ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Управление инцидентами информационной безопасности

Часть 2

Руководящие указания по планированию и подготовке к реагированию на инциденты

(ISO/IEC 27035-2:2016, MOD)

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «Единый интегратор по созданию и поддержке государственных информационных систем UZINFOCOM» (Единый интегратор UZINFOCOM)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере информационных технологий и телекоммуникаций № 7

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 07.03.2019 № 05-1033

4 Настоящий стандарт модифицирован по отношению к международному стандарту ISO/IEC 27035-2:2016 Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response (Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Часть 2. Руководящие указания по планированию и разработке реагирования на инциденты)

Сведения о соответствии ссылочных международных стандартов государственным стандартам Республики Узбекистан приведены в дополнительном приложении D.

Полный перечень технических отклонений с объяснением причин их внесения приведен в дополнительном приложении E.

Перевод с английского языка (en).

Степень соответствия - модифицированная (MOD).

5 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт».

Содержание

Введение

Стандарты O‘z DSt 3386, O‘z DSt 3387 продолжает серию стандартов O‘z DSt ISO/IEC 27000, и уделяет основное внимание управлению инцидентами информационной безопасности (ИБ), которое, согласно серии стандартов O‘z DSt ISO/IEC 27000, определено как один из решающих факторов успеха системы управления информационной безопасностью (СУИБ).

Существует большая разница между планом управления инцидентами ИБ организации и осведомленностью организации о готовности реагирования на инциденты, поэтому в настоящем стандарте рассматривается разработка руководящих указаний по повышению уверенности в реальной готовности организации реагировать на инцидент ИБ. Это достигается путем рассмотрения политик и планов, связанных с управлением инцидентами, создания группы реагирования на инциденты ИБ (ГРИИБ) и улучшения ее работы путем освоения извлеченного опыта и оценки.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
ХАВФСИЗЛИКНИ ТАЪМИНЛАШ УСУЛЛАРИ
Ахборот хавфсизлиги инцидентларини бошқариш
2-қисм
Инцидентларга таъсир этишни режалаштириш ва унга тайёрланиш бўйича раҳбарий кўрсатмалар

Информационная технология
МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Управление инцидентами информационной безопасности
Часть 2
Руководящие указания по планированию и подготовке к реагированию на инциденты

Information technology. Security techniques.
Information security incident management.
Part 2. Guidelines to plan and prepare for incident response

Дата введения 01.04.2019

1 Область применения

Настоящий стандарт содержит руководящие указания по планированию и подготовке к реагированию на инциденты. Эти указания основаны на этапах «Планирование и подготовка» и «Извлеченный опыт», представленных в O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD)

Основные моменты этапа «Планирование и подготовка» включают следующее:

- политику управления инцидентами ИБ и вовлеченность высшего руководства в разработку данной политики;
- политики ИБ, в том числе связанные с управлением рисками, их обновление как на корпоративном уровне, так и на уровне систем, служб и сетей;
- план управления инцидентами ИБ;
- создание ГРИИБ;
- установление и поддержание соответствующих отношений и связей с внутренними и внешними организациями;

Издание официальное

- техническую и другую поддержку (включая организационное и эксплуатационное сопровождение);
- оперативные совещания и тренинги по повышению осведомленности по управлению инцидентами ИБ;
- тестирование плана управления инцидентами ИБ.

Принципы, изложенные в настоящем стандарте, носят общий характер и предназначены для применения всеми организациями, независимо от их типа, размера или вида деятельности. Организации могут корректировать руководство, предоставленное в настоящем стандарте, в соответствии с их типом, размером и видом деятельности, применительно к ситуации с рисками ИБ. Настоящий стандарт также применим к внешним организациям, предоставляющим услуги по управлению инцидентами ИБ.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O‘z DSt ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь

O‘z DSt ISO/IEC 27001:2016 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования

O‘z DSt ISO/IEC 27002:2016 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

O‘z DSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности

O‘z DSt ISO/IEC 27031:2016 Информационная технология. Методы обеспечения безопасности. Руководящие указания по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса

O‘z DSt ISO/IEC 27033-1:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции

O‘z DSt ISO/IEC 27033-2:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 2. Руководящие указания по проектированию и внедрению сетевой безопасности

O‘z DSt ISO/IEC 27033-3:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

O‘z DSt ISO/IEC 27033-4:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для

обеспечения безопасности между сетями с применением шлюзов безопасности

O‘z DSt ISO/IEC 27033-5:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных сетей

O‘z DSt ISO/IEC 27033-6:2018 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 6. Защищенный доступ к беспроводной IP-сети

O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами

O‘z DSt ISO/IEC 27039:2017 Информационная технология. Методы обеспечения безопасности. Выбор, применение и операции систем обнаружения и предотвращения вторжений

Примечание - При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов на территории Узбекистана по соответствующему указателю стандартов, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по O‘z DSt ISO/IEC 27000, O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD), а также следующий термин с соответствующим определением:

3.1.1 **пользователи** (users): Физические и/или юридические лица, которые используют услуги, предоставляемые группой реагирования на инциденты ИБ.

Примечание - Пользователи могут быть внутренними (внутри организации) или внешними (вне организации).

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

Blu-ray — Blu-ray Disc - формат оптического носителя, используемый для записи с повышенной плотностью хранения

	цифровых данных, включая видео высокой четкости
CD	Compact Disk - компакт-диск
DNS	Domain Name System - система доменных имен
DVD	Digital Video/Versatile Disk - цифровой видео/многофункциональный диск
HTTP	HyperText Transfer Protocol - протокол передачи гипертекста
HTTPS	HyperText Transfer Protocol Secure - расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
ICMP	Internet Control Message Protocol - протокол межсетевых управляющих сообщений
IP	Internet Protocol - протокол Интернета
IPv4	Internet Protocol v4 - протокол Интернета версии 4
IPv6	Internet Protocol v6 - протокол Интернета версии 6
SMTP	Simple Mail Transfer Protocol - простой протокол передачи почты
SQL	Structured Query Language - язык структурированных запросов
SSL	Secure Sockets Layer - уровень защищенных сокетов
TCP	Transmission Control Protocol - протокол управления передачей
TLP	Traffic Light Protocol - «протокол Светофор» (набор обозначений для маркировки конфиденциальной информации с целью указания аудитории ее дальнейшего распространения; информация маркируется одним из четырех цветов)
TLS	Transport Layer Security - протокол защиты транспортного уровня
UDP	User Datagram Protocol - протокол пользовательских датаграмм
Wi-Fi	Wireless Fidelity - технология беспроводных локальных сетей
ГРИИБ	группа реагирования на инциденты информационной безопасности
ИБ	информационная безопасность
ИТ	информационная технология
СОиПВ	система обнаружения и предотвращения вторжений
СУИБ	система управления информационной безопасностью

4 Политика управления инцидентами информационной безопасности

4.1 Общие положения

В разделе 4 подробно описано содержание O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) (5.2, перечисление a)).

Политика управления инцидентами ИБ организации должна обеспечивать использование официально задокументированных указаний и намерений по непосредственному принятию решений, последовательной и надлежащей реализации процессов и процедур применительно к этой политике.

Любая политика управления инцидентами ИБ должна быть частью стратегии ИБ для организации. Она также должна поддерживать существующую миссию головной организации и соответствовать уже существующим политикам и процедурам.

Организация должна внедрять политику управления инцидентами ИБ, в которой описываются процессы, ответственные лица, полномочия и формы отчетности (в частности, основное контактное лицо для сообщений о наличии подозрений на инцидент) при возникновении инцидента ИБ. Политику следует регулярно пересматривать, чтобы она отражала актуальную организационную структуру, процессы и технологии, которые могут повлиять при реагировании на инциденты. В политике также должны быть изложены любые инициативы по повышению осведомленности и тренингам, связанные с реагированием на инциденты (см. раздел 10).

Организация должна документировать свою политику для управления событиями, инцидентами и уязвимостями ИБ в качестве самостоятельного документа в рамках своей общей политики СУИБ (см. O‘z DSt ISO/IEC 27001 (5.2)) или как часть своей политики ИБ (см. O‘z DSt ISO/IEC 27002 (5.1.1)). Тип, размер или вид деятельности организации и степень распространения ее программы управления инцидентами ИБ являются определяющими факторами при определении того, какой из этих вариантов принять. Политика управления инцидентами ИБ организации должна быть направлена на каждого человека, имеющего санкционированный доступ к информационным системам и связанным с ними ресурсам.

Прежде чем сформулировать политику управления инцидентами ИБ, организация должна определить следующее в отношении управления инцидентами ИБ:

a) цели;

b) внутренние и внешние заинтересованные стороны;

c) особые типы инцидентов и уязвимостей, которые необходимо выделить;

d) любые особые роли (должности), которые необходимо выделить;
e) выгоды для всей организации в целом и ее подразделений.

4.2 Вовлеченные стороны

Успешная политика управления инцидентами ИБ должна быть создана и внедрена как процесс на уровне всей организации. С этой целью все заинтересованные стороны или их представители должны быть вовлечены в разработку политики с начальных этапов планирования путем участия в какомлибо процессе или в группе реагирования. В такую группу могут входить юрисконсульты, сотрудники по связям с общественностью и маркетингу, руководители отделов, сотрудники службы безопасности, системные и сетевые администраторы, сотрудники ИТ, персонал службы поддержки, представители руководящего состава, а в некоторых случаях и производственный персонал.

Организация должна обеспечить, чтобы ее политика управления инцидентами ИБ была одобрена членом высшего руководства с подтвержденным обязательством со стороны всего высшего руководства.

Обеспечение непрерывного исполнения обязательств руководства имеет жизненно важное значение для принятия структурированного подхода к управлению инцидентами ИБ. Персоналу необходимо распознать инцидент, знать, что делать и понимать преимущества подхода организации. Руководство должно поддерживать политику инцидентов ИБ, чтобы гарантировать, что организация берет на себя обязательства по обеспечению ресурсами и поддержанию потенциала реагирования на инциденты.

Политика управления инцидентами ИБ должна предоставляться каждому сотруднику и подрядчику, а также должна быть рассмотрена на оперативных совещаниях и тренингах по повышению осведомленности ИБ.

4.3 Содержание политики управления инцидентами информационной безопасности

Политика управления инцидентами ИБ должна быть разработана на высшем уровне. Подробная информация и пошаговые инструкции должны быть включены в ряд документов, составляющих план управления инцидентами ИБ, который представлен в разделе 6.

Организация должна обеспечить, чтобы содержание политики управления инцидентами ИБ рассматривало (но не ограничивалось этим) следующие темы:

a) цель, задачи и область применения (к кому применяется и при каких обстоятельствах) политики;

b) владелец политики и периодичность пересмотра;

c) значимость плана управления инцидентами ИБ для организации и приверженности высшего руководства ему и соответствующей документации;

d) определение того, что представляет собой инцидент ИБ;

e) описание типов или категорий инцидентов ИБ (или ссылка на другой документ с более подробным описанием);

f) описание того, как следует сообщать об инцидентах ИБ, в том числе, что, когда и кому сообщать, а также механизмы, используемые для отчетности;

g) качественное рассмотрение или визуализация процесса управления инцидентами (с указанием основных шагов по обработке инцидента ИБ) от обнаружения до отчетности, обобщения информации, анализа, реагирования, уведомления, эскалации (процесса привлечения дополнительных полномочий) и разрешения;

h) требования к последующей деятельности по разрешению инцидентов ИБ, включая изучение и совершенствование процесса, следующего после разрешения инцидентов ИБ;

i) сводка отчетности по уязвимостям и их обработке (может быть в виде отдельной политики);

j) определенный набор ролей, обязанностей и полномочий принятия решений для каждого этапа процесса управления инцидентами ИБ и связанной с ним деятельности (включая отчетность по уязвимостям и их обработке, при необходимости);

k) ссылка на документ, описывающий классификацию событий и инцидентов ИБ, степень серьезности (если используется) и соответствующие термины. Обзор должен содержать либо описание того, что представляет собой инцидент, либо ссылку на документ, где это описано;

l) обзор ГРИИБ, охватывающий организационную структуру ГРИИБ, ключевые роли, обязанности и полномочия, а также свод задач, включая (но не ограничиваясь этим) следующее:

1) требования к отчетности и уведомлению об инцидентах, которые были подтверждены;

2) инструктаж высшего руководства по инцидентам;

3) рассмотрение запросов по инцидентам, мониторинг их исполнения и разрешение инцидентов;

4) взаимодействие с внешними организациями (при необходимости);

5) требование и обоснование по обеспечению надлежащей регистрации всей деятельности по управлению инцидентами ИБ, выполняемой ГРИИБ, для последующего анализа;

m) требование совместного взаимодействия всех подразделений организации для обнаружения, анализа и реагирования на инциденты ИБ;

n) описание любого контролирующего органа, а также его полномочий и обязанностей, если это применимо;

o) перечень организаций, предоставляющих специфичные внешние услуги, например, группы судебной экспертизы, юрисконсульты и т.д.;

p) краткое изложение законодательных и нормативно-правовых требований, связанных с деятельностью по управлению инцидентами ИБ (более подробная информация приведена в приложении А);

q) список и ссылки на другие политики, процедуры и документы, которые поддерживают процесс управления инцидентами ИБ и связанную с ними деятельность. Многие позиции, перечисленные в политике, могут иметь свои собственные более подробные процедуры или руководящие документы.

Существуют другие политики или процедуры, которые будут поддерживать политику управления инцидентами ИБ и могут быть установлены как часть подготовительного этапа (при его отсутствии) в случае, если они подходят для организации. Они включают (но не ограничиваются) следующее:

- план управления инцидентами ИБ, описанный в разделе 6;

- политику непрерывного мониторинга, формулирующую проведение подобной деятельности организацией и описание основных задач мониторинга. Непрерывный мониторинг обеспечивает сохранение электронных доказательств в случае, если это требуется для следственных действий или внутренних дисциплинарных мер;

- полномочия, предоставляющие ГРИИБ доступ к результатам вышеуказанного мониторинга или возможность запрашивать по мере необходимости соответствующие журналы регистрации (данный пункт рекомендуется включить в политику управления инцидентами ИБ);

- политики обмена информацией, раскрытия информации и взаимодействия, в которых описывается, каким образом, когда и кому информация, связанная с деятельностью по управлению ИБ, может быть передана. Такая информация должна быть конфиденциальной и раскрываться только в соответствии с законодательством. Во многих случаях законодательство требует, чтобы затрагиваемые стороны были уведомлены, если какие-либо персональные данные были подвержены компрометации. Помимо нормативных требований, информация также должна соответствовать любым политикам организации по раскрытию информации. В ходе обработки инцидентов, при вовлечении в процесс третьего лица, информация может быть опубликована или изменена. Область действия, обстоятельства и цель такого опубликования информации должны быть описаны или упомянуты в соответствующих политиках и процедурах. Примером руководства по раскрытию и маркировке информации является использование протокола TLP;

- политику хранения и обработки информации, которая требует, чтобы записи, данные и другая информация, связанная с расследованиями, хранились надежно и обрабатывались способом, соответствующим их конфиденциальности. Если организация применяет маркировку документов или имеется схема классификации документации, такая политика также будет важна для деятельности по управлению инцидентами ИБ и персонала;

- положение ГРИИБ, которое более подробно определяет деятельность ГРИИБ, и полномочия, в соответствии с которыми группа действует. Как минимум, положение должно включать в себя формулировку миссии, определение области действия ГРИИБ и подробную информацию об источнике финансирования (или спонсоре для частных ГРИИБ) на уровне высшего руководства, полномочном органе ГРИИБ, контактную информацию, список услуг и основных видов деятельности группы, область действия ее полномочий и деятельности, цели и задачи, а также структуру управления:

1) цели и задачи ГРИИБ особенно важны и требуют четкого, однозначного определения;

2) область действия ГРИИБ обычно охватывает все информационные системы, услуги и сети организации. В некоторых случаях организация может потребовать, чтобы область действия была изменена (стала более расширенной, либо наоборот - ограниченной), и в этом случае необходимо четко задокументировать, что находится в области действия ГРИИБ и вне ее;

3) примеры полномочий ГРИИБ включают поиск и конфискацию личных вещей, задержание людей и мониторинг сообщений;

4) управление ГРИИБ может включать в себя определение должностного лица, члена совета директоров или топ-менеджера, который имеет полномочия принимать решения по ГРИИБ, а также устанавливать уровни полномочий для группы. Это поможет всему персоналу организации понять назначение ГРИИБ, что является жизненно важной информацией для укрепления доверия к группе. Следует отметить, что до того, как эта деталь будет обнародована, ее следует проверить с юридической точки зрения. В некоторых случаях раскрытие информации о полномочиях группы может подвергнуть ее требованиям об ответственности;

- обзор программы тренингов по повышению осведомленности по управлению инцидентами ИБ. Обзор должен включать в себя любые мандаты, политики или требования в отношении подготовки персонала по повышению осведомленности сотрудников и обучения управлению инцидентами для членов ГРИИБ.

5 Обновление политики управления инцидентами информационной безопасности

5.1 Общие положения

В разделе 5 подробно описано содержание O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) (5.2, перечисление b)).

Организация должна включать вопросы управления инцидентами ИБ в свою политику ИБ как на корпоративном уровне, так и на уровне определенной системы, услуги и сети и должна соотносить эти вопросы с политикой управления инцидентами. Интеграция должна быть направлена на достижение следующего:

a) описание, почему важно управление инцидентами ИБ, в частности, отчетность и план обработки инцидентов ИБ;

b) обозначение заинтересованности высшего руководства в необходимости надлежащей подготовки и реагирования на инциденты ИБ, то есть на план управления инцидентами ИБ;

c) обеспечение согласованности различных политик;

d) обеспечение спланированного, систематического и адекватного реагирования на инциденты ИБ, что позволит свести к минимуму неблагоприятное воздействие инцидентов.

Руководство по определению и управлению рисками ИБ приведено в O‘z DSt ISO/IEC 27005.

5.2 Взаимосвязь документов политики

Организация должна обновлять и поддерживать свои корпоративные политики ИБ и управления рисками, а также конкретные политики безопасности системы, службы или сети одновременно, чтобы гарантировать, что они остаются непротиворечивыми и действующими. Эти политики корпоративного уровня должны прямо указывать на политику управления инцидентами ИБ и связанные с ней планы.

Политика корпоративного уровня должна включать требование о необходимости создания надлежащих механизмов анализа. Эти механизмы анализа должны обеспечивать, чтобы информация, связанная с выявлением, мониторингом и разрешением инцидентов ИБ, а также с обработкой подтвержденных уязвимостей ИБ использовалась в качестве исходных данных для процесса, призванного поддерживать постоянную эффективность политик.

6 Разработка плана управления инцидентами информационной безопасности

6.1 Общие положения

В разделе 6 подробно описано содержание O‘z DSt 3386:2019 (ISO/IEC 27035-1;2016, MOD) (5.2, перечисление c)).

Целью плана управления инцидентами ИБ является документирование действий и процедур для обработки событий, инцидентов и уязвимостей ИБ, а также их взаимодействия. Этот план основывается на политике управления инцидентами ИБ.

В целом, документация плана должна включать в себя множество документов, включая формы, процедуры, организационные элементы и инструментальные средства поддержки для выявления и отчетности, оценки и принятия решений, ответного реагирования и извлеченного опыта из инцидентов ИБ.

Этот план может включать в себя детально проработанную схему основных мероприятий по управлению инцидентами для обеспечения структуры и указателей на различные детализированные компоненты плана. Эти компоненты предоставят пошаговые инструкции для обработчиков инцидентов, чтобы те придерживались метода использования определенных инструментов, следования определенным рабочим процессам или обработки определенных типов инцидентов, исходя из ситуации.

План управления инцидентами ИБ вступает в силу каждый раз, когда выявляется событие ИБ или сообщается об уязвимости ИБ.

Организация должна использовать план в качестве руководства для:

a) реагирования на события ИБ;

b) определения того, становятся ли события ИБ инцидентами;

c) управления инцидентами ИБ вплоть до их разрешения;

d) реагирования на уязвимости ИБ;

e) требований к отчетности;

f) требований к хранению информации (включая ее формат) в течение всего процесса управления инцидентами;

g) правил и обстоятельств, при которых может осуществляться обмен информацией с внутренними и внешними группами или организациями;

h) определения извлеченного опыта и любых требуемых улучшений в плане и/или безопасности в целом;

i) реализации этих выявленных улучшений.

Планирование и подготовка плана реагирования на инциденты должны проводиться владельцем процесса с четкой целью или набором целей для

реагирования на инциденты в рамках определенной области действия, основанной на политике управления инцидентами ИБ.

6.2 Согласованная разработка плана управления инцидентами информационной безопасности

Настоящий стандарт рекомендует разработку политики управления инцидентами ИБ. Однако в тех случаях, когда отсутствует руководящая политика, стандарт или другой нормативный документ, процесс планирования управления инцидентами должен основываться на согласованном мнении всех сторон для обеспечения эффективной работы, связи и отношений с внешними организациями.

Термины и определения должны быть унифицированы между членами ГРИИБ и организациями-партнерами. Сюда входят наименования и идентификаторы организаций и групп, информационные активы, бизнес-процессы и т.д. Если терминология является трудной или подверженной неправильной интерпретации, план управления инцидентами должен включать стандартные термины и определения в глоссарии.

Роли и отношения с внешними ГРИИБ и другими организациями по реагированию на инциденты, а также структура и границы деятельности при реагировании должны быть определены владельцем процесса управления инцидентами. Ответственность вовлеченных сторон может совпадать и должна быть скорректирована на основе согласованного мнения в процессе планирования управления инцидентами. При совпадении границ принятия решений по инциденту, в плане должна быть указана конкретная ответственная сторона.

Вовлеченные стороны и внешние ГРИИБ часто имеют несопоставимые количественные показатели. Участники планирования должны оценивать имеющиеся количественные показатели, предоставляемые им соответствующими сторонами или внешними организациями и, либо соглашаться на основе согласованного мнения относительно определенного набора существующих количественных показателей, либо соглашаться связать несопоставимые показатели, используя метод двухстороннего (взаимного) сопоставления. Независимо от подхода, план должен выбирать или связывать количественные показатели, чтобы их области действия были идентичны и выбирать или связывать качественные показатели с фиксированным равенством.

6.3 Вовлеченные стороны

Организация должна обеспечить, чтобы план управления инцидентами ИБ был доведен до сведения всего ее персонала и взаимодействующих с ней

подрядчиков, провайдеров ИТ-услуг, провайдеров услуг телекоммуникаций и аутсорсинговых компаний, включая следующее:

a) выявление и отчетность о событиях ИБ (это ответственность любого штатного (постоянного) или внештатного (привлекаемого на основании договора) персонала организации и ее филиалов);

b) оценка и реагирование на события и инциденты ИБ, участие в мероприятиях (после разрешения инцидента) по изучению полученного опыта и улучшению ИБ и самого плана управления инцидентами ИБ (это ответственность координаторов, ГРИИБ, управленческого персонала, персонала по связям с общественностью и законных представителей);

c) отчетность по уязвимостям ИБ (это ответственность любого постоянного или привлекаемого на основании договора персонала в организации и ее филиалах) и их обработке.

В плане также должны учитываться любые сторонние организации, а также инциденты ИБ и связанные с ними уязвимости, сообщенные сторонними организациями, а также государственными и негосударственными организациями, предоставляющими информацию по инцидентам и уязвимостям ИБ.

Если предполагается, что вовлеченные стороны будут активно участвовать в обработке инцидентов ИБ, тогда должно быть проведено четкое разделение ролей и обязанностей, о чем каждая сторона должна быть проинформирована. Разделение ролей должно сопровождаться согласованным протоколом передачи информации об инциденте для обеспечения обмена информацией соответствующим образом. Если это необходимо и возможно, для ускорения процесса необходимо автоматизировать процесс передачи инцидента и обмена информацией о нем. Такое развитие событий может возникнуть, если некоторые из возможностей организации или ГРИИБ передаются на аутсорс сторонним организациям. Примерами таких случаев являются случаи, когда организация использует облачную систему, обслуживаемую сторонней организацией, или когда сторонняя организация проводит экспертизу цифровых доказательств для данной организации, а также когда данная организация взаимодействует с поставщиком услуг при обработке инцидентов.

6.4 Содержание плана управления инцидентами информационной безопасности

Ключевые критерии принятия решений и процессы для поддержки предполагаемых этапов управления должны быть определены и рассмотрены до того, как в процессе планирования и подготовки будут изучены конкретные типы инцидентов и соответствующие процессы реагирования. Это требует наличия политики, формального или неформального понимания активов и

средств управления, а также содействия со стороны всех участников и поддержки со стороны руководства.

Содержание плана управления инцидентами ИБ должно предоставлять как общий обзор, так и специфичные подробные действия. Как отмечалось выше, документация плана должна охватывать множество документов, включая формы, процедуры, организационные элементы и вспомогательные средства.

Подробные действия, процедуры и информация должны быть связаны со следующим:

а) план и подготовка:

1) стандартизованный подход к категоризации и классификации событий и инцидентов ИБ, позволяющий обеспечить согласованные результаты. В любом случае, решение должно основываться на фактических или прогнозируемых неблагоприятных последствиях для бизнес-процессов организации и связанных с ними руководящих принципов.

Примечание - В приложении В приведены примеры подходов к категоризации и классификации событий и инцидентов ИБ;

2) база данных ИБ, сформированная для обмена информацией, предоставит возможность обмениваться отчетами и предупреждениями, сравнивать результаты, улучшать информацию о предупреждениях и обеспечивать более точное представление об угрозах и уязвимостях информационных систем. Фактический формат и использование базы данных будут зависеть от требований организации. Например, малая организация может использовать документы, в то время как более крупная организация может использовать более сложные технологии, такие как служебные базы данных и прикладные инструментальные средства;

3) руководящие принципы для определения необходимости эскалации в течение каждого соответствующего процесса, с указанием ответственных лиц и связанных процедур. Основываясь на руководящих принципах, представленных в плане управления инцидентами ИБ, любой, кто оценивает событие, инцидент или уязвимость ИБ, должен знать, при каких обстоятельствах и кому необходимо эскалировать процесс. Кроме того, могут возникнуть непредвиденные обстоятельства, при которых процесс эскалации необходим. Например, незначительный инцидент ИБ может перерасти в значительную или кризисную ситуацию, если его не обработать должным образом, или незначительный инцидент ИБ, не доведенный до конца через неделю, может стать серьезным инцидентом ИБ;

4) процедуры, которые необходимо соблюдать для обеспечения надлежащей регистрации всей деятельности по управлению инцидентами ИБ и проведения анализа журнала регистрации ответственным персоналом;

5) процедуры и механизмы, обеспечивающие сохранение режима контроля за изменениями, касающимися отслеживания событий, инцидентов и уязвимостей ИБ, а также обновлений отчетов ИБ и самого плана;

6) процедуры для проведения анализа доказательств ИБ;

7) процедуры и руководство по использованию СОиПВ, обеспечивающие рассмотрение соответствующих законодательных и нормативно-правовых вопросов. Руководство должно включать обсуждение преимуществ и недостатков проведения надзорной деятельности за нарушителем. Дополнительная информация о СОиПВ содержится в O‘z DSt ISO/IEC 27039;

8) руководство и процедуры, связанные с техническими и организационными механизмами, которые создаются, внедряются и эксплуатируются в целях предотвращения инцидентов ИБ и снижения их вероятности, а также для обработки инцидентов ИБ по мере их возникновения;

9) материал для программ по тренингам и повышению осведомленности о событиях, инцидентах и уязвимостях ИБ;

10) процедуры и спецификации для тестирования плана управления инцидентами ИБ;

11) план организационной структуры управления инцидентами ИБ;

12) сфера компетенции и ответственности ГРИИБ, в целом, и отдельных ее членов;

13) важная контактная информация;

14) процедуры и руководство по обмену информацией, согласованные с отделом по связям с общественностью, юридическим отделом и высшим руководством организации;

b) выявление и отчетность:

1) требования к планированию и подготовке для выявления и отчетности должны обеспечивать и поддерживать разработку и эксплуатацию процессов для поиска или принятия информации об инцидентах ИБ;

2) критерии принятия отчета об инциденте должны определяться на основе полноты отчета и подтверждения одного или нескольких событий ИБ. Для поддержки принятия последующих решений перед процессом планирования должны быть определены минимальные критерии принятия предупреждения или оповещения вручную о любом выявленном событии. Критерии, как минимум, должны включать определение затронутой среды или актива, заявление одного или нескольких потенциальных или подтвержденных событий или квалифицированного типа события, а также время получения предупреждения или оповещения. Для поддержки принятия решений процесс планирования должен включать метод возврата процесса выявления или отчетов, не имеющих достаточной информации;

3) результаты отчетности или уведомления должны определяться, исходя из контекста организации, политики реагирования на инциденты и

назначения технических и управленческих ролей. Формат отчетов и уведомлений должен соответствовать шкале классификации инцидентов или согласованным количественным показателям;

4) выявление и отчетность о событиях ИБ (с помощью ручных или автоматических средств);

5) реагирование на неправильное использование процесса отчетности (возможно включая принятие мер, выходящих за область действия плана управления инцидентами);

6) сбор информации о событиях ИБ;

7) выявление и отчетность об уязвимостях ИБ;

8) регистрация информации, собранной в базе данных ИБ;

c) оценка и принятие решений:

1) требования к планированию и подготовке для оценки и принятия решения должны позволять и поддерживать разработку и эксплуатацию процессов для оценки и направления действий при реагировании на инциденты ИБ;

2) до разработки процессов оценки и принятия решений владелец процесса должен обеспечить, чтобы была определена минимальная информация для идентификации и классификации инцидента безопасности, состоящая из конкретных элементов необходимой и вспомогательной информации. Такое определение позволит планировщикам реагирования разрабатывать согласованные процессы для полноты и классификации выявленных и зарегистрированных событий. Необходимо определить полноту информации, необходимой для разграничения истинно положительных и ложноположительных отчетов, и обеспечить накопление информации для поддержки оценки и реагирования на ложноположительные выявление и отчетность;

3) если процесс планирования по инциденту должен зависеть от автоматизированных систем управления информацией и поддержки принятия решений, следует определить функции, реализацию и текущую работу этих систем. Владелец процесса обработки инцидентов должен обеспечить, чтобы база данных ИБ была достаточно определена до разработки процессов реагирования, зависящих от нее;

4) координатор, проводящий оценку событий ИБ (включая процесс эскалации, при необходимости), используя шкалу классификации событий/инцидентов ИБ (включая определение влияния событий на основе затронутых активов/служб) должен решить, следует ли классифицировать события как инциденты ИБ;

5) ГРИИБ, оценивающая события ИБ, должна подтвердить, является ли событие инцидентом ИБ или нет. Для этого необходимо провести еще одну оценку, используя шкалу классификации событий/инцидентов ИБ, чтобы подтвердить детали типа события (предполагаемого инцидента) и

затронутого ресурса (категоризация). За этим должны следовать решения, касающиеся того, как должен быть обработан подтвержденный инцидент ИБ, кем и с каким приоритетом, а также уровнем эскалации;

6) оценка уязвимостей ИБ (которые еще не были использованы и не стали причиной возникновения событий ИБ и потенциальных инцидентов ИБ) с принятием решений по их разрешению, с кем, каким образом и с каким приоритетом;

7) полная запись всех результатов оценки и соответствующих решений в базу данных ИБ;

d) ответное реагирование:

1) требования к планированию и подготовке к ответному реагированию должны обеспечивать и поддерживать разработку и реализацию процессов реагирования на инциденты ИБ. Перед планированием процесса реагирования владелец процесса обработки инцидентов должен обобщить критерии определения или создать рабочие пороговые значения или категории для приоритета информации и информационной системы, воздействия каждого типа вторжения, шкалы ущерба, уровня сигнализации о вторжении и степени серьезности. Они могут быть качественными или количественными, если они согласуются с подготовкой оценки и принятия решений и позволяют члену ГРИИБ поручать (выдавать задание) исполнителям выполнение ответных действий на инцидент;

2) классы реагирования также должны быть определены до процесса планирования, и сформированы по затратам, времени, минимуму технических ресурсов и другим показателям, чтобы дать возможность назначить класс ответа применительно к известной информации о сообщенном и оцененном инциденте. Также необходимо определить процесс немедленного или отложенного реагирования и управление отдельными или циклическими задачами по инциденту в этом процессе;

3) анализ ГРИИБ для определения нахождения инцидента ИБ под контролем:

- если инцидент находится под контролем, запрос требуемого реагирования либо немедленно (в режиме реального времени или практически немедленно), либо позднее;

- если инцидент не находится под контролем или он оказывает серьезное влияние на ключевые службы организации, запрос антикризисных мероприятий посредством эскалации до функции урегулирования кризисов;

4) определение схемы всех внутренних и внешних функций и организаций, которые должны участвовать в управлении инцидентом;

5) сдерживание и ликвидация инцидента ИБ, при необходимости, для смягчения или предотвращения расширения области действия и воздействия инцидента;

6) проведение анализа доказательств ИБ, при необходимости;

7) процесс эскалации, при необходимости;

8) обеспечение надлежащей регистрации действий всех участников процесса для последующего анализа;

9) обеспечение идентификации, сбора, получения и сохранения цифровых доказательств;

10) обеспечение функционирования режима контроля за изменениями и, таким образом, поддержание базы данных ИБ в актуальном состоянии;

11) сообщение о наличии инцидента ИБ или любых соответствующих подробностей другим внутренним и внешним организациям;

12) обработка уязвимостей ИБ;

13) официальное закрытие инцидента после успешной обработки и внесение записи о нем в базу данных ИБ;

14) последующая за инцидентом деятельность при необходимости должна включать дальнейший анализ процессов реагирования на инциденты ИБ;

e) организация должна обеспечить, чтобы документация по управлению инцидентами ИБ позволяла реагировать на эти инциденты как в безотлагательном, так и в долгосрочном плане. Все инциденты ИБ должны пройти раннюю оценку потенциального негативного воздействия на бизнес-процессы, как краткосрочные, так и долгосрочные (например, существенный сбой может произойти спустя некоторое время после первичного инцидента ИБ). Кроме того, необходимо предусмотреть процессы реагирования, необходимые для таких инцидентов ИБ, которые полностью непредвиденны и когда требуются ситуативные средства управления. В любом случае, организации должны включать общие руководящие принципы в документацию по плану;

f) извлеченный опыт:

1) определение опыта, извлеченного из инцидентов и уязвимостей ИБ;

2) изучение, выявление и усовершенствование реализации средств управления ИБ (новые и/или обновленные средства управления), а также самой политики управления инцидентами ИБ, исходя из извлеченного опыта;

3) изучение, выявление и, по возможности, усовершенствование существующей системы определения и управления рисками ИБ организации, исходя из извлеченного опыта;

4) изучение эффективности процессов, процедур, форматов отчетности и/или организационной структуры, отвечающих за оценку и восстановление после каждого инцидента ИБ и устранения уязвимостей ИБ, а также на основе извлеченного опыта определение и совершенствование плана управления инцидентами ИБ и соответствующей документации;

5) обновление базы данных ИБ;

6) взаимодействие и обмен результатами анализа внутри доверенного круга лиц (по желанию организации).

6.5 Классификация инцидентов

Для оценки событий и инцидентов следует использовать шкалу классификации событий и инцидентов ИБ. В любом случае, решение должно основываться на фактическом или прогнозируемом неблагоприятном воздействии на бизнес-процессы организации.

Примечание - В приложении В приведены примеры подходов к категоризации и классификации событий и инцидентов ИБ.

6.6 Формы отчетов о событиях и инцидентах

Формы отчетов о событиях и инцидентах, если они используются, должны быть созданы до того, как они понадобятся. Количество, тип и формат форм должны определяться ГРИИБ и периодически пересматриваться для обеспечения их актуальности. Необходимо наличие дополнительного типа формы с описанием определенной информации. Его цель - предоставить механизм для сбора информации в случаях, когда существующие формы недостаточны или соответствующая форма еще не создана.

Персонал, сообщающий о событиях и инцидентах информационной безопасности, должен быть оповещен о наличии форм отчетов о событиях и инцидентах, должен получить эти формы и ознакомиться с ними.

Примеры форм показаны в приложении С.

Рекомендуется использовать общепризнанные стандартизированные форматы электронного обмена и ввода информации об инцидентах, связанных непосредственно с электронной базой данных ИБ. Использование стандартизованного формата электронного обмена позволяет увеличить автоматизацию обработки данных и может уменьшить усилия по корреляции информации, когда несколько групп сотрудничают при обработке инцидента. Бумажная схема может потребоваться для случая, когда электронная схема не может быть использована.

6.7 Процессы и процедуры

Прежде чем приступить к работе над планом управления инцидентами ИБ важно, чтобы организация документировала и проверяла наличие необходимых процессов и процедур.

Примечание - Для удобства, в нижеследующем тексте термин «документ» будет использоваться для обозначения как процессов, так и процедур, если различие между процессом и процедурой не является значительным.

В каждом документе должны указываться группы или лица, ответственные за его использование и управление.

Важно понимать, что не все документы должны быть легко доступны как внутри организации, так и для широкой общественности. Например, всему персоналу организации не обязательно понимать внутреннюю работу ГРИИБ для взаимодействия с ней. ГРИИБ должна обеспечить, чтобы имеющееся руководство, включая информацию, полученную в результате анализа инцидентов ИБ, находилось в легкодоступной форме, например, на корпоративном портале организации и/или на общедоступном веб-сайте, в зависимости от ситуации. Также может быть важно сохранить в тайне некоторые детали плана управления инцидентами ИБ для предотвращения вмешательства инсайдера в процесс расследования. Например, если сотрудник банка, расхищающий его средства, осведомлен о каких-либо подробностях проведения расследования, он может быть в состоянии лучше скрыть свою деятельность от следователей или иным образом препятствовать обнаружению, расследованию и восстановлению после инцидента ИБ.

Содержание операционных процедур зависит от ряда критериев, в особенности связанных с характером известных потенциальных событий, инцидентов и уязвимостей ИБ, а также типов активов информационной системы, которые могут быть задействованы, и их среды. Таким образом, операционная процедура может быть связана с конкретным типом инцидента или продукта (например, межсетевыми экранами, базами данных, операционными системами, приложениями) или конкретным продуктом. Каждая операционная процедура должна четко определять шаги, которые необходимо предпринять и ответственное за них лицо. Она должна отражать опыт внешних (например, государственных и частных ГРИИБ, поставщиков) и внутренних источников.

Необходимо наличие операционных процедур для борьбы с типами событий и инцидентов ИБ, которые уже известны, а также уязвимостями. Также должны быть соблюдены рабочие процедуры, когда идентифицированное событие, инцидент или уязвимость ИБ не имеют какого-либо известного типа. В этом случае необходимо рассмотреть следующее:

a) процесс отчетности для обработки таких исключений;

b) руководящие указания по срокам получения разрешения от руководства организации во избежание любой задержки реагирования;

c) предварительно уполномоченное делегирование принятия решений при отсутствии нормального процесса разрешения.

Эксплуатационные процедуры для ГРИИБ должны разрабатываться с учетом документированных процессов и связанных с ними обязанностей и распределения ролей назначенным лицам для проведения различных мероприятий (физическому лицу может быть выделено более одной роли

в зависимости от размера, структуры и организационной деятельности), в том числе:

- прекращение работы затронутой системы, службы и/или сети при определенных обстоятельствах, согласованных по предварительной договоренности с соответствующим ИТ-отделом и/или руководством;
- поддержание затронутой системы, службы и/или сети в подключенном и работающем состоянии;
- мониторинг данных (поступающих, исходящих и циркулирующих внутри) затронутой системы, службы и/или сети;
- активация шаблонных процедур и мероприятий резервного копирования и антикризисного управления в соответствии с политикой безопасности системы, службы и/или сети;
- мониторинг и поддержание безопасного хранения цифровых доказательств для случаев следственных действий или внутренних дисциплинарных мер;
- передача информации о деталях инцидента ИБ внутренним и внешним организациям. Это может включать в себя взаимодействие с несколькими внешними сторонами, такими как другие группы реагирования на инциденты, организации по обмену информацией, провайдеры интернет-услуг, поставщики программного обеспечения и технической поддержки, правоохранительные органы, клиенты, средства массовой информации и другие причастные стороны. Все контакты и взаимодействие с внешними сторонами должны быть задокументированы в целях обеспечения ответственности и доказательств.

6.8 Доверие

ГРИИБ играет решающую роль в обеспечении общей ИБ организации. Для эффективной работы при выявлении, разрешении и расследовании инцидентов ИБ ГРИИБ необходимо взаимодействие всего персонала организации. Принципиально важно доверие ГРИИБ как внутри своей организации, так и со стороны внешних организаций. Доверие внутри организации основывается на поддержке высшего руководства (т.е. доверие присутствует изначально), в то время как внешние организации, имеющие дело с ГРИИБ (например, ГРИИБ других организаций), должны быть уверены в том, что ГРИИБ будет выполнять свою работу профессионально (т.е. доверие необходимо заслужить).

ГРИИБ может получить доверие применением прозрачных и тщательно обдуманных процессов. ГРИИБ должна проводить мероприятия по обучению пользователей (внутренних и внешних), пояснению деятельности ГРИИБ, обеспечению конфиденциальности собранной информации,

обращению с отчетами о событиях, инцидентах и уязвимостях ИБ. ГРИИБ должна документировать и публиковать положения, которые наглядно указывают на анонимность (или ее отсутствие) лиц или сторон, сообщающих о потенциальном инциденте или уязвимости ИБ.

ГРИИБ должна быть способна эффективно удовлетворять функциональные, финансовые, юридические и политические потребности организации и проявлять осмотрительность при управлении инцидентами и уязвимостями ИБ. Деятельность ГРИИБ также должна независимо проверяться для подтверждения эффективного исполнения всех требований бизнеса.

Кроме того, хорошим способом достижения дополнительного фактора независимости является разделение цепочки отчетности об инцидентах и уязвимостях от действующей линии управления и прямое назначение руководителя высшего звена ответственным за руководство реагированием на инциденты и уязвимости. Финансовая деятельность также должна быть отделена во избежание чрезмерного влияния.

6.9 Обработка конфиденциальной информации

План управления инцидентами ИБ может содержать конфиденциальную информацию, и лица, занимающиеся устранением инцидентов и уязвимостей, могут столкнуться с необходимостью обработки конфиденциальной информации. Организация должна наладить необходимые процессы для обеспечения безопасности конфиденциальной информации, при необходимости. Если события, инциденты, уязвимости регистрируются через единую систему управления проблемами, в которой невозможно ограничить доступ к ней, возможно понадобится исключить конфиденциальные данные. Следует предусмотреть наличие доступа ГРИИБ к исключенной информации, это возможно в том случае, если ГРИИБ будет поддерживать свою собственную базу данных ИБ.

Как уже отмечалось, организации следует также обеспечить, чтобы план управления инцидентами ИБ предусматривал контроль за взаимодействием по инцидентам и уязвимостям с внешними сторонами, включая средства массовой информации, бизнес-партнеров, клиентов, правоохранительных органов и широкую общественность.

7 Создание группы реагирования на инциденты информационной безопасности

7.1 Общие положения

В разделе 7 подробно описано содержание O‘z DSt 3386 (ISO/IEC 27035-1:2016, MOD) (5.2, перечисление d)).

Цель создания ГРИИБ заключается в предоставлении организации соответствующих возможностей для оценки, реагирования и изучения опыта из инцидентов ИБ, а также обеспечении необходимой координации, управления, обратной связи и коммуникации. ГРИИБ способствует уменьшению физического и денежного ущерба, а также снижению репутационных потерь организации, которые зачастую бывают связаны с инцидентами ИБ.

В зависимости от размера организации, ее персонала и отрасли, ГРИИБ может быть организована по-разному.

7.2 Типы и роли ГРИИБ

ГРИИБ должна иметь определенный круг заинтересованных лиц, в рамках которого она осуществляет свою основную деятельность. Этот круг может быть определен различными способами и включать (но не ограничиваться) следующие области действия:

- сотрудники организации;
- назначенный определенный диапазон IP-адресов;
- определенная автономная система с IP-маршрутизацией;
- определенный домен (например, example.uz);
- имеющиеся клиенты какого-либо продукта;
- имеющиеся клиенты коммерческой услуги по реагированию на инциденты;
- население региона или страны.

Круг заинтересованных лиц может пополняться участниками в результате договорных соглашений (например, при приобретении услуги или продукта) или исходя из положений законодательства (например, создание национальной Службы реагирования на компьютерные инциденты).

Характеристики и размер круга заинтересованных лиц, а также уровень полномочий и контроля, который ГРИИБ имеет над его участниками, будут влиять на виды услуг, которые может предложить ГРИИБ, и соответствующую форму организации их предоставления. Например, ГРИИБ может самостоятельно выполнять реагирование на инцидент (как корпоративное, так и по договору), координировать работу других ГРИИБ, или предоставлять

информацию и помогать отдельным участникам по запросу (например, ГРИИБ какого-либо продукта).

Независимо от того, какие услуги предлагает ГРИИБ, ей потребуется политика реагирования (определение того, что представляет собой инцидент, какое ответное реагирование требуется и какие полномочия должна предоставить ГРИИБ), процесс реагирования (определение того, как группа будет реагировать на заданный инцидент с заданным процессом реагирования) и оперативные возможности для осуществления этого процесса.

Несмотря на то, что основная роль ГРИИБ заключается в реагировании на инциденты (независимо от того, были ли они обнаружены в своих системах мониторинга, сообщены из круга заинтересованных лиц или из внешних источников), многие группы также вносят свой вклад профилактического характера, улучшая стандарты безопасности и практику в своих кругах заинтересованных лиц, с тем чтобы уменьшить вероятность и/или тяжесть инцидентов. ГРИИБ также может иметь административную роль, например, при отчетности и управлении собственными политиками, процессами и ресурсами.

ГРИИБ могут быть организованы различными способами, в том числе по сфере отрасли, направленности круга заинтересованных лиц, организационной структуре или другим атрибутам. Один из методов организации структуры основывается на типе области проводимого мониторинга, и в этом случае существует три разных типа, как показано на рисунке 1: одиночный, иерархический и удаленный. При создании ГРИИБ следует учитывать размер организации, важность информации и функциональное взаимодействие с другими организациями. На рисунке 1 буквой «Ц» обозначены цели, мониторинг которых выполняется определенными ГРИИБ:

- одиночный тип ГРИИБ. Область мониторинга - это одиночная организация или одна ГРИИБ, осуществляющая мониторинг нескольких организаций или целей. Этот тип обычно используется для управления инцидентами, реагирования и эксплуатационной деятельности;

- иерархический тип ГРИИБ. Одна или несколько ГРИИБ перекрывают области мониторинга. Это повышает надежность действий по реагированию на инциденты;

- удаленный тип ГРИИБ. Данный тип обобщает события ИБ из удаленных местоположений и обычно используется предприятиями, предоставляющими аутсорсинг (специализированные предприятия ИБ) для мониторинга целей.

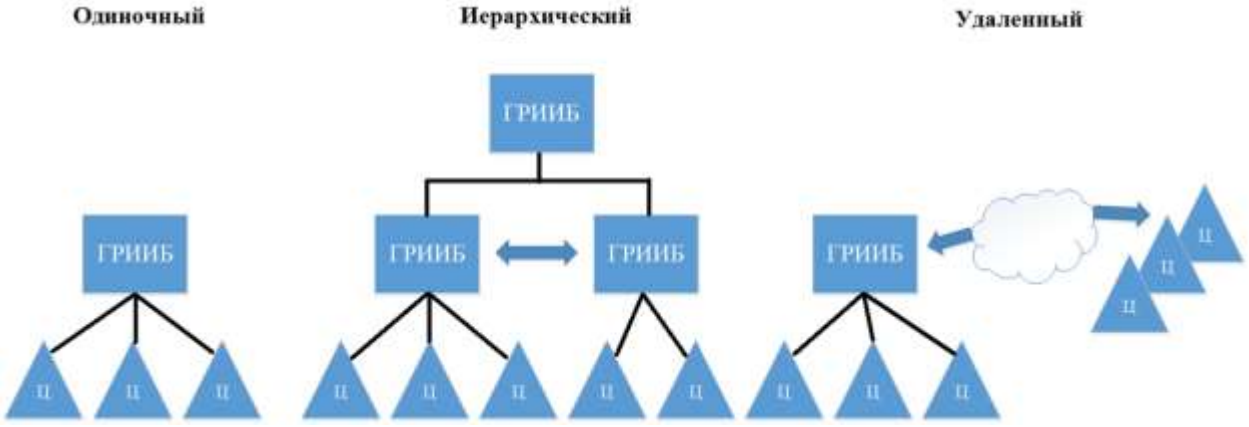

Рисунок 1 - Примеры структуры ГРИИБ

Основные виды деятельности ГРИИБ могут включать (но не ограничиваться) следующее:

- управление интегрированными системами безопасности. Мониторинг и управление агентами, установленными на гетерогенных системах (например, СОиПВ, межсетевой экран, сетевой ресурс и т.д.);

- внедрение согласованной политики. Минимизация рисков для информационной системы путем применения согласованного набора задач реагирования в соответствии с обозначенной политикой;

- безотлагательное реагирование. Быстрое реагирование на угрозы, нарушения и атаки для минимизации ущерба и снижения затрат на восстановление.

Обязанности ГРИИБ также могут включать в себя деятельность по мониторингу и управлению, в соответствии с нижеследующим:

- интегрированное управление и мониторинг. Круглосуточный мониторинг целей, превентивный мониторинг и реагирование на инциденты, управление журналами регистрации;

- управление отчетами. Периодическая отчетность по безопасности, управление исправлениями (патчами) безопасности, отчеты по инцидентам;

- административное управление. Управление политикой для различных системных сред, включая управление задачами и деятельность ГРИИБ;

- техническое управление. Управление сетью, системой, приложением, контентной частью и службой безопасности;

- эксплуатация и управление системой. Пропускная способность системы, производительность, конфигурация безопасности и управление конфигурацией среды.

Примечание - Некоторые из перечисленных обязанностей могут передаваться или выполняться другими организационными подразделениями вне ГРИИБ.

7.3 Персонал ГРИИБ

Эффективное реагирование на инцидент зависит от способностей и добросовестности персонала ГРИИБ. Персонал ГРИИБ и его способности становятся еще более важными, если деятельность ГРИИБ включает в себя разработку политики управления инцидентами ИБ, аудит, координацию с другими отделами и совершенствование технических мероприятий. Навыки, необходимые для персонала ГРИИБ, могут включать следующее:

a) личные навыки: коммуникабельность, решение проблем, взаимодействие с группой, управление временем и проектами;

b) технические навыки: принципы безопасности, анализ рисков, моделирование угроз, анализ уязвимостей, анализ журналов регистрации;

c) навыки реагирования на инциденты: политика и процедуры группы, анализ инцидентов, запись и отслеживание информации об инцидентах;

d) специализированные навыки: представление себя, лидерские навыки, понимание вопроса (по инциденту), программирование.

Для реагирования на различные типы инцидентов, персонал ГРИИБ должен обладать техническими знаниями и навыками, такими как:

- существующие проблемы сетевой безопасности, включая атаки, угрозы, вредоносный код и уязвимости;
- методы безопасности системного администрирования, такие как управление исправлениями (патчами), безопасная настройка, резервное копирование и аварийное восстановление;
- криптография (алгоритмы шифрования и хеширования), цифровые подписи, протоколы защиты данных, такие как SSL/TLS;
- общие сетевые протоколы, такие как Ethernet, Wi-Fi, IPv4, IPv6, ICMP, UDP, TCP;
- общие протоколы сетевых приложений, такие как DNS, SMTP, HTTP/HTTPS;
- сбор цифровых доказательств, обратный инжиниринг;
- общие понятия компьютерной науки и программирования, такие как энтропия, безопасная разработка, функциональное и объектно-ориентированное программирование, архитектура системы и распределение ячеек памяти.

Другие специфичные знания и навыки должны определяться обязанностями ГРИИБ и технологиями, используемыми организацией. Примеры в приведенном списке являются актуальными на момент разработки настоящего стандарта. Персонал ГРИИБ должен поддерживать актуальные знания и навыки.

Для организации ГРИИБ можно определить роли участников, как показано в таблице 1. Некоторые из этих задач могут передаваться или

выполняться другими организационными подразделениями вне ГРИИБ. ГРИИБ может предоставлять вводные данные, но не иметь окончательных полномочий.

Таблица 1 - Примеры ролей и задач персонала ГРИИБ

Роль	Описание
Руководитель ГРИИБ	Руководитель несет ответственность за управление персоналом, определением области действия работ и предоставления отчетности о текущем положении организациям более высокого уровня
Планировщик	Ответственный за функционирование ГРИИБ. Устанавливает или планирует различные политики безопасности, сообщает о них вышестоящим инстанциям, сотрудничает с третьими сторонами, регистрирует и утверждает отчеты об уязвимостях. Его роли заключаются в следующем: - создание и планирование политики безопасности; - внедрение процессов безопасности; - корректировка приоритетов рисков; - взаимодействие с организациями более высокого уровня и другими сторонними организациями; - поддержка администрации; - обсуждение, регистрация, утверждение отчетов об уязвимостях для целевых организаций; - выполнение других мероприятий по указанию руководителя ГРИИБ
Сотрудник по мониторингу	Ответственный за мониторинг в режиме реального времени и фактическую деятельность, такую как мониторинг, выявление, идентификация событий ИБ, регистрация инцидентов и их предотвращение. Осуществляет мероприятия по мониторингу безопасности в режиме реального времени и следующее: - мониторинг и деятельность в круглосуточном режиме; - обнаружение вторжений, регистрацию инцидентов и первичное реагирование; - установку исправлений (патчей) и обновлений безопасности; - внедрение политики безопасности и управление резервными копиями;

Окончание таблицы 1

Роль	Описание
	- службу поддержки; - управление объектами; - выполнение других мероприятий по указанию руководителя ГРИИБ
Сотрудник по реагированию	Обрабатывает каждый запрос от агентов по мониторингу по инцидентам, связанным с вторжением, хищением, фильтрацией или раскрытием данных; выполняет вторичный дальнейший анализ и действия, включая мероприятия по расследованию, восстановительные мероприятия и установление адекватной стратегии. Оказывает услуги по реагированию в режиме реального времени, технической поддержке, а также следующее: - распространение и отчетность по инцидентам; - корреляционный анализ между системами мониторинга; - поддержку расследования инцидентов и восстановления; - анализ уязвимости в целевой организации и ГРИИБ; - выполнение других мероприятий по указанию руководителя ГРИИБ
Аналитик	В сотрудничестве с группой реагирования проводит углубленный анализ, включая корреляционный анализ инцидентов, а также следующее: - планирование анализа уязвимости для целевой организации и ГРИИБ; - совершенствование инструментов анализа безопасности и контрольного списка; - совершенствование правил мониторинга; - публикацию информационного бюллетеня; - выполнение других мероприятий по указанию руководителя ГРИИБ

В таблице 2 приведен пример типов кадрового обеспечения, позиций и задач для различных должностей, которые могут потребоваться ГРИИБ.

Таблица 2 - Пример должностей ГРИИБ

Должность	Задачи
Руководитель группы	- обеспечивает стратегическое направление; - обеспечивает и облегчает работу членов группы; - курирует группу; - представляет ГРИИБ руководству и другим подразделениям; - интервьюирует и нанимает новых членов группы
Помощники руководителей группы	- поддерживают стратегическое направление назначенной функциональной области; - поддерживают руководство командой по мере необходимости; - обеспечивают руководство и наставничество для членов группы; - назначают задачи и обязанности; - участвуют в интервью с новыми членами группы
Персонал службы поддержки	- обрабатывает телефонные звонки, поступившие в ГРИИБ с информацией об инцидентах или нарушениях безопасности; - оказывает первичную помощь, в зависимости от навыков; - осуществляет ввод исходных данных и сортировку и определение приоритетов поступающей информации
Обработчики инцидентов	- проводят анализ, отслеживание, запись и реагирование на инциденты; - координируют активное и превентивное руководство, которое будет предоставлено кругу заинтересованных лиц (разработка документации, контрольных списков, передовой практики и руководящих принципов); - распространяют информацию; - взаимодействуют должным образом с ГРИИБ, внешними экспертами и другими субъектами (например, веб-сайт, средства массовой информации, правоохранительные органы или юридический отдел) путем назначения от руководителя группы или другого управленческого персонала; - проводят технологические наблюдения, если они назначены;

Окончание таблицы 2

Должность	Задачи
	- разрабатывают соответствующие учебные материалы (для персонала ГРИИБ и/или круга заинтересованных лиц); - наставляют новых членов ГРИИБ при назначении; - контролируют системы обнаружения вторжений, если эта услуга является частью деятельности ГРИИБ; - выполняют тестирование на проникновение, если эта услуга является частью деятельности ГРИИБ; - участвуют в интервью с новыми сотрудниками ГРИИБ, по соответствующему указанию
Обработчики уязвимостей	- анализируют, тестируют, отслеживают и записывают отчеты об уязвимостях и доказательства уязвимостей; - исследуют или разрабатывают исправления (патчи) в рамках усилий по реагированию на уязвимость; - взаимодействуют с кругом заинтересованных лиц, ГРИИБ, разработчиками программного обеспечения, внешними экспертами (другими ГРИИБ, исследователями, поставщиками) и другими субъектами (средства массовой информации, правоохранительные органы или юридический отдел), по мере необходимости; - распространяют информацию об уязвимостях и соответствующих исправлениях (патчах) или обходных решениях; - проводят технологические наблюдения, если они назначены; - наставляют новых членов ГРИИБ при назначении; - участвуют в интервью с новыми членами ГРИИБ
Разработчики технической документации	- оказывают помощь и содействуют ГРИИБ в разработке таких публикаций, как консультативные заключения, применение передовой практики или технические советы

8 Взаимодействие с другими подразделениями организации и другими организациями

8.1 Общие положения

В разделе 8 подробно описано содержание O‘z DSt 3386:2019 (ISO/IEC 27035-1;2016, MOD) (5.2, перечисление e)).

Необходимо установить и поддерживать соответствующие отношения и связи с внутренними и внешними организациями, которые непосредственно вовлечены в управление событиями, инцидентами и уязвимостями ИБ.

8.2 Взаимодействие с другими подразделениями организации

Управление инцидентами не является самодостаточным процессом. Отношения, каналы связи, соглашения о совместном использовании данных, а также политики и процедуры должны устанавливаться во всей организации. Взаимодействие ГРИИБ с другими подразделениями организации может включать взаимодействие со следующими участниками:

- бизнес-менеджеры. Им нужно понять, что представляет собой ГРИИБ и как она может помочь в поддержке их бизнес-процессов. Должны быть достигнуты договоренности относительно полномочий ГРИИБ над бизнес-системами и ответственного лица, который будет принимать решения, если возникнет необходимость в отключении от сети или прекращении функционирования критически важных бизнес-систем;

- ИТ-представители. Необходимо определить взаимодействие и рабочий процесс между ИТ-персоналом и ГРИИБ, включая действия, которые будут предприняты ИТ-персоналом и членами ГРИИБ, а также какую информацию ИТ-персонал может предоставить ГРИИБ, а какую ГРИИБ может предоставить ИТ-отделу, и какие роли и полномочия у них имеются;

- представители юридического отдела. Эти представители могут давать рекомендации по вопросам ответственности и соблюдения законодательных требований, определяют влияние инцидентов на соглашения об уровне услуг, и предоставляют указания относительно соблюдения конфиденциальности и гражданских свобод, чтобы во время мероприятий по расследованию и реагированию не нарушались права сотрудников;

- представители отдела по работе с персоналом (отдел кадров). Их участие требуется в разработке политики и процедур в части применения мер дисциплинарного взыскания к сотрудникам организации, уличенных в несанкционированной или незаконной компьютерной деятельности;

- представители отдела по связям с общественностью. Они должны быть готовы обработать любые запросы средств массовой информации

и помогать в разработке политики в области раскрытия информации и применения передового опыта;

- любые существующие группы безопасности, включая группу обеспечения физической безопасности. ГРИИБ должна будет обмениваться информацией о компьютерных инцидентах с этими группами и может разделять с ними ответственность за решение проблем, связанных с кражей средств вычислительной техники или данных;

- специалисты по аудиту и управлению рисками. Они могут оказать помощь в разработке показателей угроз и определении рисков для систем круга заинтересованных лиц;

- любые сотрудники правоохранительных органов или следователи. Они дадут разъяснения, как ГРИИБ должна работать с правоохранительными органами, когда обращаться в правоохранительные органы и кто будет проводить расследования и криминалистическую экспертизу;

- генеральные представители круга заинтересованных лиц. Они могут обеспечить понимание своих потребностей и требований.

ГРИИБ должна нести ответственность за обеспечение разрешения инцидентов, и в этом контексте руководитель и члены ГРИИБ должны обладать полномочиями для принятия необходимых мер, которые считаются подходящими при реагировании на инциденты ИБ. Однако действия, которые могут оказать неблагоприятное воздействие в целом на организацию, будь то финансовые потери или репутационные, должны быть согласованы высшим руководством. По этой причине крайне важно, чтобы в политике и плане управления инцидентами ИБ был указан соответствующий представитель высшего руководства организации, которому руководитель ГРИИБ докладывает о серьезных инцидентах ИБ. Этот представитель высшего руководства организации, со своей стороны, должен взять на себя обязательство быть доступным членам ГРИИБ и своевременно предоставлять свои рекомендации.

Процедуры и обязанности в отношении средств массовой информации также должны быть согласованы высшим руководством и документированы. Эти процедуры должны указывать, какой отдел организации взаимодействует со средствами массовой информации, и как он взаимодействует с ГРИИБ. Все члены ГРИИБ должны быть обучены правилам взаимодействия со средствами массовой информации в соответствии с политикой в области средств массовой информации.

8.3 Взаимодействие с внешними заинтересованными сторонами

Организация должна установить отношения между ГРИИБ и соответствующими внешними заинтересованными сторонами. ГРИИБ часто приходится взаимодействовать с внешними сторонами по инциденту, и они должны

делать это при необходимости, например, при обращении в правоохранительные органы, обработке запросов средств массовой информации и поиске стороннего экспертного заключения. Другим примером является обсуждение инцидентов с другими вовлеченными сторонами, такими как провайдеры интернет-услуг, поставщики программного обеспечения с выявленной уязвимостью или другие ГРИИБ. ГРИИБ могут также заранее делиться информацией об индикаторах соответствующего инцидента с аналогичными организациями для совершенствования процессов выявления и анализа инцидентов.

Информация должна передаваться внешним сторонам исключительно в соответствии с политиками и процедурами организации и ГРИИБ, а также с законодательными нормами.

Члены ГРИИБ должны стремиться присоединиться к доверенным сообществам коллег в области применения практики ГРИИБ для повышения своих профессиональных навыков и создания доверительных отношений для обмена информацией. Обмен технической информацией с доверенными партнерами ГРИИБ на этапах выявления и отчетности при обработке инцидентов может повысить эффективность реагирования и помочь минимизировать воздействие на другие организации. Поскольку многие угрозы кибербезопасности затрагивают одновременно несколько организаций, этот тип обмена информацией считается решающим для ответственных операций ГРИИБ. Там, где это целесообразно, необходимо автоматизировать обмен информацией об инцидентах для увеличения скорости обнаружения новых инцидентов посредством коллективной деятельности ГРИИБ.

Внешние заинтересованные стороны могут включать (но не ограничиваться) следующее:

a) внештатный вспомогательный персонал, привлекаемый на основании договора;

b) ГРИИБ внешних организаций;

c) провайдеров услуг, включая провайдеров услуг телекоммуникаций, провайдеров интернет-услуг, поставщиков оборудования и/или программного обеспечения;

d) правоохранительные органы;

e) органы по чрезвычайным ситуациям;

f) соответствующие государственные органы;

g) юридический персонал;

h) должностных лиц по связям с общественностью и/или представителей средств массовой информации;

i) деловых партнеров;

j) клиентов;

k) широкую общественность.

9 Организация технической и другой поддержки

9.1 Общие положения

В разделе 9 подробно описано содержание O‘z DSt 3386 (ISO/IEC 27035-1:2016, MOD) (5.2, перечисление f)).

Организация должна приобрести, подготовить и протестировать все необходимые технические и другие вспомогательные средства для обеспечения быстрого и эффективного реагирования на инциденты ИБ. Необходимо определить все внутренние и внешние стороны по поддержке и отчетности и согласовать каналы связи и рабочий процесс. Эти действия включают следующее:

- доступ к активам организации с использованием современного реестра активов и увязки информации с бизнес-функциями;
- доступ к документированным процедурам, связанным с антикризисным управлением;
- документированные и обнародованные процессы коммуникации, включая коммуникации со средствами массовой информации, соответствующие политикам организации в отношении взаимодействия со средствами массовой информации и раскрытия информации. Например, организация может затребовать участия своих специалистов по связям с общественностью и юристконсультов во всех обсуждениях со средствами массовой информации по инцидентам;
- использование базы данных ИБ и технических средств для быстрого заполнения и обновления базы данных, анализа содержащейся в ней информации и упрощения реагирования (в некоторых случаях организации могут затребоваться ручные записи), с наглядным подтверждением сохранности базы данных в безопасном состоянии;
- использование стандартного формата и протокола обмена для приема и обработки предупреждений или информации о событиях, инцидентах, уязвимостях для информирования о состоянии ИБ операционной среды с учетом превентивной ремедиации, основанной на рисках;
- средства для сбора и анализа цифровых доказательств и доказательств ИБ;
- адекватные механизмы антикризисного управления для базы данных ИБ (руководство по управлению непрерывностью бизнеса приведено в O‘z DSt ISO/IEC 27031);
- определение внешних сторон по поддержке и отчетности, координатора между организацией и внешними сторонами, а также того, каким образом и в каком случае взаимодействовать.

Организация должна обеспечить, чтобы технические средства, используемые для быстрого заполнения и обновления базы данных, анализа содержащейся в ней информации и упрощения реагирования на инциденты ИБ, поддерживали следующее:

a) быстрое получение отчетов о событиях, инцидентах, уязвимостях ИБ;

b) уведомление ранее определенного внешнего персонала с использованием соответствующих средств (например, электронной почты, факса или телефона), что требует поддержания в актуальном состоянии надежной, легкодоступной базы данных контактов (включая бумажные и другие резервные копии) и устройств для передачи информации отдельным лицам в безопасном режиме, при необходимости;

c) принятие мер предосторожности, соизмеримых с оцененными рисками, чтобы электронные сообщения (передаваемые посредством Интернета или другой сети передачи данных) не могли быть перехвачены и оставались доступными, когда система, служба и/или сеть подвергаются атаке (для этого могут потребоваться заранее запланированные и задействованные альтернативные механизмы связи);

d) обеспечение сбора всех данных об информационной системе, службе и/или сети и всех данных, которые хранятся и обрабатываются, соответственно;

e) использование криптографического контроля целостности, соизмеримого с оцененными рисками, для определения изменений элементов системы, службы и/или сети, а также данных;

f) упрощение архивирования и защиты собранной информации (например, путем применения цифровых подписей к журналам и другим доказательствам до автономного хранения в носителях, доступных только для чтения, таких как CD, DVD или Blu-ray);

g) обеспечение подготовки распечаток (например, журналов регистрации), включая те, что показывают ход инцидента, а также процесс его разрешения и обеспечение сохранности;

h) восстановление информационной системы, службы и/или сети до нормальной работы со следующими процедурами, которые соответствуют соответствующему антикризисному управлению:

1) тестирование резервных копий;

2) управление вредоносным кодом;

3) использование исходных носителей с системным и прикладным программным обеспечением;

4) использование загрузочных носителей;

5) применение чистых, надежных и современных обновлений (патчей) системного и прикладного программного обеспечения.

Организации могут создавать стандартный базовый образ с установочного носителя и использовать его в качестве чистой основы для создания систем. Использование такого образа вместо исходного носителя часто предпочтительнее, потому что образ зачастую бывает уже обновленным (пропатченным), защищенным, протестированным и т.д.

Атакованная информационная система, служба или сеть могут работать неправильно. Таким образом, учитывая определенные риски, никакие технические средства (программное обеспечение и аппаратные средства), необходимые для реагирования на инцидент ИБ, не должны, по возможности, опираться в своем функционировании на основные системы, службы и/или сети организации. Все технические средства должны тщательно отбираться, правильно использоваться и регулярно тестироваться (включая тестирование имеющихся резервных копий). Если это возможно, технические средства должны быть полностью независимыми.

Примечание - Технические средства, описанные в 9.1, не включают технические средства, используемые для непосредственного обнаружения инцидентов и вторжений ИБ и автоматического уведомления соответствующих лиц. Такие технические средства описаны в O‘z DSt ISO/IEC 27039.

9.2 Примеры технической поддержки

Механизмы технической поддержки могут включать следующее:

a) внутренние механизмы аудита ИБ для оценки уровня безопасности и отслеживания уязвимых систем;

b) управление уязвимостями (включая обновления безопасности и исправление уязвимых систем);

c) технологию наблюдения для выявления новых видов угроз и атак;

d) СОиПВ (более подробно см. O‘z DSt ISO/IEC 27039);

e) устройства сетевой безопасности, средства защиты и средства мониторинга (более подробная информация приведена в O‘z DSt ISO/IEC 27033-1, O‘z DSt ISO/IEC 27033-2, O‘z DSt ISO/IEC 27033-3, O‘z DSt ISO/IEC 27033-4, O‘z DSt ISO/IEC 27033-5, O‘z DSt ISO/IEC 27033-6;

f) программное обеспечение для защиты от вредоносного кода;

g) записи журнала аудита и программное обеспечение для мониторинга журналов.

9.3 Примеры другой поддержки

Механизмы для оказания других видов поддержки могут включать документированные обязанности и рабочие процедуры для службы технической поддержки.

10 Повышение осведомленности, обучение и тренинги по инцидентам информационной безопасности

В разделе 10 подробно описано содержание O‘z DSt 3386 (ISO/IEC 27035-1:2016, MOD) (5.2, перечисление g)).

Управление инцидентами ИБ - это процесс, который включает не только технические средства, но и людей. Поэтому он должен поддерживаться лицами, надлежащим образом обученными и осведомленными касательно ИБ (также отмечается в O‘z DSt ISO/IEC 27001 (7.2)).

Осведомленность и участие всего персонала организации имеет решающее значение для успеха структурированного подхода к управлению инцидентами ИБ. Пользователи должны быть осведомлены о том, как они и их отдел могут извлечь выгоду из участия в структурированном подходе к управлению инцидентами ИБ. Кроме того, операционная эффективность и качество структурированного подхода к управлению инцидентами ИБ основываются на ряде факторов, включая обязательство уведомлять об инцидентах заинтересованные стороны, качество уведомления, простоту использования, скорость и обучение. Некоторые из этих факторов связаны с тем, что пользователи знают о ценности управления инцидентами ИБ и мотивированы сообщать об инцидентах.

Организация должна обеспечить активное поощрение роли управления инцидентами ИБ в рамках корпоративной программы повышения осведомленности и тренингов ИБ. Программа повышения осведомленности и соответствующие материалы должны быть доступны для всего персонала, включая новых сотрудников, сторонних пользователей и подрядчиков, в зависимости от ситуации. При необходимости, должна быть предусмотрена специальная учебная программа для координаторов, членов ГРИИБ, ИБ-персонала и особых администраторов. Каждая группа людей, непосредственно связанных с управлением инцидентами, может потребовать различного уровня подготовки, в зависимости от типа, частоты и критичности их взаимодействия с планом управления инцидентами ИБ.

Оперативные совещания организации по повышению осведомленности должны освещать следующее:

a) преимущества, получаемые от структурированного подхода к управлению инцидентами ИБ как для организации, так и для ее персонала;

b) принципы работы плана управления инцидентами ИБ, включая его область действия и рабочий процесс управления событием, инцидентом и уязвимостью ИБ;

c) процедуры отчетности о событиях, инцидентах и уязвимостях ИБ;

d) информацию об инцидентах из базы данных ИБ и ее исходных данных;

e) средства обеспечения конфиденциальности источников (при необходимости);

f) планирование соглашений об уровне обслуживания;

g) уведомление о результатах деятельности: при каких обстоятельствах информируются источники;

h) любые ограничения, налагаемые соглашениями о неразглашении;

i) представитель высшего руководства, на которого возлагается организация плана по управлению инцидентами ИБ и его линия отчетности;

j) получателей отчетов из плана управления инцидентами ИБ и способы распространения отчетов.

В некоторых случаях может быть желательно, чтобы организация специально включала информацию о повышении осведомленности при управлении инцидентами ИБ в другие учебные программы (например, программы ориентации персонала или общие корпоративные программы повышения осведомленности ИБ). Такой подход может обеспечить ценную практику применительно к конкретным группам людей, и повысить эффективность программ тренингов.

Прежде чем план управления инцидентами ИБ начнет действовать, организация должна обеспечить, чтобы весь соответствующий персонал был ознакомлен с процедурами, связанными с выявлением и отчетностью о событиях ИБ, а отобранный персонал очень хорошо осведомлен о последующих действиях. За этим должны последовать соответствующее оперативное совещание по повышению осведомленности и тренинги. Тренинги должны содержать конкретные задания и тестирование для координаторов, членов ГРИИБ, ИБ-персонала и особых администраторов.

Кроме того, программы повышения осведомленности и тренинги должны дополняться созданием и эксплуатацией «горячей линии» со стороны персонала по управлению инцидентами ИБ, с тем чтобы свести к минимуму задержки при представлении отчетности и обработке событий, инцидентов и уязвимостей ИБ.

11 Тестирование плана управления инцидентами информационной безопасности

11.1 Общие положения

В разделе 11 подробно описано содержание O‘z DSt 3386 (ISO/IEC 27035-1:2016, MOD) (5.2, перечисление h)).

Организация должна планировать регулярную проверку и тестирование процессов и процедур управления инцидентами ИБ для выявления потенциальных недостатков и проблем, которые могут возникнуть во время

управления событиями, инцидентами и уязвимостями ИБ. Следует организовать периодическое тестирование для проверки процессов/процедур и реагирования ГРИИБ. Эти моделируемые сценарии могут варьироваться от серьезных и сложных инцидентов, основанных на реалистичных атаках, сбоях или ошибках до испытаний по моделированию ситуаций за круглым столом. Формат моделирования будет зависеть от заранее определенных целей испытаний. В тестировании могут принять участие не только ГРИИБ, но также все или некоторые внутренние и внешние организации, которые задействованы в управлении инцидентами ИБ. Организация должна обеспечить, чтобы любые изменения, сделанные по итогам тестирования, подлежали тщательной проверке, включая дальнейшие испытания, до того, как измененный план начнет функционировать.

При проведении испытания очень важно, чтобы все участники знали, что они имеют дело с учебной атакой. Важно установить и сохранять эту разницу, чтобы персонал организации не мог инициировать действия, которые могут иметь гораздо большие последствия для организации (например, начать эвакуацию здания). Это правило можно игнорировать только при особых обстоятельствах, когда испытание выполняется в строго контролируемой среде, что предотвращает выход испытания за пределы операционной среды.

Основными видами испытаний являются:

- на основе обсуждения;
- моделирование ситуаций за круглым столом;
- в реальной обстановке;
- комбинация вышеуказанных видов.

Выбор вида испытания будет зависеть от цели, которую необходимо достичь, а также доступного времени и ресурсов.

Каждое испытание проходит через следующие этапы:

- планирование и подготовка;
- выполнение;
- заслушивание отчета и анализ после выполнения.

Планирование и подготовка испытаний основаны на текущих планах реагирования на инциденты и предполагаемых будущих угрозах и тенденциях. Результаты анализа после выполнения испытаний используются в качестве вклада в совершенствование планов реагирования на инциденты.

11.2 Испытание

11.2.1 Определение целей испытания

В целом, испытание может иметь следующие три основные цели:

а) валидация: проверка планов реагирования на инциденты и выявление потенциальных упущений;

b) обучение: выполнение персоналом своих ролей и приобретение навыков по их выполнению;

c) тестирование: проверка существующих процессов и процедур.

Каждое испытание, как правило, имеет более чем одну цель. Цель испытания в значительной степени определяется общим состоянием готовности организации. Когда организация готовит новые планы реагирования на инциденты или обновляет существующие, она может использовать испытания для их проверки. После разработки и введения планов в действие, организация будет использовать испытания для обучения персонала. После того, как существующие процессы и процедуры будут хорошо отработаны, их необходимо периодически проверять, чтобы убедиться, что они все еще актуальны.

Таблица 3 приводится в качестве руководства о том, какие виды испытаний могут быть использованы для достижения той или иной цели.

Таблица 3 - Сопоставление целей испытаний с видами испытаний

Цель	Виды испытаний
Проверка новых планов	- на основе обсуждения; - моделирование ситуаций за круглым столом
Обучение персонала	- на основе обсуждения; - моделирование ситуаций за круглым столом; - в реальной обстановке
Проверка актуальности текущих планов	- моделирование ситуаций за круглым столом; - в реальной обстановке

11.2.2 Определение области действия испытания

Область действия испытания в основном определяется его целями. При определении области действия испытания необходимо учитывать следующее:

a) испытание планируется только для внутреннего персонала (внутри организации) или в него будет вовлечена внешняя организация;

b) кто именно должен быть вовлечен в испытание, т. е. только ГРИИБ или участники других групп тоже должны быть включены и, если да, то какие группы;

c) как много испытаний потребуется руководителям ГРИИБ.

Область действия испытания оказывает непосредственное влияние на то, какие организации будут представлены при его осуществлении и профиль его участников.

11.2.3 Проведение испытания

При проведении испытания очень важно, чтобы все участники знали, что рассматриваемый сценарий - это симуляция, а не реальное событие. Если участники не смогут отличить симуляцию от реальных событий, существует вероятность того, что они вызовут действия с более широкими последствиями или привлекут людей, не входящих в программу испытания. В худшем случае это может вызвать панику среди широкой общественности.

Существует ряд задач, которые необходимо выполнить для успешного выполнения испытания. Общий обзор основных задач включает:

a) краткое изложение целей испытания его участникам;

b) обеспечение безопасности всех участников (это особенно важно при проведении интерактивных испытаний с использованием добровольцев);

c) подтверждение всеми участниками испытания понимания своих ролей;

d) обеспечение наличия достаточного количества персонала для руководства участниками во время испытаний;

e) выделение достаточного времени для обсуждений во время испытания, которые не приведут к срыву этого испытания;

f) предоставление достаточного времени и ресурсов для опроса всех участников после проведения испытания и сбора их отзывов (при этом, отзыв должен состоять из двух частей: что именно являлось целью испытания и как оно было проведено);

g) создание и распространение отчетов об испытании заинтересованным сторонам.

11.3 Мониторинг возможностей реагирования на инциденты

11.3.1 Внедрение программы мониторинга возможностей реагирования на инциденты

Возможности реагирования на инциденты охватывают не только возможности ГРИИБ, но и возможности отдельных лиц и групп, которых ГРИИБ может попросить о помощи во время обработки инцидентов. Несмотря на то, что большая часть возможностей реагирования на инциденты будет сосредоточена внутри ГРИИБ, возможно, что в некоторых узких областях группа может не обладать специальными знаниями. По этой причине ГРИИБ может привлекать отдельных лиц или другие команды для восполнения таких пробелов.

Путем мониторинга характеристик инцидентов и частоты выявления этих характеристик в инцидентах, можно составить представление о возможностях, которыми должны обладать ГРИИБ. Эти возможности будут меняться со временем. Некоторые изменения произойдут вследствие изменения

принятой технологии внутри организации либо путем отказа от нее, либо введения новой. Примером отказа от технологии может быть перемещение всех данных из баз данных SQL в базы данных, отличных от SQL. Разрешение сотрудникам использовать мобильные телефоны для выполнения своих задач - пример внедрения новой технологии, которая ранее не существовала в организации. Другой причиной, которая может потребовать изменений возможностей ГРИИБ, является разработка новых методов атак.

Не все возможности носят технический характер. Некоторые угрозы, особенно те, которые не основаны на технологии, лучше всего решать с помощью нетехнических средств (например, методы социальной инженерии).

11.3.2 Мониторинг показателей и управления возможностями реагирования на инциденты

Возможности ГРИИБ должны быть достаточно эффективными для устранения текущих угроз, с которыми сталкивается организация. По мере изменения угроз изменяются и возможности ГРИИБ, соответственно, организация может эффективно реагировать на новые угрозы. В то же время некоторые возможности могут больше не понадобиться, поскольку либо угрозы были окончательно сокращены до незначительных уровней, либо была устранена основная причина возникновения риска. От ГРИИБ не требуется обладания всеми возможностями обработки инцидентов, несмотря на то, что на нее возложены функции центра компетенции при обработке инцидентов. Редко используемые компетенции (знания) и возможности могут быть распределены между отдельными лицами или группами как внутри организации, так и вне ее. Основной причиной этого является экономическая эффективность.

При таком распределении возможностей и изменяющихся потребностей организация должна создать реестр, отражающий текущие возможности организации. В таком реестре может содержаться (но не исчерпываться) следующая информация:

a) возможности, доступные для организации;

b) персонал или лицо, обладающее этими возможностями;

c) отношение персонала или лица к организации (внутреннее или внешнее);

d) способ привлечения персонала или лица, обладающее возможностями;

e) актуальность возможностей (или их репрезентативных данных при последнем использовании);

f) частота использования возможностей в течение последнего временного интервала.

Далее эта информация используется при планировании развития возможностей ГРИИБ. Редко используемые возможности могут исчезнуть со

временем, а часто используемые, не присутствующие в настоящее время внутри ГРИИБ, накоплены с течением времени и так далее.

12 Извлеченный опыт

12.1 Общие положения

В разделе 12 подробно описано содержание O‘z DSt 3386 (ISO/IEC 27035-1:2016, MOD) (пункт 5.6).

После закрытия инцидента ИБ важно, чтобы организация быстро выявляла и получала опыт по обработке инцидента ИБ и следила за тем, чтобы были приняты соответствующие выводы. Кроме того, может быть извлечен опыт из оценки и разрешения переданных уязвимостей ИБ. Полученный опыт может привести к одному или нескольким из следующих результатов:

a) новые или измененные требования к средствам управления ИБ. Это могут быть технические или нетехнические (в том числе физические) средства управления. В зависимости от полученного опыта они могут включать в себя необходимость быстрого обновления материалов и проведения оперативных совещаний по повышению осведомленности ИБ (для пользователей, а также другого персонала) и быстрого пересмотра и опубликования руководящих принципов и/или стандартов безопасности;

b) новая или измененная информация об угрозах и уязвимостях и, таким образом, изменения текущих результатов определения и анализа управления рисками ИБ организации;

c) изменения в плане управления инцидентами ИБ и его процессах, процедурах, форматах отчетности и/или организационной структуре и базе данных ИБ.

12.2 Определение извлеченного опыта

Организация не должна ориентироваться только на один лишь инцидент или уязвимость ИБ и должна следить за тенденциями и шаблонами, которые сами по себе могут помочь определить необходимость изменений в средствах управления или подходе. Также, разумным подходом является отслеживание ИТ-ориентированного инцидента ИБ для проведения тестирования ИБ, в частности оценки уязвимости. Таким образом, организация должна регулярно анализировать данные в базе данных ИБ для:

- определения тенденций и шаблонов;
- выявления проблемных участков, вызывающих озабоченность;
- изучения для принятия превентивных мер по снижению вероятности будущих инцидентов.

Вся соответствующая информация, полученная в ходе инцидента ИБ, должна обобщаться и анализироваться для выявления тенденций и шаблонов (аналогично тому, как обрабатываются уязвимости ИБ). Это в значительной степени способствует раннему выявлению инцидентов ИБ и предупреждению о том, какие еще инциденты ИБ могут возникнуть, исходя из предыдущего опыта и документированных знаний.

Следует также использовать информацию об инциденте ИБ и связанной с ним уязвимости, полученной от вышестоящих инстанций, других ГРИИБ и поставщиков.

Оценка уязвимости и тестирование безопасности информационной системы, службы и/или сети после инцидента ИБ не должны ограничиваться только информационной системой, службой и/или сетью, затронутых инцидентом ИБ. Необходимо расширение этой деятельности путем включения любых связанных с ними информационных систем, служб и/или сетей. Полноценная оценка уязвимости используется, чтобы подчеркнуть наличие уязвимостей, которые были использованы во время инцидента ИБ в других информационных системах, службах и/или сетях, и обеспечить, чтобы новые уязвимости не были задействованы.

Важно подчеркнуть, что оценки уязвимостей должны проводиться на регулярной основе и что переоценка уязвимостей после инцидента ИБ должна быть частью этого процесса непрерывной оценки, а не заменой.

Сводный анализ инцидентов и уязвимостей ИБ должен быть подготовлен для вынесения на обсуждение на каждом общем собрании по управлению ИБ организации и/или другого общего собрания, определенного в общей политике ИБ организации.

12.3 Определение и внесение улучшений в процесс использования средства управления информационной безопасностью

По итогам разрешения одного или нескольких инцидентов или уязвимостей ИБ процедура проверки может выявить необходимость реализации новых или измененных средств управления. При этом рекомендации и связанные с ними требования к средству управления могут быть не выполнимыми безотлагательно ввиду финансовых или технических аспектов, и в этом случае они должны быть отражены в долгосрочных целях организации. Например, переход на более безопасный и надежный межсетевой экран не может быть финансово осуществимым в краткосрочной перспективе, но его необходимо учитывать в долгосрочных целях ИБ организации.

В соответствии с согласованными рекомендациями организации следует внедрить обновленные и/или новые средства управления. Это могут быть технические (в том числе физические) средства управления, и они могут

включать в себя необходимость быстрого обновления материалов и проведения оперативных совещаний по повышению осведомленности ИБ (для пользователей, а также другого персонала) и быстрого пересмотра и опубликования руководящих принципов и/или стандартов безопасности. Помимо этого, информационные системы, службы и/или сети организации должны подвергаться регулярным оценкам уязвимости для их своевременного выявления и обеспечения непрерывного усиления систем, служб и/или сетей.

Кроме того, несмотря на то, что проверки процедур и документации ИБ могут проводиться непосредственно после инцидента ИБ или разрешенной уязвимости, более вероятно, что данная мера потребуется в качестве более позднего реагирования. Обработав инцидент ИБ или разрешив уязвимость, организация, при необходимости, должна обновить свои политики и процедуры ИБ, чтобы учесть полученную информацию и любые проблемы, выявленные в ходе процесса управления инцидентами. Долгосрочной целью ГРИИБ совместно с отделом ИБ организации должно являться обеспечение распространения данных политик ИБ и обновленных процедур по всей организации.

На этапе освоения извлеченного опыта можно выявить другие улучшения, например, изменения в политике, стандартах и процедурах ИБ, а также изменения в конфигурациях оборудования и программного обеспечения ИТ. Организация должна обеспечить принятие соответствующих мер.

Особым случаем применения извлеченного опыта является анализ нестандартного применения плана управления инцидентами ИБ. Такая ситуация может возникнуть, если процессы отчетности используются для сообщений о таких событиях, как ИТ-проблемы (например, неисправность компьютера или приложения), нарушение дисциплины внутри организации (инсайдеры) или отдельных событиях, не связанных с ИБ. Слишком частое применение такого подхода может означать наличие проблем в других подразделениях организации или недостаточную подготовку при надлежащем назначении и использовании процессов отчетности. Потенциальным результатом такого анализа может быть выявление недостатков в других не связанных с безопасностью процессах или подразделениях организации, вплоть до высшего руководства.

12.4 Определение и совершенствование результатов анализа определения рисков ИБ и управления ими

В зависимости от серьезности и влияния инцидента ИБ (или серьезности и потенциального воздействия, связанного с уязвимостью ИБ) для оценки новых угроз и уязвимостей может потребоваться оценка результатов анализа определения рисков ИБ и управления ими. В рамках последующей деятельности по обновлению информации по анализу определения рисков ИБ и

управления ими может потребоваться введение измененных или новых средств управления (см. 11.3).

12.5 Определение и совершенствование плана управления инцидентами информационной безопасности

В рамках деятельности, проводимой после инцидента, руководитель ГРИИБ должен проанализировать все, что произошло для оценки и, таким образом, определить эффективность всего процесса реагирования на инцидент ИБ.

Такой анализ направлен на определение тех частей плана управления инцидентами ИБ, которые успешно работают и необходимости каких-либо улучшений.

Важным аспектом такого анализа является передача информации и знаний обратно в план управления инцидентами ИБ. Если инцидент достаточно серьезный, организация должна обеспечить проведение совещания всех причастных сторон вскоре после его разрешения. Факторы, которые следует учитывать на таком совещании, включают следующее:

a) работали ли процедуры, изложенные в плане управления инцидентами ИБ так, как предполагалось;

b) существуют ли какие-либо процедуры или методы, которые могли бы помочь в выявлении инцидента;

c) были ли определены какие-либо процедуры или методы, которые могли бы помочь в процессе реагирования;

d) были ли какие-либо процедуры, которые могли бы восстановить информационные системы после определения инцидента;

e) было ли эффективным взаимодействие по ходу инцидента со всеми соответствующими сторонами в процессе выявления, отчетности и реагирования.

Результаты совещания должны быть задокументированы. Организация должна обеспечить, чтобы области, определенные для совершенствования плана управления инцидентами ИБ, были рассмотрены и обосновывали изменения, включенные в обновление документации плана. Все изменения в процессах и процедурах управления инцидентами ИБ и формах отчетности должны подвергаться тщательной проверке и тестированию перед вводом в эксплуатацию.

12.6 Оценка ГРИИБ

По сравнению с извлеченным опытом оценка представляет собой периодическую и более целостную калькуляцию эффективности ГРИИБ.

Как только ГРИИБ начинает свою деятельность, группа и ее руководство должны оценивать эффективность группы и то, насколько она удовлетворяет потребности круга заинтересованных лиц. Оценка может проводиться периодически, либо аспекты оценки могут быть интегрированы в оперативные процессы и процессы извлеченного опыта.

Примеры мероприятий по оценке включают следующее:

- определение того, какие виды деятельности работают хорошо, а какие нет;
- пересмотр политики и разработку и реализацию планов, в зависимости от ситуации;
- оценку возможностей и услуг после их начала работы;
- проверку взаимодействия ГРИИБ с кругом заинтересованных лиц и любыми внешними партнерами и компаньонами.

Примеры более конкретных механизмов обратной связи включают следующее:

a) сопоставительный анализ (бенчмаркинг);

b) общие обсуждения или обмен мнениями с представителями круга заинтересованных лиц и внешними партнерами и компаньонами;

c) опросы, периодически распространяемые среди членов круга заинтересованных лиц;

d) создание набора критериев или параметров качества, которые затем используются аудитом или третьей стороной для оценки ГРИИБ.

Также могут быть собраны и обобщены показатели эффективности для оценки деятельности ГРИИБ. Возможные показатели могут включать (но не ограничиваться) следующее:

- статистические данные об инцидентах, такие как подсчет различных типов инцидентов, времени реагирования, времени жизни инцидента, разрешений или ликвидаций инцидентов;
- объем информации, сообщаемой кругу заинтересованных лиц о проблемах ИБ или текущей деятельности;
- превентивные методы и методы обеспечения безопасности на местах.

Любые изменения и улучшения должны основываться на результатах оценки.

12.7 Другие улучшения

Иногда результаты анализа инцидента могут приводить к результатам, которые не имеют непосредственного отношения к управлению инцидентами, но могут помочь в оптимизации работы организации или других улучшений. Следующий список приведен в качестве иллюстрации таких улучшений (и не является исчерпывающим или исключительным):

- чрезмерно длительное или редкое улучшение продукции может привести к уточнению критериев выбора поставщика программного обеспечения или оборудования;

- недостаточное укомплектование персоналом во время обработки инцидента может подсказать о необходимости улучшения планирования графика отсутствия на работе (отпусков);

- отсутствие знаний может указывать на пробелы в образовании.

Приложение А
(справочное)

Законодательные и нормативно-правовые аспекты

Следующие законодательные и нормативно-правовые аспекты управления инцидентами ИБ должны быть рассмотрены в политике управления инцидентами ИБ и связанном с ней планом:

a) обеспечение адекватной защиты данных и конфиденциальности личной информации. Часто обеспечение конфиденциальности и целостности данных ограничивается контролем персональных данных. Поскольку при расследовании инцидентов ИБ должна быть установлена личность нарушителя, информация персонального характера должна регистрироваться и управляться соответствующим образом, поэтому структурированный подход к управлению инцидентами ИБ должен учитывать надлежащую защиту конфиденциальности, которая может включать следующее:

1) те лица, которые имеют доступ к персональным данным, должны, по мере возможности, не знать лично лицо, находящееся под расследованием;

2) соглашения о неразглашении должны подписываться лицами, имеющими доступ к персональным данным, до того, как им будет разрешен доступ к ним;

3) информация должна использоваться только для той цели, для которой она была получена, то есть для расследования инцидентов ИБ;

b) ведение надлежащего учета (записей). В некоторых случаях может потребоваться, чтобы компании вели надлежащий учет своей деятельности для проверки в ходе ежегодного аудита организации. Аналогичные требования могут существовать в отношении государственных организаций. Возможно, организациям потребуется предоставлять или создавать архивы для правоохранительных органов (например, в отношении любого случая, который может быть связан с серьезным преступлением или проникновением в критические государственные информационные системы);

c) создание средств управления для обеспечения выполнения коммерческих договорных обязательств. В тех случаях, когда существуют обязательные требования к предоставлению службы управления инцидентами ИБ, например, учет требуемого времени реагирования, организация должна обеспечить соответствующую ИБ для выполнения таких обязательств при любых обстоятельствах. В связи с этим, если организация заключает договор с внешней стороной, например, внешней ГРИИБ, то необходимо обеспечить, чтобы все требования, включая время реагирования, были включены в этот договор;

d) рассмотрение правовых вопросов, связанных с политикой и процедурами. Политики и процедуры, связанные с планом управления инцидентами ИБ, должны быть проверены на предмет возможных законодательных и нормативно-правовых вопросов, например, имеются ли заявления о дисциплинарных и/или судебных исках против тех, кто вызывает инциденты ИБ. В некоторых странах прекращение трудовой деятельности в одностороннем порядке со стороны работодателя может вызвать проблемы;

e) проверка отказов от ответственности на предмет юридической силы. Все отказы от ответственности за действия, предпринятые ГРИИБ и любым внешним персоналом поддержки, должны быть проверены на предмет юридической силы;

f) охват договорами с внешним персоналом поддержки всех необходимых аспектов. Договоры с любым внешним персоналом поддержки, например, из внешней ГРИИБ, должны быть тщательно рассмотрены относительно отказа от ответственности, неразглашения, доступности услуг и последствий вследствие некорректной рекомендации;

g) исполнение соглашений о неразглашении подлежат исполнению. Члены ГРИИБ могут подписывать соглашения о неразглашении как при приеме на работу, так и расторжении трудового договора;

h) рассмотрение требований правоохранительных органов. Все вопросы, связанные с возможностью законного запроса правоохранительными органами информации из плана управления инцидентами ИБ, должны быть прояснены. Может понадобиться внести ясность на минимальном уровне, требуемом законом, на котором должны быть задокументированы инциденты и определен срок хранения этой документации;

i) прояснение аспектов ответственности. Необходимо уточнить вопросы потенциальной ответственности и соответствующих необходимых средств управления. Примеры событий, которые могут касаться вопросов ответственности, следующие:

1) если инцидент мог повлиять на другую организацию (например, имело место раскрытие общей информации, об этом не было сообщено вовремя, вследствие этого другая организация подвергается неблагоприятному воздействию);

2) если обнаружена новая уязвимость в продукте, а поставщик данного продукта не был уведомлен, вследствие этого позже происходит крупный инцидент с серьезным воздействием на одну или несколько других организаций;

3) если не создан отчет той организацией, которая обязана сообщать или создавать архивы для правоохранительных органов в отношении любого случая, который может быть связан с серьезным преступлением, или проникновением в конфиденциальные государственные информационные системы;

4) если раскрывается информация, которая, возможно, указывает на то, что какое-либо лицо или организация могут быть вовлечены в атаку. Это может нанести ущерб репутации и ведению бизнеса лица или организации;

5) если раскрывается информация о проблемах с конкретным элементом программного обеспечения, которая оказывается недействительной;

j) рассмотрение особых нормативных требований. В соответствии с особыми нормативными требованиями, в некоторых случаях инциденты должны сообщаться в специально назначенный орган, например, как это требуется в атомной энергетике, телекоммуникационных компаниях и провайдерах интернет-услуг во многих странах;

k) успешность следственных действий или внутренних дисциплинарных процедур. Должны быть предусмотрены соответствующие средства управления ИБ, в том числе доказуемо защищенные от несанкционированного доступа журналы аудита в целях обеспечения успешного следственного действия или проведения внутренних дисциплинарных процедур по отношению к злоумышленникам, независимо от того, являются ли проведенные ими атаки технического или физического характера. В подтверждение этого, доказательства должны быть собраны таким образом, чтобы они были приняты в соответствующих судах или при других дисциплинарных процедурах. Необходимо продемонстрировать, что:

1) записи являются полноценными и никоим образом не подделаны;

2) копии электронных доказательств доказуемо идентичны оригиналам;

3) любая ИТ-система, из которой были собраны доказательства, функционировала правильно на момент регистрации доказательств;

l) рассмотрение правовых аспектов, связанных с методами мониторинга. Последствия использования методов мониторинга необходимо рассматривать в контексте соответствующего законодательства. Законность различных методов будет варьироваться в зависимости от соответствующего законодательства. Например, может понадобиться необходимость в информировании людей о внедренном мониторинге их деятельности, в том числе с помощью методов наблюдения. Факторы, которые необходимо учитывать: кто/что находится под мониторингом, как они/оно отслеживаются и в какое время происходит мониторинг. Более подробная информация о мониторинге в контексте СОиПВ представлена в O‘z DSt ISO/IEC 27039;

m) определение и распространение политики допустимого использования. Действия, допустимые внутри организации должны быть определены, задокументированы и сообщены всем предполагаемым пользователям. Например, пользователи должны быть проинформированы о политике допустимого использования и должны предоставить письменное подтверждение того, что они понимают и принимают эту политику при вступлении в организацию или получении доступа к информационным системам.

Приложение В
(справочное)

Примеры подходов к категоризации и классификации событий и инцидентов информационной безопасности

В.1 Общие положения

Настоящее приложение содержит примеры подходов к категоризации и классификации инцидентов ИБ. Данные подходы позволяют персоналу и организациям документировать инциденты ИБ на постоянной основе, получая, таким образом, следующие преимущества:

1) повышение уровня обмена и распространения информации об инцидентах ИБ;

2) упрощение автоматизации процессов отчетности и реагирования на инциденты ИБ;

3) повышение эффективности и результативности обработки и управления инцидентами ИБ;

4) содействие в сборе и анализе данных об инцидентах ИБ;

5) установление уровней серьезности инцидентов ИБ с использованием последовательных критериев.

Эти примеры подходов к категоризации и классификации также могут быть применены к событиям ИБ, но они не охватывают уязвимости ИБ.

В.2 Категоризация инцидентов информационной безопасности

Инциденты ИБ могут быть вызваны преднамеренными или случайными действиями человека, а также техническими или физическими средствами. Следующий подход классифицирует инциденты ИБ, рассматривая угрозы как факторы категоризации (примеры типичных угроз приведены в O‘z DSt ISO/IEC 27005 (приложение В)). Список категорий инцидентов ИБ в соответствии с угрозами приведен в таблице В.1.

Таблица В.1 - Категории инцидентов информационной безопасности в соответствии с угрозами

Категория инцидента	Описание	Примеры
Стихийное бедствие	Нарушение ИБ вызвано стихийными бедствиями, неподвластными человеку	Землетрясение, извержение вулкана, наводнение, ураган, молния, цунами, обвал грунта и т.д.

Продолжение таблицы В.1

Категория инцидента	Описание	Примеры
Массовые волнения	Нарушение ИБ вызвано нестабильностью в обществе	Вторжение, террористическое нападение, война и т.д.
Материальный ущерб	Нарушение ИБ вызвано намеренными или случайными физическими действиями	Воздействие огня, воды, электростатического разряда, окружающей среды (загрязнение, пыль, коррозия, холод), выведение из строя, хищение, утеря, порча оборудования, носителей и т.д.
Сбой в работе инфраструктуры	Нарушение ИБ вызвано сбоями в работе базовых систем и сервисов, которые поддерживают функционирование информационных систем	Сбой питания, отказ сети, отказ системы кондиционирования, нарушение системы водоснабжения и т.д.
Воздействие излучения	Нарушение ИБ вызвано воздействием излучения	Электромагнитное излучение, электромагнитный импульс, радиопомехи, колебания напряжения, тепловое излучение и т.д.
Технические сбои	Нарушение ИБ вызвано сбоями в работе информационных систем или связанных с ними нетехнических средств, а также непреднамеренными техногенными проблемами, которые приводят к недоступности информационных систем или их уничтожению	Аппаратный сбой, сбой программного обеспечения, перегрузка (переполнение объемов информационных систем), нарушение правил эксплуатации и т.д.
Вредоносные программы	Нарушение ИБ вызвано вредоносными программами, которые создаются и распространяются намеренно. Вредоносная программа внедряется в информационные системы с целью нанесения ущерба конфиденциальности, целостности или доступности данных, приложений или операционных систем и/или влияет на нормальное функционирование информационных систем	Компьютерные вирусы, сетевые черви, троянские программы, бот-сети, атаки смешанного типа, вредоносный код, внедренный в веб-страницу или размещенный на веб-сайте и т.д. Компьютерный вирус - это набор машинных команд или кодов, который внедряется в компьютерные программы. В отличие от обычных программ, вирус может самовоспроизводиться, и, как правило, содержит информацию, которая может нарушить работу компьютера или уничтожить данные. В отличие от компьютерных вирусов,

Продолжение таблицы B.1

Категория инцидента	Описание	Примеры
		сетевые черви - это вид вредоносной программы, которая распространяется и воспроизводит себя через сеть автоматически, используя уязвимости информационных систем в сетях. Троянская программа - это разновидность вредоносной программы, замаскированная под какую-либо функцию информационных систем и позволяющая ее автору контролировать информационные системы, в том числе похищать либо перехватывать информацию из этих систем. Бот-сеть - это группа зараженных компьютеров в сети, централизованно контролируемых автором бот-сети, который известен как контроллер бот-сети. Бот-сети сознательно формируются путем массового заражения компьютеров в сетях с помощью бот-программ. Бот-сети могут использоваться для отражения возможных сетевых атак, хищения информации, а также распространения троянских программ, сетевых червей и других вредоносных программ. Атаки смешанного типа могут представлять собой комбинации компьютерных вирусов, сетевых червей, троянских программ или бот-сетей и так далее. Такие атаки могут также возникать в результате совместных операций ряда различных вредоносных программ. Например, компьютерный вирус или сетевой червь проникает в компьютерную систему, а затем устанавливает троянскую программу в системе. Вредоносный код, внедренный в веб-страницу, поражает веб-сайт и устанавливает вредоносное программное обеспечение на компьютер, с которого осуществляется доступ к этому веб-сайту. Вредоносный код, размещенный

Продолжение таблицы В.1

Категория инцидента	Описание	Примеры
		на веб-сайте, при посещении зараженных веб-сайтов загружается целевыми пользователями.
Технические атаки	Нарушение ИБ вызвано атаками на информационные системы через сети или с помощью других технических средств, либо путем использования уязвимостей информационных систем в конфигурациях, протоколах или программах, либо применением силовых методов, которые приводят в ненормальное состояние информационные системы или к нанесению вреда текущему состоянию системы	Сканирование сети, использование уязвимости, использование лазеек («черных входов»), попытки входа в систему, атаки типа «отказ в обслуживании» и т.д. Сканирование сети использует соответствующее программное обеспечение для получения информации о конфигурациях, портах, услугах и существующих уязвимостях сети. Использование уязвимостей заключается в использовании дефектов информационных систем (конфигурации, протоколы или программы). Использование лазеек заключается в использовании «черных ходов» или вредоносных программ, которые были преднамеренно оставлены при процессе разработки программного и аппаратного обеспечения. Попытки входа в систему осуществляются путем угадывания, взлома или грубого подбора паролей. Создание помех с помощью технических средств затрудняет работу компьютерных сетей, проводных или беспроводных сетей передачи радио- или телевизионных сигналов или спутниковых радио- и телесигналов. Атаки типа «отказ в обслуживании» вызываются чрезмерной загрузкой ресурсов информационной системы или сети, таких как процессор, оперативная память, дисковое пространство или пропускная способность сети и, таким образом, воздействуют на функционирование информационных систем. Примерами таких атак являются

Продолжение таблицы В.1

Категория инцидента	Описание	Примеры
		использование SYN-запросов, пинг-флуда, почтовых бомб.
Нарушение правил	Нарушение ИБ вызвано намеренным или случайным нарушением правил	Несанкционированное использование ресурсов, нарушение авторского права и т.д. Несанкционированное использование ресурсов приводит к получению доступа к ресурсам в несанкционированных целях, например, использование электронной почты для отправления нежелательных писем с целью получения прибыли или построения финансовых пирамид. Нарушение авторского права является результатом продажи или установки копий нелицензионного коммерческого программного обеспечения или других, защищенных авторским правом продуктов.
Компрометация функций	Нарушение ИБ вызвано намеренной или случайной компрометацией функций информационных систем с точки зрения безопасности	Злоупотребление правами, фальсификация прав, отказ от выполнения действий, неправильное выполнение операций, недоступность персонала и т.д. Злоупотребление правами предполагает использование прав вне сферы компетентности. Фальсификация прав предполагает создание ложных прав с целью обмана. Отказ от выполнения действий предполагает отрицание действий, совершенных тем или иным лицом. Неправильное выполнение операций предполагает неправильное или неумышленное проведение операций. Недоступность персонала является результатом нехватки или отсутствия человеческих ресурсов.
Компрометация информации	Нарушение ИБ вызвано намеренной или случайной компрометацией безопасности	Перехват, слежка, прослушивание, разглашение, маскарад, социальная инженерия, фишинг сети, хищение данных,

Продолжение таблицы В.1

Категория инцидента	Описание	Примеры
	информации (нарушением конфиденциальности, целостности, доступности и т.д.)	утеря данных, фальсификация данных, ошибка данных, анализ потока данных, определение положения и т.д. В ходе перехвата данные перехватываются до того, как они попадают к целевым получателям. Слежка предназначена для тайного сбора и передачи информации о деятельности другой организации. Прослушивание заключается в подслушивании переговоров сторонних организаций без их ведома. Разглашение информации приводит к опубликованию конфиденциальной информации для общественности. Маскарад - попытка какого-либо логического объекта выдать себя за другой логический объект для получения несанкционированного доступа. Социальная инженерия - психологическое манипулирование (нетехническим способом) человеком для получения от него информации, например, с помощью лжи, хитрости, подкупа или угроз. Фишинг сети - это использование фальсифицированных компьютерных сетевых технологий с целью побудить пользователей разглашать важную информацию, такую как получение реквизитов банковского счета пользователей и паролей обманным путем через электронную почту. Хищение данных заключается в их краже. Фальсификация данных - это возможность доступа и внесения изменений в данные без авторизации. Ошибка данных - ошибочное введение или обработка данных. Определение позиции - обнаружение расположения конфиденциальной информации или систем.

Окончание таблицы В.1

Категория инцидента	Описание	Примеры
Вредительский контент	Нарушение ИБ вызвано распространением нежелательного контента через информационные сети, что ставит под угрозу национальную безопасность, социальную стабильность и/или общественную безопасность	Нелегальный контент, тревожный контент, вредоносный контент, нежелательный контент и т.д. Нелегальный контент - это опубликованный контент, распространение которого запрещено конституцией, законодательными и нормативно-правовыми актами, например, детская порнография, пропаганда насилия, контрафактная продукция, мошенничество. Тревожный контент - злонамеренное вызывание нездорового интереса к щекотливым вопросам в Интернете, приводящие к общественному беспокойству или панике. Вредоносный контент - контент, распространение которого приводит к умышленной травле общества или лица, например, мистификации, домогательства. Нежелательный контент предполагает распространение контента, не желаемого получателями, например, спам.
Другие категории	Не входящие в любую из представленных выше категорий инцидентов	

В.3 Классификация инцидентов информационной безопасности

Ниже приводятся два примера подходов к классификации инцидентов ИБ.

Следует отметить, что это только примеры, и они могут быть изменены в соответствии с потребностями бизнеса. Существуют и другие, такие как Общая система оценки уязвимостей (Common Vulnerability Scoring Sistem) Форума групп реагирования на происшествия и обеспечения безопасности (Forum of incident Response and Security Teams).

B.3.1 Примерный подход 1

B.3.1.1 Классификационные факторы

B.3.1.1.1 Общие положения

Этот подход классифицирует инциденты ИБ, рассматривая следующие три фактора:

a) важность информационной системы;

b) снижение бизнес-деятельности;

c) социальное воздействие.

B.3.1.1.2 Важность информационной системы

Важность информационных систем, затронутых инцидентами ИБ, определяется с учетом важности бизнес-деятельности организации, поддерживаемой этими информационными системами. Важность может быть выражена в отношении национальной безопасности, социального порядка, экономического развития и общественных интересов, а также зависимости бизнеса от информационных систем. Этот подход классифицирует информационную систему на три обширных уровня: особенно важную информационную систему, важную информационную систему и обычную информационную систему.

B.3.1.1.3 Снижение бизнес-деятельности

Снижение бизнес-деятельности организации, вызванное инцидентами ИБ, определяется исходя из серьезности воздействия прерывания бизнес-деятельности из-за повреждения аппаратных средств и/или программного обеспечения, функций и данных информационных систем. Тяжесть воздействия может зависеть от стоимости восстановления бизнес-деятельности до нормальных показателей и других негативных последствий инцидентов ИБ, включая потерю прибыли и/или потенциальных сделок. Этот подход классифицирует снижение бизнес-деятельности на четыре обширных уровня: особо серьезное снижение бизнес-деятельности, серьезное снижение бизнес-деятельности, значительное и незначительное снижение бизнес-деятельности:

a) особо серьезное снижение бизнес-деятельности означало бы существенную приостановку бизнес-деятельности вплоть до полного прекращения деловой активности, и/или очень серьезный ущерб конфиденциальности, целостности и доступности ключевых бизнес-данных. Это привело бы к огромным затратам на восстановление бизнес-деятельности до нормальных показателей и устранение негативных последствий. Организация может не перенести подобный уровень снижения бизнес-деятельности;

b) серьезное снижение бизнес-деятельности будет означать прерывание бизнес-операций на длительное время или локальный паралич бизнес-деятельности вплоть до серьезного влияния на деловую активность, и/или серьезный ущерб конфиденциальности, целостности и доступности ключевых бизнес-данных. Это привело бы к высокой стоимости на восстановление бизнес-деятельности до нормальных показателей и устранение негативных последствий. Организация может перенести такой уровень снижения бизнес-деятельности;

c) значительное снижение бизнес-деятельности будет означать прерывание бизнес-операций вплоть до значительного влияния на деловую активность, и/или значительный ущерб конфиденциальности, целостности и доступности важных бизнес-данных. Это привело бы к значительным затратам на восстановление бизнес-деятельности до нормальных показателей и устранения негативных последствий. Организация может полностью перенести этот уровень снижения бизнес-деятельности;

d) незначительное снижение бизнес-деятельности будет означать прерывание бизнес-операций на короткое время вплоть до несущественного влияния на деловую активность, и/или незначительное влияние на конфиденциальность, целостность и доступность важных бизнес-данных. Это привело бы к незначительным затратам на восстановление бизнес-деятельности до нормальных показателей и устранение негативных последствий.

B.3.1.1.4 Социальное воздействие

Воздействие на общество, вызванное инцидентами ИБ, определяется путем изучения масштабов и степени воздействия на национальную безопасность, социальный порядок, экономическое развитие и общественные интересы. Этот подход классифицирует социальное воздействие на четыре уровня: особенно важное социальное воздействие, важное социальное воздействие, значительное социальное воздействие и незначительное социальное воздействие:

a) особенно важное социальное воздействие будет означать неблагоприятные последствия, охватывающие большую часть одной или нескольких областей, значительную угрозу национальной безопасности, провоцирование общественных беспорядков, окажет крайне неблагоприятный эффект на экономическое развитие и/или нанесет серьезный ущерб общественным интересам;

b) важное социальное воздействие будет означать неблагоприятные последствия, охватывающие большую часть одного или нескольких городов, угрозу национальной безопасности, общественную панику, окажет значительный неблагоприятный эффект на экономическое развитие и/или нанесет ущерб общественным интересам;

c) значительное социальное воздействие будет означать неблагоприятные последствия, охватывающие меньшую часть одного или нескольких городов с ограниченной угрозой национальной безопасности, с небольшим нарушением общественного порядка, окажет несущественный неблагоприятный эффект на экономическое развитие и/или влияние на общественные интересы;

d) незначительное социальное воздействие будет означать неблагоприятные последствия на небольшой части одного города с минимальными шансами на угрозу национальной безопасности, социальному порядку, экономическому развитию и общественным интересам, но с ущербом для интересов отдельных лиц, корпораций и других организаций.

B.3.1.2 Классы

B.3.1.2.1 Общие положения

Основываясь на классификационных факторах, инциденты ИБ следует классифицировать по степени тяжести с использованием шкалы. Такая шкала может быть простой, с использованием категорий «значительный» и «незначительный», или более подробной, например:

1) чрезвычайный: серьезное воздействие;

2) критический: среднее воздействие;

3) предупреждающий: низкое воздействие;

4) информационный: без какого-либо воздействия, но анализ инцидента может быть использован для улучшения политик, процедур или средств управления ИБ.

Согласно классификационным факторам, этот подход классифицирует инциденты ИБ на четыре класса серьезности:

a) очень серьезный (класс IV);

b) серьезный (класс III);

c) менее серьезный (класс II);

d) небольшой (класс I).

Необходимо отметить, что классы серьезности являются примером. В некоторых подходах наиболее серьезный класс представлен как самый высокий уровень шкалы. В других подходах наиболее серьезный класс представляется как самый низкий уровень шкалы.

B.3.1.2.2 Очень серьезный (класс IV)

Очень серьезные инциденты - это те, которые:

- происходят в критических информационных системах;
- приводят к особо серьезному снижению бизнес-деятельности;
- приводят к особенно важным социальным последствиям.

B.3.1.2.3 Серьезный (класс III)

Серьезными инцидентами являются те, которые:

- происходят в критических или важных информационных системах;
- приводят к серьезному снижению бизнес-деятельности;
- приводят к важным социальным последствиям.

B.3.1.2.4 Менее серьезный (класс II)

Менее серьезные инциденты - это те, которые:

- происходят в важных или типичных информационных системах;
- приводят к значительному снижению бизнес-деятельности;
- приводят к значительным социальным последствиям.

B.3.1.2.5 Небольшой (класс I)

Небольшие инциденты - это те, которые:

- происходят в типичных информационных системах;
- приводят к незначительному снижению бизнес-деятельности или вовсе не затрагивают ее;
- приводят к незначительным социальным последствиям или не оказывают никакого влияния.

Как правило, по таким инцидентам никаких действий не требуется.

B.3.1.3 Категория инцидентов и класс серьезности

Категория инцидента ИБ и класс серьезности часто связаны между собой. Одна и та же категория инцидента ИБ может иметь различный класс серьезности, зависящий не только от вида бизнес-деятельности, но и от характера инцидента ИБ, с учетом:

- преднамеренности;
- целевой направленности;
- продолжительности;
- интенсивности.

Некоторые примеры категорий инцидентов ИБ, которые могут иметь разные классы серьезности в зависимости от их характера, приведены в таблице B.2.

Таблица В.2 - Примеры категорий инцидентов и степени тяжести

Класс / Категория	Небольшой	Менее серьезный	Серьезный	Очень серьезный
Технические атаки	Неудачные попытки входа в систему	Одна типичная атака (компрометация пользователя)	Несколько атак (компрометация пользователя) Одна серьезная (атака на приложение, компрометация привилегированного доступа)	Массовая атака (атака на приложение, компрометация привилегированного доступа)
Технические атаки		Создание помех работе системы (поверхностная атака)	Нарушение работы системы (воздействие на пропускную способность)	Недоступность системы (остановка сервисов)
Вредоносные программы	Одна известная программа (обнаружена и заблокирована антивирусной системой)	Одна неизвестная программа	Несколько случаев заражения Заражение сервера	Массовое заражение

В.3.2 Примерный подход 2

В.3.2.1 Общие положения

В данном подходе представлены примерные рекомендации для оценки неблагоприятных последствий инцидентов ИБ, где каждая рекомендация использует шкалу от 1 (низкая) до 10 (высокая) для классификации инцидентов ИБ. (На практике можно использовать другую градацию, например, от 1 до 5, и организация должна принять шкалу, наиболее подходящую для ее среды.)

Перед изучением рекомендаций необходимо отметить следующее пояснение:

- в некоторых из приведенных ниже рекомендаций содержатся примечания «Нет записи». Это объясняется тем, что рекомендации формулируются таким образом, что неблагоприятные последствия, приведенные для каждой градации инцидентов ИБ (от 1 до 10), в целом аналогичны для всех шести типов, представленных в В.3.2.2 - В.3.2.7. Однако на некоторых градациях (по шкале от 1 до 10) для определенных типов 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, при более высоких градациях считается, что неблагоприятные последствия для них не могут быть серьезнее тех, что указаны для самой высокой градации и, следовательно, для этих градаций действует примечание «Нет записи». Таким образом, было бы логически неправильно исключить указания с пометкой «Нет записи» и сузить градацию шкалы.

Приведенный в В.3.2.2 - В.3.2.7 набор рекомендаций следует использовать при рассмотрении неблагоприятного воздействия инцидента ИБ на бизнес-деятельность организации вследствие:

- несанкционированного раскрытия информации;
- несанкционированной модификации информации;
- искажения смысла переданной информации;
- недоступности информации и/или услуги;
- уничтожения информации и/или услуги.

Первым делом следует определить, какой из нижеследующих типов подходит для определенного случая. Для определенных типов необходимо применять рекомендации по категоризации для определения реальных неблагоприятных воздействий на бизнес-процессы (или значимости) с целью занесения в форму отчета об инциденте ИБ.

В.3.2.2 Финансовые убытки/прерывание бизнес-деятельности

Последствия от несанкционированного раскрытия и модификации, искажения смысла переданной информации, а также недоступности и уничтожения такой информации могут привести к финансовым потерям, например, из-за снижения цен на акции, мошенничества или нарушения договорным обязательств из-за запоздалых соответствующих действий или их отсутствия. Также, последствием, особенно из-за недоступности или уничтожения какой-либо информации может быть прерывание бизнес-деятельности. Исправление ситуации и/или восстановление после таких инцидентов потребуют времени и усилий. В некоторых случаях эти издержки будут значительными и должны обязательно учитываться. В целях использования общего подхода, время на восстановление должно рассчитываться на единицу рабочего времени персонала и пересчитываться в финансовые затраты. Эти затраты должны рассчитываться с учетом средней стоимости рабочего времени человека в месяц, в соответствии с градацией/уровнем, принятым в организации. Следует руководствоваться следующими рекомендациями:

- величина финансовых потерь/затрат равна или меньше x_1;
- величина финансовых потерь/затрат находится в диапазоне между x_1+1 и x_2;
- величина финансовых потерь/затрат находится в диапазоне между x_2+1 и x_3;

- величина финансовых потерь/затрат находится в диапазоне между x_3+1 и x_4;

- величина финансовых потерь/затрат находится в диапазоне между x_4+1 и x_5;

- величина финансовых потерь/затрат находится в диапазоне между x_5+1 и x_6;

- величина финансовых потерь/затрат находится в диапазоне между x_6+1 и x_7;

- величина финансовых потерь/затрат находится в диапазоне между x_7+1 и x_8;

- величина финансовых потерь/затрат больше x_8;

- организация выйдет из бизнеса;

где *xi* (i=1, 2, ..., 8) представляют собой восемь градаций/уровней финансовых потерь/затрат, которые определяются организацией.

B.3.2.3 Коммерческие и экономические интересы

Коммерческая и экономическая информация должна быть защищена, и ее оценивают, рассматривая ее значимость для конкурентов или последствия вследствие ее компрометации для коммерческих интересов. Следует использовать следующие рекомендации, если такая информация:

- представляет интерес для конкурента, но не имеет коммерческой ценности;

- представляет интерес для конкурента при значении, равному y_1 или меньше (товарооборот);

- представляет значимость для конкурента при значении, которое находится в диапазоне между y_1+1 и y_2 (товарооборот) или вызывает финансовые потери, потерю потенциального дохода, способствует необоснованной выгоде или получению преимущества физическими лицами или организациями или нарушению обязательств для сохранения конфиденциальности информации, предоставленной третьими сторонами;

- представляет значимость для конкурента при значении, которое находится в диапазоне между y_2+1 и y_3 (товарооборот);

- представляет значимость для конкурента при значении, которое находится в диапазоне между y_3+1 и y_4 (товарооборот);

- представляет значимость для конкурента при значении, превышающем y_4+1 (товарооборот);

- нет записи (здесь и далее для всех подобных примечаний - для этого уровня последствий нет соответствующей записи);

- нет записи;

- может существенно повлиять на коммерческие интересы или подорвать финансовую устойчивость организации;

- нет записи,

где *yi* (i=1, 2, ..., 4) представляют собой четыре градации/уровня значимости для конкурента с точки зрения товарооборота, которые определяются организацией.

B.3.2.4 Персональные данные

В тех случаях, когда информация о физических лицах хранится и обрабатывается, естественно и этически правильно, а иногда в соответствии с законодательством необходимо, чтобы такая информация была защищена от несанкционированного раскрытия, которое может привести в лучшем случае, к причинению дискомфорта у физического или юридического лица, а в худшем - к следственным действиям в отношении лица, раскрывшего информацию, в соответствии с требованием законодательства в части защиты персональных данных. В равной степени необходимо, чтобы информация, содержащая персональные данные, была верной, поскольку ее несанкционированная модификация, приводящая к появлению неверных данных, может иметь такое же последствие, что и несанкционированное разглашение. Также важно, чтобы информацию, содержащую персональные данные, нельзя было сделать недоступной или уничтожить, поскольку это может привести к принятию неправильных решений или бездействию при необходимости, и иметь такое же последствие, что и несанкционированное разглашение или модификация информации. Следует использовать следующие рекомендации:

- нанесение незначительного ущерба (причинение беспокойства) физическому лицу (гнев, расстройство, разочарование) без нарушения законодательных или нормативных требований;

- нанесение ущерба (причинение беспокойства) физическому лицу (гнев, расстройство, разочарование) без нарушения законодательных или нормативных требований;

- нарушение законодательных, нормативных или этических требований или обнародованного намерения по защите информации, приводящее к причинению дискомфорта физическому лицу;

- нарушение законодательных, нормативных или этических требований или обнародованного намерения по защите информации, приводящее к причинению значительного дискомфорта отдельному лицу или незначительного - группе лиц;

- нарушение законодательных, нормативных или этических требований или обнародованного намерения по защите информации, приводящее к причинению серьезного дискомфорта физическому лицу;

- нарушение законодательных, нормативных или этических требований или обнародованного намерения по защите информации, приводящее к причинению серьезного дискомфорта группе лиц;

- нет записи;
- нет записи;
- нет записи;
- нет записи.

B.3.2.5 Нормативно-правовые обязательства

Данные, хранимые и обрабатываемые организацией, могут храниться и обрабатываться с целью обеспечения соблюдения организацией нормативно-правовых обязательств. Несоблюдение таких обязательств, намеренное или непреднамеренное, может привести к применению уголовных или административных мер в отношении причастных лиц в организации. Эти меры могут привести к штрафам и/или тюремным заключениям. Следует использовать следующие рекомендации:

- нет записи;
- нет записи;
- уведомление о принудительном исполнении, гражданский иск или уголовное преступление, приводящие к финансовому ущербу/штрафу, равному z_1 или менее;
- уведомление о принудительном исполнении, гражданский иск или уголовное преступление, приводящие к финансовому ущербу/штрафу в диапазоне между z_1+1 и z_2;
- уведомление о принудительном исполнении, гражданский иск или уголовное преступление, приводящие к финансовому ущербу/штрафу в диапазоне между z_2+1 и z_3 или тюремному сроку до двух лет;
- уведомление о принудительном исполнении, гражданский иск или уголовное преступление, приводящие к финансовому ущербу/штрафу в диапазоне между z_3+1 и z_4 или тюремному сроку от двух до десяти лет;
- уведомление о принудительном исполнении, гражданский иск или уголовное преступление, приводящие к неограниченному чем-либо финансовому ущербу/штрафу или тюремному сроку более десяти лет;
- нет записи;
- нет записи;
- нет записи.

B.3.2.6 Руководство и бизнес-деятельность

Информация может носить такой характер, что ее компрометация способна нанести ущерб эффективной деятельности организации. Например, информация, связанная с изменением политики, может вызвать различную реакцию общественности в случае раскрытия, вплоть до невозможности реализации данной политики. Несанкционированная модификация информации, искажение смысла переданной информации, недоступность информации,

касающейся финансовых аспектов или программного обеспечения, также могут иметь серьезные последствия для деятельности организации. Неблагоприятные последствия для бизнес-деятельности может иметь также отказ от ранее данных обязательств. Следует использовать следующие рекомендации:

- неэффективная работа какого-либо подразделения организации;
- нет записи;
- срыв надлежащего управления организацией и ее деятельностью;
- нет записи;
- препятствование эффективному развитию или использованию политик организации;
- отсутствие преимущества организации при переговорах с другими организациями касательно политик или коммерческих вопросов;
- создание серьезных препятствий для разработки или использования основных организационных политик, а также прекращение или существенное прерывание важной бизнес-деятельности;
- нет записи;
- нет записи;
- нет записи.

B.3.2.7 Утрата репутации организации

Несанкционированное раскрытие или модификация, искажение смысла переданной информации или отсутствие информации может привести к утере репутации организации, что приведет к нанесению ущерба, утрате доверия и другим неблагоприятным последствиям. Следует использовать следующие рекомендации:

- нет записи;
- создание атмосферы дискомфорта внутри организации;
- негативное влияние на отношения с акционерами, заказчиками, поставщиками, сторонними пользователями, регулирующими органами, правительством, другими организациями или общественностью, приводящее к незначительному отрицательному имиджу в местном/региональном масштабе;
- нет записи;
- негативное влияние на отношения с акционерами, заказчиками, поставщиками, сторонними пользователями, регулирующими органами, правительством, другими организациями или общественностью, приводящее к существенному отрицательному имиджу в национальном масштабе;
- нет записи;
- существенное негативное влияние на отношения с акционерами, заказчиками, поставщиками, сторонними пользователями, регулирующими органами, правительством, другими организациями или общественностью, приводящее к повсеместному отрицательному имиджу;

- нет записи;
- нет записи;
- нет записи.

Приложение С
(справочное)

Примеры отчетов о событиях, инцидентах и уязвимостях информационной безопасности и образец формы отчета

С.1 Общие положения

Данное приложение содержит примеры регистрационных форм событий, инцидентов и уязвимостей ИБ, а также примеры форм отчетов о событиях, инцидентах и уязвимостях ИБ с соответствующими примечаниями. Необходимо отметить, что это только примеры. Существуют и другие примеры, такие как схема из стандарта IODEF (Incident Object Decription Exchange Format, формат обмена объектными описаниями инцидентов).

С.2 Примеры регистрационных форм

С.2.1 Пример регистрационной формы для события информационной безопасности

Форма включает в себя базовую информацию о событии ИБ, такую как когда, какое, каким образом и почему произошло событие, а также контактные данные лица, представляющего отчет.

Основная информация:
- дата события;
- номер события;
- соответствующие номера событий и/или инцидентов (если применимо).

Сведения о сообщающем лице:
- имя;
- контактная информация, такая как адрес, наименование организации, подразделение, телефон и электронная почта.

Описание события:
- что произошло;
- каким образом произошло;
- почему произошло;
- первоначальное представление по затронутым компонентам/активам;
- неблагоприятные последствия для бизнес-деятельности;
- любые идентифицированные уязвимости.

Сведения о событии:
- дата и время события;
- дата и время обнаружения события;
- дата и время отчета о событии.

С.2.2 Пример регистрационной формы для инцидента информационной безопасности

Форма включает в себя базовую информацию об инциденте ИБ, такую как когда, какой, каким образом и почему произошел инцидент, а также категорию инцидента, его воздействие и результат реагирования на инцидент.

Основная информация:
- дата инцидента;
- номер инцидента;
- соответствующие номера событий и/или инцидентов (если применимо).

Сведения о сообщающем лице:
- имя;
- контактная информация, такая как адрес, наименование организации, подразделение, телефон и электронная почта.

Сведения о координаторе:
- имя;
- контактная информация, такая как адрес, наименование организации, подразделение, телефон и электронная почта.

Сведения о члене ГРИИБ:
- имя;
- контактная информация, такая как адрес, наименование организации, подразделение, телефон и электронная почта.

Описание инцидента:
- что произошло;
- каким образом произошло;
- почему произошло;
- первоначальное представление по затронутым компонентам/активам;
- неблагоприятные последствия для бизнес-деятельности;
- любые идентифицированные уязвимости.

Сведения об инциденте:
- дата и время инцидента;
- дата и время обнаружения инцидента;
- дата и время отчета об инциденте.

Категория инцидента:
- затронутые компоненты/активы;
- неблагоприятные последствия инцидента для бизнес-деятельности;
- общая стоимость восстановления после инцидента;
- разрешение инцидента;
- вовлеченное лицо/исполнитель (если инцидент вызван человеком);
- описание исполнителя;
- фактическая или предполагаемая мотивация;
- действия, предпринятые для разрешения инцидента;
- действия, запланированные для разрешения инцидента:
- прочие действия;
- заключение;
- внутренние физические и юридические лица, которые были извещены;
- внешние физические и юридические лица, которые были извещены.

С.2.3 Пример регистрационной формы для уязвимости информационной безопасности

Форма включает в себя базовую информацию об уязвимости ИБ, такую как когда, какая и каким образом была выявлена уязвимость, а также о ее потенциальном воздействии и разрешении.

Основная информация:
- дата выявления уязвимости;
- номер уязвимости.

Сведения о сообщающем лице:
- имя;
- контактная информация, такая как адрес, наименование организации, подразделение, телефон и электронная почта.

Описание уязвимости:
- разрешение уязвимости.

С.3 Использование форм

С.3.1 Формат времени и даты

Даты должны быть введены в формате «Число-Месяц-Год» (и, если потребуется, в формате «Час-Минуты-Секунды»). Если события происходят в разных часовых поясах, следует использовать указатель зоны по Всемирному координированному времени (указать смещение относительно Всемирного координированного времени).

С.3.2 Рекомендации по заполнению

Предназначение форм отчетов о событиях и инцидентах ИБ заключается в обеспечении соответствующих лиц информацией о событии ИБ, а затем, если оно определено как инцидент ИБ, то и об инциденте ИБ.

В том случае, если имеются подозрения на то, что событие ИБ развивается или уже свершилось, особенно то, которое может нанести существенный ущерб собственности или репутации организации, то необходимо немедленно заполнить и передать форму отчета о событии ИБ в соответствии с процедурами, описанными в плане управления инцидентами ИБ организации.

Предоставленная информация будет использована для инициирования соответствующего процесса оценки, который определит, должно ли это событие классифицироваться как инцидент ИБ и, в случае положительного решения, какие корректирующие меры, необходимые для предотвращения или ограничения ущерба следует предпринять. Учитывая, что данный процесс может требовать незамедлительных действий, в настоящее время не обязательно заполнять все поля формы отчета.

Координатору, анализирующему полностью или частично заполненные формы, необходимо будет принять решение о том, должно ли событие классифицироваться как инцидент ИБ и, если событие классифицируется как инцидент, внести в форму отчета об инциденте ИБ как можно больше информации и передать в ГРИИБ формы отчетов о событии и инциденте ИБ. Независимо от того, будет ли событие ИБ классифицировано как инцидент ИБ, система управления инцидентами должна быть обновлена.

Члену ГРИИБ, анализирующему формы отчетов о событиях и инцидентах ИБ, переданные координатором, необходимо обновлять форму отчета об инциденте по ходу расследования и, соответственно, должна обновляться система управления инцидентами.

Форма отчета об уязвимости ИБ предназначается для предоставления информации о предполагаемой уязвимости и выступает в качестве хранилища информации по разрешениям сообщенных уязвимостей.

При заполнении форм необходимо соблюдать следующие рекомендации:

- форму рекомендуется заполнять и предоставлять в электронном виде.

Примечание - Например, на безопасной веб-странице с привязкой к электронной базе данных событий/инцидентов/уязвимостей ИБ. В настоящее время, работа с планом в бумажном виде занимает много времени. Тем не менее, такие планы должны быть готовы для случая, когда электронные планы не могут быть использованы.

При наличии проблем или подозрении в их наличии в отношении механизмов электронной отчетности (например, электронная почта), включая случаи, когда система может подвергаться атаке и отчеты могут быть прочитаны неавторизованными пользователями, должны использоваться альтернативные средства отчетности. Альтернативными средствами могут быть использование курьерской доставки, телефонных или текстовых сообщений;

- необходимо предоставлять фактическую информацию, не следует заниматься домыслами при заполнении всех полей. Если возникает необходимость в предоставлении информации, которую невозможно подтвердить, следует указать, что это неподтвержденная информация, и причину убежденности в ее достоверности;

- необходимо предоставлять полную контактную информацию. Возможно, понадобится связаться с лицом, предоставившим отчет (незамедлительно или позже) для получения дополнительной информации, касающейся отчета.

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

С.4 Образец форм отчета

С.4.1 Пример формы для отчета о событии информационной безопасности

Отчет о событии информационной безопасности			**Стр. 1 из 1**
1. Дата события		**3. Соответствующие номера событий и/или инцидентов** *(если применимо)*	
2. Номер события *(Номера событий присваиваются руководителем ГРИИБ)*			
4. Сведения о сообщающем лице			
4.1 ФИО		**4.2 Адрес**	
4.3 Наименование организации		**4.4. Подразделение**	
4.5 Телефон		**4.6 Электронная почта**	
5. Описание события информационной безопасности			
5.1 Описание события □ Что произошло □ Каким образом произошло □ Почему произошло □ Первоначальное представление по затронутым компонентам/активам □ Негативные последствия для бизнес-деятельности □ Любые идентифицированные уязвимости			
6. Сведения о событии информационной безопасности			
6.1 Дата и время наступления события			
6.2 Дата и время обнаружения события			
6.3 Дата и время отчета о событии			
6.4 Завершился ли процесс реагирования на данное событие?		**ДА** □ **НЕТ** □ *(отметить нужное)*	
6.5 Если «ДА», то указать длительность события *(Дни/Часы/Минуты)*			

С.4.2 Пример формы для отчета об инциденте информационной безопасности

Отчет об инциденте информационной безопасности			**Стр. 1 из 6**
1. Дата инцидента		**3. Соответствующие номера событий и/или инцидентов** *(если применимо)*	
2. Номер инцидента *(Номера инцидентов присваиваются руководителем ГРИИБ и привязываются к соответствующим номерам событий ИБ)*			
4. Сведения о координаторе			
4.1 ФИО		**4.2 Адрес**	
4.3 Наименование организации		**4.4. Подразделение**	
4.5 Телефон		**4.6 Электронная почта**	
5. Сведения о члене ГРИИБ			
5.1 Имя		**5.2 Адрес**	
5.3 Наименование организации		**5.4. Подразделение**	
5.5 Телефон		**5.6 Электронная почта**	
6. Описание инцидента информационной безопасности			
6.1 Дополнительное описание инцидента □ Что произошло □ Каким образом произошло □ Почему произошло □ Первоначальное представление по затронутым компонентам/активам □ Негативные последствия для бизнес-деятельности □ Любые идентифицированные уязвимости			
7. Сведения об инциденте информационной безопасности			
7.1 Дата и время наступления инцидента			
7.2 Дата и время обнаружения инцидента			
7.3 Дата и время отчета об инциденте			
7.4 Завершен ли инцидент?		**ДА** □ **НЕТ** □ *(отметить нужное)*	
7.5 Если «ДА», то указать длительность инцидента *(Дни/Часы/Минуты)*			

Отчет об инциденте информационной безопасности	**Стр. 2 из 6**

8. Категория инцидента информационной безопасности

(Отметьте один, затем заполните соответствующий раздел ниже)
8.1 Фактический *(инцидент произошел)* □
8.2 Предполагаемый *(предположение возникновения инцидента без подтверждения)* □

(Выбрать один) **8.3 Стихийное бедствие** □ *(указать тип)*
Землетрясение □ **Извержение вулкана** □ **Наводнение** □ **Ураган** □
Молния □ **Цунами** □ **Обвал грунта** □ **Другое** □

Дополнительно:

(Выбрать один) **8.4 Массовые волнения** □ *(указать тип)*
Протест/Демонстрация □ **Террористическая атака** □ **Война** □ **Другое** □

Дополнительно:

(Выбрать один) **8.5 Материальный ущерб** □ *(указать тип)*
Воздействие огня □ **Воздействие воды** □
Воздействие электростатического разряда □
Воздействие окружающей среды (загрязнение, пыль, коррозия, холод) □
Выведение из строя оборудования □ **Выведение из строя носителей** □
Хищение оборудования □ **Хищение носителей** □
Утеря оборудования □ **Утеря носителей** □
Порча оборудования □ **Порча носителей** □
Другое □

Дополнительно:

(Выбрать один) **8.6 Сбой в работе инфраструктуры** □ *(указать тип)*
Сбой питания □ **Отказ сети** □ **Отказ системы кондиционирования** □
Нарушение системы водоснабжения □ **Другое** □

Дополнительно:

(Выбрать один) **8.7 Воздействие излучения** □ *(указать тип)*
Электромагнитное излучение □ **Электромагнитный импульс** □ **Радиопомехи** □
Колебания напряжения □ **Тепловое излучение** □ **Другое** □

Дополнительно:

(Выбрать один) **8.8 Технические неполадки** □ *(указать тип)*
Аппаратный сбой □ **Сбой программного обеспечения** □
Перегрузка (переполнение объемов информационных систем) □
Нарушение правил эксплуатации □ **Другое** □

Дополнительно:

Отчет об инциденте информационной безопасности	**Стр. 3 из 6**
8. Категория инцидента информационной безопасности	
(Выбрать один) **8.9 Вредоносные программы** □ *(указать тип)* **Сетевой червь** □ **Троянская программа** □ **Бот-сеть** □ **Атака смешанного типа** □ **Вредоносный код, внедренный в веб-страницу** □ **Вредоносный код, размещенный на веб-сайте** □ **Другое** □ *Дополнительно:*	
(Выбрать один) **8.10 Технические атаки** □ *(указать тип)* **Сканирование сети** □ **Попытки входа в систему** □ **Использование уязвимости** □ **Использование лазеек («черных входов»)** □ **Отказ в обслуживании** □ **Другое** □ *Дополнительно:*	
(Выбрать один) **8.11 Нарушение правил** □ *(указать тип)* **Несанкционированное использование ресурсов** □ **Нарушение авторского права** □ **Другое** □ *Дополнительно:*	
(Выбрать один) **8.12 Компрометация функций** □ *(указать тип)* **Злоупотребление правами** □ **Фальсификация прав** □ **Отказ от выполнения действий** □ **Неправильное выполнение операций** □ **Недоступность персонала** □ **Другое** □ *Дополнительно:*	
(Выбрать один) **8.13 Компрометация информации** □ *(указать тип)* **Перехват** □ **Слежка** □ **Прослушивание** □ **Разглашение** □ **Маскировка** □ **Социальная инженерия** □ **Фишинг сети** □ **Хищение данных** □ **Утеря данных** □ **Фальсификация данных** □ **Ошибка данных** □ **Анализ потока данных** □ **Определение позиции** □ **Другое** □ *Дополнительно:*	
(Выбрать один) **8.14 Вредительский контент** □ *(указать тип)* **Нелегальный контент** □ **Тревожный контент** □ **Вредоносный контент** □ **Нежелательный контент** □ **Другое** □ *Дополнительно:*	
8.15 Другое □ *(если принадлежность инцидента к какой-либо из вышеуказанных категорий не установлена, отметьте здесь)* *Дополнительно:*	

Отчет об инциденте информационной безопасности	**Стр. 4 из 6**
9. Затронутые компоненты/активы (*для получения более подробной информации о компонентах/активах, которые были затронуты, если они доступны в ходе исследований и анализа (на ранних этапах анализа событий и инцидентов будет собираться только информация «высокого уровня»)).*	
Затронутые компоненты/активы *(при наличии)*	*(Описание компонентов/активов, затронутых инцидентами (в том числе, связанными), с указанием серийных и лицензионных номеров и номеров версий)*
9.1 Информация/данные	
9.2 Аппаратные средства	
9.3 Программное обеспечение	
9.4 Средства связи	
9.5 Документация	
9.6 Процессы	
9.7 Другое	

10. Негативное воздействие/влияние инцидента на бизнес-деятельность			
Отметить, если необходимо, каждую из нижеуказанных позиций. В колонке «Значимость» указать степень негативного воздействия на бизнес, с охватом всех сторон, затронутых инцидентом, по шкале от 1 до 10, используя следующие категории: финансовые убытки/прерывание бизнес-деятельности, коммерческие и экономические интересы, персональные данные, нормативно-правовые обязательства, руководство и бизнес-деятельность, утрата репутации организации. Указать кодовые буквы для применимых рекомендаций в колонке «Руководство»; если известны фактические материальные издержки, указать их в колонке «Расходы».			
	Значимость	**Руководство**	**Расходы**
10.1 Нарушение конфиденциальности □ *(т.е. несанкционированное разглашение)*			
10.2 Нарушение целостности □ *(т.е. несанкционированное изменение)*			
10.3 Нарушение доступности □ *(т.е. недоступность)*			
10.4 Нарушение неотказуемости □			
10.5 Уничтожение □			

11. Общая стоимость восстановления после инцидента			
(Там, где возможно, необходимо указать общую стоимость восстановления после инцидента по шкале от 1 до 10 для колонки «Значимость» и в денежном эквиваленте для колонки «Расходы»).	**Значимость**	**Руководство**	**Расходы**

Отчет об инциденте информационной безопасности	**Стр. 5 из 6**
12. Разрешение инцидента	
12.1 Дата начала расследования инцидента	
12.2 ФИО лица, проводившего расследование	
12.3 Дата завершения инцидента	
12.4 Дата окончания воздействия инцидента	
12.5 Дата завершения расследования инцидента	
12.6 Ссылка и местонахождение отчета о расследовании	
13. Вовлеченное лицо/исполнитель *(если инцидент вызван человеком)*	
(Выбрать один) **Лицо □ Организация, созданная законным путем □** **Организованная группа □ Случайность □** **Без исполнителя □** *(например, природные факторы, отказ оборудования, человеческий фактор)*	
14. Описание исполнителя	
15. Фактическая или предполагаемая мотивация	
(Выбрать один) **Преступная/финансовая выгода □ Хакерство □** **Политический мотив/Терроризм □ Месть □ Другое □** *Дополнительно:*	
16. Действия, предпринятые для разрешения инцидента	
(например, «бездействие», «штатные средства», «внутреннее расследование», «внешнее расследование с привлечением ...»)	
17. Действия, запланированные для разрешения инцидента	
(например, «бездействие», «штатные средства», «внутреннее расследование», «внешнее расследование с привлечением ...»)	
18. Прочие действия	
(например, дополнительно требуется проведение расследования другим персоналом)	

Отчет об инциденте информационной безопасности	**Стр. 6 из 6**
19. Заключение	
(*отметьте соответствующий пункт; приложите краткое обоснование этого заключения)* **Значительный □ Незначительный □** *(указать любые другие выводы)*	
20. Уведомленные физические и юридические лица внутри организации	
(Этот пункт заполняется соответствующим лицом, на которое возложены обязанности по обеспечению ИБ, устанавливающим требуемые действия. Как правило, этим лицом является руководитель службы (отдела) ИБ организации или другое ответственное должностное лицо)	**Руководитель службы ИБ/другое ответственное должностное лицо □** **Руководитель ГРИИБ □** **Менеджер веб-сайта □** *(установить, какой веб-сайт)* **Руководитель информационных систем □** **Автор отчета □** **Руководитель автора отчета □** **Другое □** *(например, справочная служба, отдел кадров, руководство, служба внутреннего аудита)*
21. Уведомленные физические и юридические лица вне организации	
(Этот пункт заполняется соответствующим лицом, на которое возложены обязанности по обеспечению ИБ, устанавливающим требуемые действия. Как правило, этим лицом является руководитель службы (отдела) ИБ организации или другое ответственное должностное лицо)	**Органы внутренних дел □** **Другое □** *(например, вышестоящие инстанции, орган-регулятор, внешняя ГРИИБ)*

22. Подписи

Автор		**Аналитик/эксперт**		**Аналитик/эксперт**	
Цифровая подпись		**Цифровая подпись**		**Цифровая подпись**	
ФИО		**ФИО**		**ФИО**	
Должность		**Должность**		**Должность**	
Дата		**Дата**		**Дата**	

С.4.3 Пример формы для отчета об уязвимости информационной безопасности

Отчет об уязвимости информационной безопасности			**Стр. 1 из 1**
1. Дата выявления уязвимости		**2. Номер уязвимости** *(Номера уязвимостей присваиваются руководителем ГРИИБ)*	

3. Сведения о сообщающем лице			
3.1 ФИО		**3.2 Адрес**	
3.3 Наименование организации		**3.4. Подразделение**	
3.5 Телефон		**3.6 Электронная почта**	

4. Описание уязвимости информационной безопасности	
4.1 Дата и время отчета об уязвимости	
4.2 Описание выявленной уязвимости информационной безопасности в повествовательной форме: □ Каким образом была замечена уязвимость □ Характеристика уязвимости (физическая, техническая и т.д.) □ Если техническая, какие ИТ/сетевые компоненты/активы причастны □ Компоненты/активы, которые могут быть затронуты при использовании уязвимости □ Потенциальное неблагоприятное воздействие на бизнес-деятельность при использовании уязвимости	

5. Разрешение уязвимости информационной безопасности			
5.1 Подтверждена ли уязвимость?		**ДА** □ **НЕТ** □ *(отметить нужное)*	
5.2 Дата и время подтверждения уязвимости			
5.3 ФИО уполномоченного лица		**5.4 Адрес**	
5.5 Наименование организации			
5.6. Телефон		**5.7 Электронная почта**	
5.8 Устранена ли уязвимость?		**ДА** □ **НЕТ** □ *(отметить нужное)*	
5.9 Описание процесса устранения уязвимости ИБ с указанием даты и имени уполномоченного лица, возглавляющего процесс устранения, в повествовательной форме			

Приложение D
(справочное)

Сведения о соответствии ссылочных международных стандартов государственным стандартам Республики Узбекистан

Таблица D.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего государственного стандарта Республики Узбекистан
ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь	MOD	O‘z DSt ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь
ISO/IEC 27001:2013 Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования	MOD	O‘z DSt ISO/IEC 27001:2016 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования
ISO/IEC 27002:2013 Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации	MOD	O‘z DSt ISO/IEC 27002:2016 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью
ISO/IEC 27005:2011 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности	MOD	O‘z DSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности

Продолжение таблицы D.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего государственного стандарта Республики Узбекистан
ISO/IEC 27031:2011 Информационные технологии. Методы обеспечения защиты. Руководящие указания по готовности информационно-коммуникационных технологий для ведения бизнеса	MOD	O‘z DSt ISO/IEC 27031:2016 Информационная технология. Методы обеспечения безопасности. Руководящие указания по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса
ISO/IEC 27033-1:2015 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции	MOD	O‘z DSt ISO/IEC 27033-1:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции
ISO/IEC 27033-2:2012 Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети	MOD	O‘z DSt ISO/IEC 27033-2:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 2. Руководящие указания по проектированию и внедрению сетевой безопасности
ISO/IEC 27033-3:2010 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления	MOD	O‘z DSt ISO/IEC 27033-3:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

Продолжение таблицы D.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего государственного стандарта Республики Узбекистан
ISO/IEC 27033-4:2014 Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности	MOD	O‘z DSt ISO/IEC 27033-4:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности
ISO/IEC 27033-5:2013 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных систем	MOD	O‘z DSt ISO/IEC 27033-5:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных сетей
ISO/IEC 27033-6:2016 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 6. Защищенный доступ к беспроводной IP-сети	MOD	O‘z DSt ISO/IEC 27033-6:2018 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 6. Защищенный доступ к беспроводной IP-сети
ISO/IEC 27035-1:2016 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Часть 1. Принципы менеджмента инцидентов	MOD	O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы

Окончание таблицы D.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего государственного стандарта Республики Узбекистан
ISO/IEC 27039:2015 Информационные технологии. Методы защиты. Выбор, применение и операции систем обнаружения и предотвращения вторжений	MOD	O‘z DSt ISO/IEC 27039:2017 Информационная технология. Методы обеспечения безопасности. Выбор, применение и операции систем обнаружения и предотвращения вторжений
Примечание - MOD - модифицированная степень соответствия государственного стандарта Республики Узбекистан международному стандарту.		

Приложение E
(справочное)

Технические отклонения и объяснение причин их внесения

E.1 По всему тексту слова «этот международный стандарт» заменены на «настоящий стандарт».

E.2 Стандарт оформлен с учетом требований O‘z DSt 1.6:2003.

E.3 В стандарт включены отдельные изменения и дополнения. Перечень внесенных модификаций и объяснение причин их внесения приведены в таблице E.1.

Таблица E.1

Раздел, пункт настоящего стандарта	Модификация	Объяснение
Предисловие	Исключено	В связи с тем, что содержит информацию только о разработке международного стандарта
Раздел 2	Международные стандарты заменены на соответствующие им государственные стандарты	В настоящее время действуют государственные стандарты в соответствии с приложением D
	Дополнительно включены государственные стандарты O‘z DSt ISO/IEC 27001 O‘z DSt ISO/IEC 27002 O‘z DSt ISO/IEC 27005 O‘z DSt ISO/IEC 27031 O‘z DSt ISO/IEC 27033-1 O‘z DSt ISO/IEC 27033-2 O‘z DSt ISO/IEC 27033-3 O‘z DSt ISO/IEC 27033-4 O‘z DSt ISO/IEC 27033-5 O‘z DSt ISO/IEC 27033-6 O‘z DSt ISO/IEC 27039	Перенесены из раздела «Библиография» в соответствии с приложением D. Ссылки по тексту стандарта на данные международные стандарты заменены соответствующими ссылками на государственные стандарты
Раздел 3	Исключены следующие сокращения: CERT, IDS, IRT,	В связи с тем, что не используются по тексту настоящего

Окончание таблицы Е.1

Раздел, пункт настоящего стандарта	Модификация	Объяснение
	ISP, PoC	стандарта, а также заменены на соответствующие сокращения на русском языке
	Добавлены следующие сокращения: Blu-ray, HTTP, HTTPS, IP, SQL, ГРИИБ, ИБ, ИТ, СОиПВ, СУИБ	В связи с тем, что используются по тексту настоящего стандарта
Раздел 9.1	Исключены ссылки на стандарты ISO 22301 и ISO 22313	В связи с тем, что носят информационно-справочный характер
Приложение С	Исключены ссылки на стандарты RFC5070, RFC6545, RFC6546, STIX, TAXII	В связи с тем, что носят информационно-справочный характер
Приложение D	Дополнительно включены в текст стандарта	Приведены сведения о соответствии ссылочных международных стандартов государственным стандартам Республики Узбекистан
Приложение Е		Содержит перечень технических отклонений и объяснение причин их внесения
Библиография	Исключена	Ссылки [1], [11] - [16] исключены в связи с исключением ссылок на них в тексте государственного стандарта
		Ссылки [2] - [10] исключены в связи с тем, что международные стандарты заменены на государственные стандарты в соответствии с приложением D и перенесены в раздел 2

ОКС 35.040

Ключевые слова: политика управления инцидентами информационной безопасности, план управления инцидентами информационной безопасности, группа реагирования на инциденты информационной безопасности, извлеченный опыт

Заместитель генерального директора Единого интегратора UZINFOCOM _____ Э. Гимранов

Начальник Единого контактного центра _____ Я. Бахтияров

Нормоконтроль ГУП «UNICON.UZ» _____ Л. Шаймарданова

СОГЛАСОВАНО

Начальник Управления информационной безопасности Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан

С. Абдуганиев
письмо от
№

СОГЛАСОВАНО

Служба государственной безопасности Республики Узбекистан

письмо от
№

СОГЛАСОВАНО

Директор ГУП Центр научно-технических и маркетинговых исследований «UNICON.UZ»

М. Махмудов
письмо от
№

СОГЛАСОВАНО

Директор ГУ «Центр информационной безопасности и содействия в обеспечении общественного порядка»

А. Ходжаев
письмо от
№