что из-за отсутствия больших различий в записях о последствиях инцидента ИБ на более низких градациях делать запись нецелесообразно и в этом случае делается примечание "Нет записи". Аналогично вышеизложенному, при более высоких градациях инцидента ИБ считается, что негативные последствия для них не могут быть серьезнее негативных последствий, показанных для самой высокой градации, и, следовательно, для этих градаций действует примечание "Нет записи". (Таким образом, было бы неправильно исключить указания с пометкой "Нет записи" и тем самым градацию шкалы);

- для приведенных рекомендаций, в которых применяются финансовые показатели, приведенные пределы колебаний кажутся несколько необычными. Перед использованием эти рекомендации должны быть дополнены нормированием колебаний курса валюты, наиболее подходящей для организации.

Таким образом, при использовании перечисляемых рекомендаций для расследования негативных последствий инцидента ИБ для бизнеса организации, являющихся следствием несанкционированного раскрытия информации, несанкционированного изменения информации, отказа от использованной информации, недоступности информации и (или) сервиса, уничтожения информации и (или) сервиса, в первую очередь необходимо определить, какая из нижеследующих категорий является соответствующей. Необходимо применять рекомендации по категорированию для определения реального негативного воздействия на бизнес-процессы ("значимость") с целью занесения в форму отчета об инциденте ИБ.

В.2. Финансовые убытки/нарушение хода бизнес-операций

Последствия несанкционированного раскрытия, модификации и искажения смысла переданной информации, а также недоступности и уничтожения такой информации могут привести к финансовым убыткам, например, в результате снижения цен на акции, мошенничества или разрыва контракта по причине бездействия или запоздалых действии в отношении этих последствий. Последствиями недоступности или уничтожения любой информации может быть также нарушение бизнес-процесса. На исправление ситуации и (или) восстановление бизнес-процесса после таких инцидентов ИБ потребуются время и усилия. Эти последствия в некоторых случаях могут быть значительными и должны обязательно приниматься во внимание. Для расчетов последствий необходимо, чтобы время восстановления вычислялось в единицах рабочего времени персонала и пересчитывалось в стоимость рабочего времени (финансовые затраты). Эти финансовые затраты должны быть вычислены, исходя из средней стоимости 1 чел.-мес по соответствующей градации/уровню, принятой/принятого внутри организации. Предлагается руководствоваться следующими рекомендациями:

1) результат в финансовых убытках/затратах x_1 или менее,

2) результат в финансовых убытках/затратах между x_1 и x_2;

3) результат в финансовых убытках/затратах между $x_2 + 1$ и x_3;

4) результат в финансовых убытках/затратах между $x_3 + 1$ и x_4;

5) результат в финансовых убытках/затратах между $x_4 + 1$ и x_5;

6) результат в финансовых убытках/затратах между $x_5 + 1$ и x_6;

7) результат в финансовых убытках/затратах между $x_6 + 1$ и x_7;

8) результат в финансовых убытках/затратах между $x_7 + 1$ и x_8;

9) результат в финансовых убытках/затратах более x_8;

10) организация выходит из бизнеса.

В.3. Коммерческие и экономические интересы

Коммерческая и экономическая информация нуждается в защите и оценивается с учетом ее значимости для конкурентов или по воздействию, которое оказывает ее компрометация на коммерческие интересы. Следует руководствоваться следующими рекомендациями по обеспечению защиты информации, представляющей интерес:

1) для конкурента, но не имеет коммерческой значимости (ценности);

2) для конкурента при значении параметра ценности информации, равном y_1 или менее (коммерческий оборот);

3) для конкурента при значении параметра ценности информации, находящегося в диапазоне $y_1 + 1$ и y_2 (оборот) или является причиной финансовых убытков, или потери заработка, или облегчает получение незаконной прибыли, или вызывает нарушение обязательств по поддержанию достоверности информации, поставляемой третьими сторонами;

4) для конкурента при значении параметра ценности информации, находящегося в диапазоне $y_2 + 1$ и y_3 (товарооборот);

5) для конкурента при значении параметра ценности информации, находящегося в диапазоне $y_3 + 1$ и y_4 (товарооборот);

6) для конкурента при значении параметра ценности информации более $y_4 + 1$ (оборот);

а также в случаях, когда:

7) нет записи <1>;

8) нет записи;

9) может существенно повлиять на коммерческие интересы или подорвать финансовое состояние организации;

10) нет записи.

<1> Термин "Нет записи" означает, что для этой градации последствий инцидента ИБ соответствующая запись отсутствует.

В.4. Информация, содержащая персональные данные

В местах хранения и обработки информации, содержащей персональные данные физических лиц, считают моральной и этически корректной, а при некоторых обстоятельствах юридически необходимой защиту этой информации от несанкционированного раскрытия, которое может привести в лучшем случае к созданию дискомфорта у юридического лица, а в худшем - к судебному преследованию лица, раскрывшего информацию, в соответствии с требованием законодательства в части защиты персональных данных. В равной степени необходимо, чтобы информация, содержащая персональные данные, была всегда правильной, поскольку ее несанкционированное изменение, приводящее к появлению некорректных данных, может иметь такое же последствие, что и ее несанкционированное раскрытие. Важно, чтобы информацию, содержащую персональные данные, нельзя было сделать доступной или уничтожить, поскольку это может привести к принятию неправильных решений юридическими лицами или их бездействию во время инцидента ИБ, что может иметь такое же воздействие, что и несанкционированное раскрытие или модификация информации. Следует руководствоваться следующим рекомендациями по градации нанесения ущерба информации, содержащей персональные данные:

1) нанесение (причинение) незначительного ущерба (беспокойства) конкретному лицу (гнев, расстройство, разочарование), но не нарушение правовых или нормативных требований;

2) нанесение (причинение) ущерба (беспокойства) конкретному лицу (гнев, расстройство, разочарование), но не нарушение правовых или нормативных требований;

3) нарушение правовых, нормативных или этических требований, а также опубликование намерения относительно нарушения защиты информации, приводящее к незначительному дискомфорту конкретного лица или группы лиц;

4) нарушение правовых, нормативных или этических требований, а также опубликование намерений относительно нарушения защиты информации, приводящее к чувству значительного дискомфорта для конкретного лица или к незначительному дискомфорту - группы лиц;

5) нарушение правовых, нормативных или этических требований, а также опубликованных намерений относительно защиты информации, приводящее к серьезным проблемам конкретного лица;

6) нарушение правовых, нормативных или этических требований, а также опубликование намерений относительно нарушения защиты информации, приводящее к серьезному дискомфорту для группы лиц;

7) нет записи;

8) нет записи;

9) нет записи;

10) нет записи.

B.5. Правовые и нормативные обязательства

Данные, хранимые и обрабатываемые организацией, могут подчиняться правовым и нормативным обязательствам или храниться и обрабатываться с целью обеспечения соответствия организации данным обязательствам. Несоблюдение таких обязательств, намеренное или ненамеренное, может привести к принятию правовых или административных мер к лицам, работающим в данной организации. Результатом принятия данных мер могут быть штрафы и (или) тюремное заключение. Предлагается руководствоваться следующими рекомендациями:

1) нет записи;

2) нет записи;

3) предупреждение о правоприменении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу z_1 или меньше;

4) предупреждение, гражданский иск или уголовное преступление, приводящее к финансовому ущербу/штрафу между $z_1 + 1$ и z_2;

5) предупреждение о правоприменении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу между $z_2 + 1$ и z_3 или тюремному заключению сроком до двух лет;

6) предупреждение о правонарушении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу между $z_3 + 1$ и z_4 или тюремному заключению сроком от двух до 10 лет;

7) предупреждение о правонарушении, гражданский иск или уголовное преступление, приводящее к финансовым убыткам/штрафу или тюремному заключению сроком более 10 лет;

8) нет записи;

9) нет записи;

10) нет записи.

B.6. Менеджмент и бизнес-операции

Информация может быть такой, что ее компрометация способна нанести ущерб эффективности работы организации. Например, будучи раскрытой, относящаяся к внесению изменений в политике информация может спровоцировать такую общественную реакцию, что реализация данной политики станет невозможной. Модификация, изменение смысла переданной информации или недоступность информации, касающейся финансовых аспектов или компьютерного программного обеспечения, могут также иметь серьезные последствия для работы организации. Кроме того, отказ от обязательств по обеспечению ИБ может иметь негативные последствия для бизнеса. Предлагается руководствоваться следующими рекомендациями по оценке последствий:

1) неэффективная работа одного подразделения организации;

2) нет записи;

3) нарушение функций (деятельности) по эффективному руководству организацией и ее работы;

4) нет записи;

5) создание препятствий для эффективной разработки или функционирования политик организации;

6) причинение ущерба организации при коммерческих или политических переговорах с другими организациями;

7) создание препятствий для разработки или функционирования главных политик организации, отключение или значительное прерывание важных операций каким-либо другим способом;

8) нет записи;

9) нет записи;

10) нет записи.

В.7. Утрата престижа

Несанкционированное раскрытие информации, отказ от обязательств по обеспечению ИБ или модификация информации, а также недоступность информации могут привести к потере престижа организации с последующим возможным нанесением ущерба ее репутации, к потере доверия и другим негативным последствиям. Предлагается руководствоваться следующими рекомендациями по оценке престижа организации:

1) нет записи;

2) создание атмосферы недовольства внутри организации;

3) негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям местного/регионального масштаба;

4) нет записи;

5) негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям национального масштаба;

6) нет записи;

7) значительное негативное влияние на отношения с акционерами, потребителями, поставщиками, регулирующими органами, правительством, с другими организациями или общественностью, приводящее к нежелательным последствиям;

8) нет записи;

9) нет записи;

10) нет записи.