ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Управление инцидентами информационной безопасности

Часть 1

Принципы управления инцидентами

(ISO/IEC 27035-1:2016, 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 27035-1:2016 Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management (Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Часть 1. Принципы менеджмента инцидентов)

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

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

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

Политики или средства управления информационной безопасности (ИБ) сами по себе не гарантируют полную защиту информации, информационных систем, служб или сетей. После реализации средств управления могут остаться уязвимости, которые могут стать причиной снижения эффективности ИБ и возникновения инцидентов ИБ. Данное обстоятельство потенциально может иметь прямое и косвенное неблагоприятное воздействие на бизнес-деятельность организации. Кроме того, неизбежно появление новых типов ранее не идентифицированных угроз. Недостаточная подготовка организации к решению таких инцидентов приведет к менее эффективному ответному реагированию и увеличит степень потенциального неблагоприятного воздействия на ее деятельность. Вследствие этого для любой организации, заинтересованной в эффективной программе ИБ, необходимо иметь структурированный и спланированный подход к:

- выявлению, отчетности и оценке инцидентов ИБ;
- реагированию на инциденты ИБ, включая активизацию соответствующих средств управления для предотвращения, уменьшения и восстановления после неблагоприятных последствий инцидентов;
- отчетности по уязвимостям ИБ для принятия соответствующих мер по их оценке и решению;
- извлечению опыта из инцидентов и уязвимостей ИБ, внедрению превентивных средств управления и совершенствованию общего подхода к управлению инцидентами ИБ.

В целях достижения такого спланированного подхода стандарты предоставляют руководство по аспектам управления инцидентами ИБ, в частности:

- O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD) (настоящий стандарт) предоставляет основные понятия и этапы управления инцидентами ИБ и способы улучшения управления инцидентами. Данная часть объединяет эти понятия с принципами структурированного подхода к выявлению, отчетности, оценке и реагированию на инциденты и применению извлеченного опыта;
- O‘z DSt 3387:2019 (ISO/IEC 27035-2:2016, MOD) описывает, как планировать и готовиться к реагированию на инциденты. Эта часть охватывает этапы «Планирование и подготовка» и «Извлеченный опыт».

Стандарты призваны дополнять другие стандарты и документы, которые предоставляют руководство по расследованию инцидентов ИБ и подготовке к расследованию. Стандарты не являются исчерпывающим руководством, а ссылаются на определенные основополагающие принципы, которые призваны обеспечить надлежащие выбор средств, способов и

методов и демонстрацию их пригодности для достижения целей в случае необходимости.

Стандарты включают в себя управление инцидентами ИБ, а также охватывают некоторые аспекты уязвимостей ИБ.

Стандарты также предназначены для информирования лиц, принимающих решения по определению достоверности представленных им цифровых доказательств (свидетельств) и применимы к организациям, которым необходимо защищать, анализировать и представлять потенциальные цифровые данные. Такими организациями являются руководящие органы, которые создают и оценивают процедуры, связанные с цифровыми доказательствами, в том числе в качестве большей совокупности доказательств.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
ХАВФСИЗЛИКНИ ТАЪМИНЛАШ УСУЛЛАРИ
Ахборот хавфсизлиги инцидентларини бошқариш
1-қисм
Инцидентларини бошқариш принциплари

Информационная технология
МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Управление инцидентами информационной безопасности
Часть 1
Принципы управления инцидентами

Information technology. Security techniques.
Information security incident management.
Part 1. Principles of incident management

Дата введения 01.04.2019

1 Область применения

Настоящий стандарт является основой стандартов серии ISO/IEC 27035. В нем представлены основные понятия и этапы управления инцидентами ИБ и связь этих понятий с принципами структурированного подхода к обнаружению, отчетности, оценке и реагированию на инциденты, а также применению извлеченного опыта.

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.

Издание официальное

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 27010:2015 Информационная технология. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью при коммуникациях между отраслями и между организациями

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 3387:2019 (ISO/IEC 27035-2:2016, MOD) Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2. Руководящие указания по планированию и подготовке к реагированию на инциденты

O‘z DSt ISO/IEC 27037:2017 Информационная технология. Методы обеспечения безопасности. Руководящие указания по идентификации, сбору, получению и сохранению цифровых доказательств

O‘z DSt ISO/IEC 27040:2018 Информационная технология. Методы обеспечения безопасности. Безопасность хранения данных

O‘z DSt 3361:2019 (ISO/IEC 27041:2015, MOD) Информационная технология. Методы обеспечения безопасности. Руководство по обеспечению пригодности и адекватности методов расследования инцидентов

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 и определения

В настоящем стандарте применены термины по O‘z DSt ISO/IEC 27000, а также следующие термины с соответствующими определениями:

3.1 **группа реагирования на инциденты информационной безопасности; ГРИИБ** (incident response team): Команда квалифицированных и доверенных сотрудников организации, которая обрабатывает инциденты в течение их жизненного цикла.

Примечание - CERT (Computer Emergency Response Team, служба реагирования на компьютерные инциденты) и CSIRT (Computer Security Incident Response Team, служба реагирования на инциденты компьютерной безопасности) являются часто используемыми синонимами ГРИИБ.

3.2 **координатор** (point of contact, PoC): Контактное лицо, определенное организационной должностью или ролью и отвечающее за координацию информации, касающейся деятельности по управлению инцидентами.

3.3 **обработка инцидентов** (incident handling): Действия по выявлению, отчетности, оценке, реагированию, решению и извлечению опыта из инцидентов информационной безопасности.

3.4 **расследование информационной безопасности** (information security investigation): Проведение экспертизы, анализа и обработка результатов анализа, которые способствуют пониманию инцидента информационной безопасности.

3.5 **реагирование на инцидент** (incident response): Действия, предпринятые для смягчения или устранения инцидента информационной безопасности, включая меры, принятые для защиты и восстановления нормальных рабочих режимов эксплуатации информационной системы и информации, хранящейся в ней.

4 Обзор

4.1 Основные понятия и принципы

Событие ИБ - идентифицированный случай состояния системы или сети, указывающий на возможное нарушение политики ИБ или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности. Инцидент ИБ - единичное событие или ряд нежелательных или непредвиденных событий ИБ, из-за которых велика вероятность компрометации защищаемой информации и реализации угрозы информационной безопасности.

Возникновение события ИБ не обязательно означает, что атака была успешной или имеются какие-либо последствия для конфиденциальности,

целостности или доступности, то есть не все события ИБ классифицируются как инциденты ИБ.

Инциденты ИБ могут быть преднамеренными (например, вызванные вредоносным программным обеспечением или умышленным нарушением эксплуатации информационной системы) или случайными (например, вызванные непреднамеренной человеческой ошибкой или неотвратимыми стихийными бедствиями), они могут быть вызваны техническими (например, компьютерными вирусами) или нетехническими (например, потеря или кража компьютеров) средствами. Последствиями влияния инцидентов могут стать несанкционированное раскрытие, модификация, уничтожение или недоступность информации, повреждение или кража информационных активов организации.

В приложении А приведено описание отдельных примеров инцидентов ИБ и их причин исключительно в ознакомительных целях. Важно отметить, что эти примеры ни в коем случае не являются исчерпывающими.

Угроза появляется при наличии уязвимостей (слабостей) в информационных системах, службах или сетях, что приводит к возникновению событий ИБ и, таким образом, потенциально вызывает инциденты в информационных активах, подверженных уязвимостям. На рисунке 1 приведена взаимосвязь объектов при инциденте ИБ.

Рисунок 1 - Взаимосвязь объектов при инциденте ИБ

Обмен информацией и координация с внешними ГРИИБ являются важными факторами. Многие инциденты развиваются вне рамок одной организации и не могут быть легко разрешены одной ГРИИБ. Обмен информацией и координация отношений или партнерство с внешними ГРИИБ могут значительно повысить способность реагировать на инциденты и разрешать их. В O‘z DSt ISO/IEC 27010 приведена дополнительная информация об обмене информацией.

4.2 Цели управления инцидентами

В качестве ключевой части общей стратегии ИБ организация должна внедрить средства управления и процедуры для обеспечения структурированного и четко спланированного подхода к управлению инцидентами ИБ. С точки зрения организации, главная цель - избегать или сдерживать воздействие инцидентов ИБ, чтобы свести к минимуму прямой и косвенный ущерб для ее деятельности, вызванный этими инцидентами. Поскольку ущерб информационным ресурсам может оказать негативное влияние на деятельность, понимание операционных и бизнес-процессов должно иметь большое влияние на определение более конкретных целей управления ИБ.

Цели структурированного и четко спланированного подхода к управлению инцидентами должны включать следующее:

a) выявление и решение событий ИБ эффективным путем, в частности, принятие решений о том, когда их следует классифицировать как инциденты ИБ;

b) оценку и реагирование на выявленные инциденты ИБ наиболее подходящим и эффективным образом;

c) сведение к минимуму неблагоприятных последствий инцидентов ИБ для организации и ее деятельности с помощью соответствующих средств управления в рамках реагирования на инциденты;

d) установление связи с соответствующими элементами управления кризисными ситуациями и управления непрерывностью бизнеса посредством процесса эскалации (процесса обращения к вышестоящим организациям);

e) оценку уязвимостей ИБ и их надлежащее решение для предотвращения или сокращения количества инцидентов. Такая оценка может быть выполнена ГРИИБ, либо другими группами внутри организации, в зависимости от распределения обязанностей;

f) быстрое извлечение опыта из инцидентов ИБ, уязвимостей и управления ими. Этот механизм обратной связи призван увеличить шансы предотвратить появление инцидентов ИБ, улучшить внедрение и

использование средств управления ИБ и общий план управления инцидентами ИБ.

Для достижения вышеперечисленных целей организации должны обеспечить документирование инцидентов ИБ согласованным образом с использованием соответствующих стандартов для распределения инцидентов по категориям и классификации, а также совместного их использования. Таким образом, количественные показатели будут получены из совокупных данных за определенный период времени, что, в свою очередь, даст ценную информацию для принятия стратегических решений при инвестировании в средства управления ИБ. Система управления инцидентами ИБ должна иметь возможность обмениваться информацией с соответствующими третьими сторонами и ГРИИБ.

Другой целью, связанной с настоящим стандартом, является предоставление руководства организациям, которые стремятся соответствовать требованиям к системам управления информационной безопасности (СУИБ), установленным в O‘z DSt ISO/IEC 27001 и поддерживаемым рекомендациями O‘z DSt ISO/IEC 27002. O‘z DSt ISO/IEC 27001 содержит требования, связанные с управлением инцидентами ИБ. В приложении В настоящего стандарта приведены сведения о соответствии между O‘z DSt ISO/IEC 27001, O‘z DSt 3386, O‘z DSt 3387. Взаимосвязи СУИБ представлены на рисунке 2. Настоящий стандарт также может удовлетворять требованиям, предъявляемым к различным СУИБ.

Рисунок 2 - Управление инцидентами ИБ применительно к СУИБ и средствам управления

4.3 Преимущества структурированного подхода

Использование структурированного подхода к управлению инцидентами ИБ может дать значительные преимущества, которые можно сгруппировать по следующим тематикам:

a) улучшение ИБ в целом.

Структурированный процесс выявления, отчетности, оценки и принятия решений, связанных с событиями и инцидентами ИБ, позволит быстро идентифицировать и реагировать на них. Это улучшит общую безопасность путем быстрого определения и внедрения последовательного решения и предоставления средств, которые будут способствовать предотвращению в будущем схожих инцидентов ИБ. Кроме того, будут получены преимущества от количественных показателей, совместного использования и совокупных данных. Доверие к организации будет улучшено путем демонстрации внедрения ею передовой практики в отношении управления инцидентами ИБ;

b) снижение неблагоприятного воздействия на бизнес.

Структурированный подход к управлению инцидентами ИБ может помочь снижению уровня возможного неблагоприятного воздействия, связанного с инцидентами ИБ, на бизнес-деятельность. Неблагоприятные последствия могут включать немедленные и долгосрочные финансовые потери, возникшие вследствие нанесенного ущерба репутации и потери доверия. Руководство по анализу воздействия инцидентов на бизнес приведено в O‘z DSt ISO/IEC 27005. Информация о готовности информационных и коммуникационных технологий к обеспечению непрерывности бизнеса приведена в O‘z DSt ISO/IEC 27031;

c) усиление акцента на предотвращении инцидентов ИБ.

Использование структурированного подхода к управлению инцидентами ИБ помогает лучше сосредоточиться на предотвращении инцидентов внутри организации, включая разработку методов выявления новых угроз и уязвимостей. Анализ данных, связанных с инцидентами, позволяет выявлять закономерности и тенденции, тем самым облегчая более точное фокусирование на предотвращении инцидентов и определении соответствующих действий для предотвращения их дальнейшего возникновения;

d) усовершенствование системы установления приоритетов.

Структурированный подход к управлению инцидентами ИБ обеспечит прочную основу для установления приоритетов при проведении расследования инцидентов ИБ, включая использование эффективной системы категорирования и классификации инцидентов. При отсутствии четко обозначенных процедур существует риск того, что деятельность по расследованию инцидентов может быть проведена в чрезмерно реактивном

режиме, реагируя на инциденты по мере их возникновения и игнорируя при этом действия с более высоким приоритетом выполнения;

e) поддержка сбора доказательств и проведения расследования.

Четкие процедуры расследования инцидентов обеспечат правильный и легитимный подход при сборе и обработке данных, когда это потребуется. Они имеют важное значение в случае судебного преследования или дисциплинарного разбирательства;

f) распределение бюджетных и ресурсных средств.

Четко спланированный и структурированный подход к управлению инцидентами ИБ будет содействовать обоснованию и упрощению распределения бюджетных и ресурсных средств для задействованных организационных подразделений. Кроме того, преимущество получит и сам план управления инцидентами ИБ, с возможностью более эффективного планирования распределения персонала и ресурсов.

Одним из способов контроля и оптимизации бюджета и ресурсов является добавление к задачам управления инцидентами ИБ функции отслеживания времени для облегчения количественной оценки процесса обработки организацией инцидентов ИБ. Такая функция позволит предоставлять информацию о том, сколько времени потребуется для решения инцидентов ИБ с различными приоритетами и на разных платформах. При наличии слабых мест процесса управления инцидентами ИБ, они также должны быть идентифицируемыми;

g) совершенствование обновлений результатов определения и управления рисками ИБ.

Использование структурированного подхода к управлению инцидентами ИБ способствует:

- улучшению сбора данных для выявления и определения характеристик различных типов угроз и связанных с ними уязвимостей;
- предоставлению данных о частоте возникновения идентифицированных типов угроз.

Полученные данные о неблагоприятном воздействии на бизнес-деятельность инцидентов ИБ будут полезны при анализе влияния на бизнес. Данные, полученные для определения частоты возникновения различных типов угроз, повысят качество оценки угрозы. Аналогичным образом, полученные данные об уязвимостях улучшат качество будущих оценок уязвимостей. Руководство по определению и управлению рисками ИБ представлено в O‘z DSt ISO/IEC 27005;

h) предоставление материала для программ повышения осведомленности и обучения ИБ.

Структурированный подход к управлению инцидентами ИБ позволит организации обобщать опыт и знания о том, как она обрабатывает инциденты, что станет ценным материалом для программы повышения осведомленности ИБ. Такая программа, учитывающая извлеченный практический опыт поможет сократить количество ошибок или неопределенностей при расследовании будущих инцидентов ИБ;

i) предоставление информации для проверок политики ИБ и соответствующей документации.

Данные, предоставленные планом управления инцидентами ИБ, могут внести ценный вклад для проверки эффективности и последующего совершенствования политики ИБ (и другой соответствующей документации ИБ). Это относится к тематическим политикам и другой документации, применимым как для всей организации, так и для отдельных систем, служб и сетей.

4.4 Применимость

Руководство, представленное в стандартах O‘z DSt 3386, O‘z DSt 3387, обширно и, если оно будет принято в полном объеме, могут потребоваться значительные ресурсы для работ по выявлению инцидентами ИБ и управления ими. В связи с этим важно, чтобы организация, применяющая это руководство, придерживалась адекватной оценки и обеспечивала пропорциональность ресурсов, применяемых для управления инцидентами ИБ, и сложность реализованных механизмов соответственно:

a) размеру, структуре и виду деятельности организации, включая ключевые критически важные активы, процессы и данные, которые должны быть защищены;

b) объему любой СУИБ для обработки инцидентов;

c) потенциальному риску вследствие инцидентов;

d) целям бизнес-деятельности.

Организации, использующей настоящий стандарт, следует применять изложенное в нем руководство пропорционально масштабу и особенностям ее бизнеса.

5 Этапы

5.1 Обзор

Для достижения целей, приведенных в 4.2, управление инцидентами ИБ состоит из следующих пяти отдельных этапов:

- планирование и подготовка (см. 5.2);
- выявление и отчетность (см. 5.3);
- оценка и принятие решений (см. 5.4);
- ответное реагирование (см. 5.5);
- извлеченный опыт (см. 5.6).

Детальное представление этих этапов представлено на рисунке 3.

Некоторые действия могут происходить в несколько этапов или на протяжении всего процесса обработки инцидентов. К таким видам деятельности относятся следующие действия:

- документирование событий и инцидентов и ключевой информации, принятых мер реагирования и последующих действий в рамках процесса обработки инцидентов;
- координация и связь между участвующими сторонами;
- уведомление руководства и других заинтересованных сторон о значительных инцидентах;
- обмен информацией между заинтересованными сторонами и внутренними и внешними сотрудниками, такими как поставщики и другие ГРИИБ.

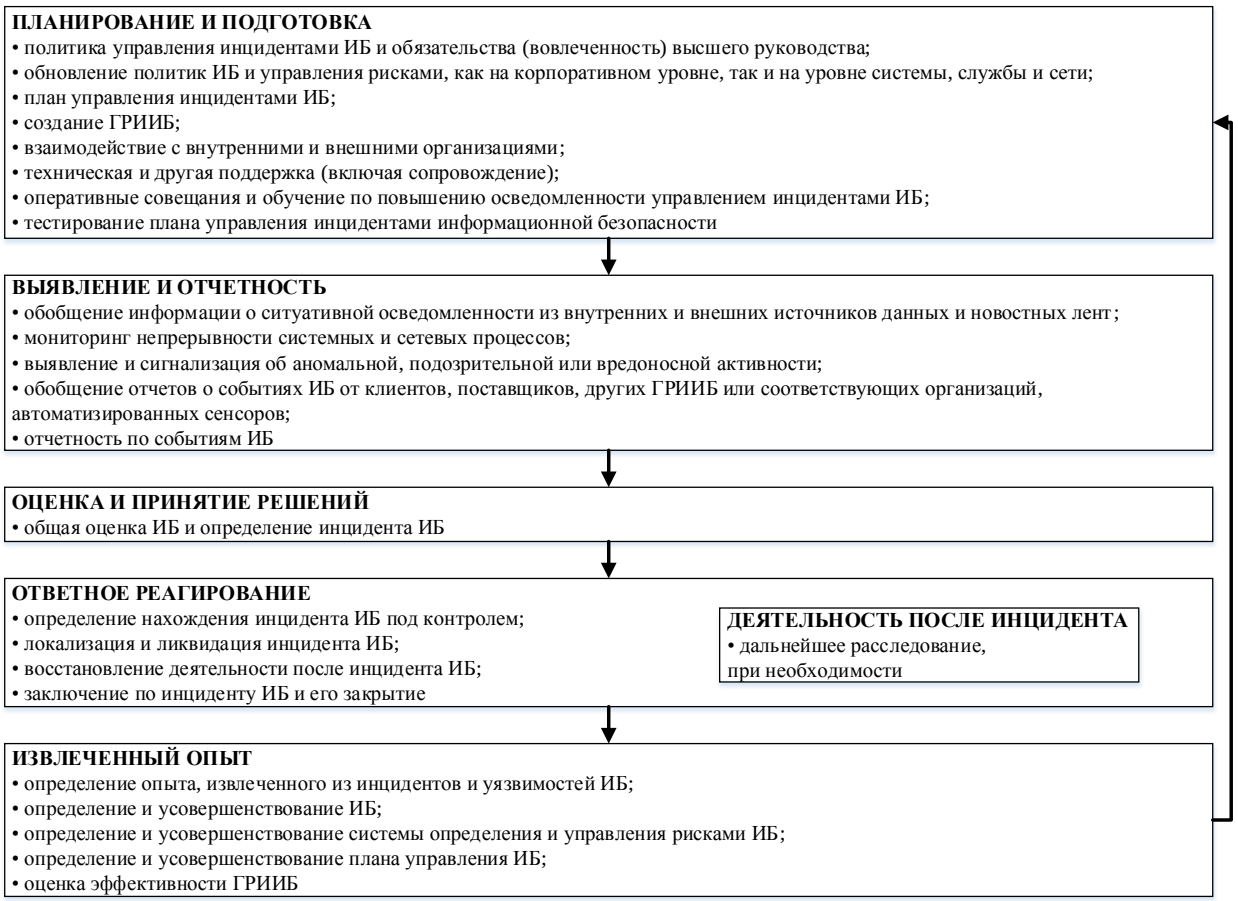

Рисунок 3 - Этапы управления инцидентами ИБ

Стандарт O‘z DSt 3386 охватывает все пять этапов.

Стандарт O‘z DSt 3387 охватывает этапы «Планирование и подготовка» и «Извлеченный опыт».

На рисунке 4 показан поток событий и инцидентов ИБ на этапах управления инцидентами ИБ и связанные с ними действия.

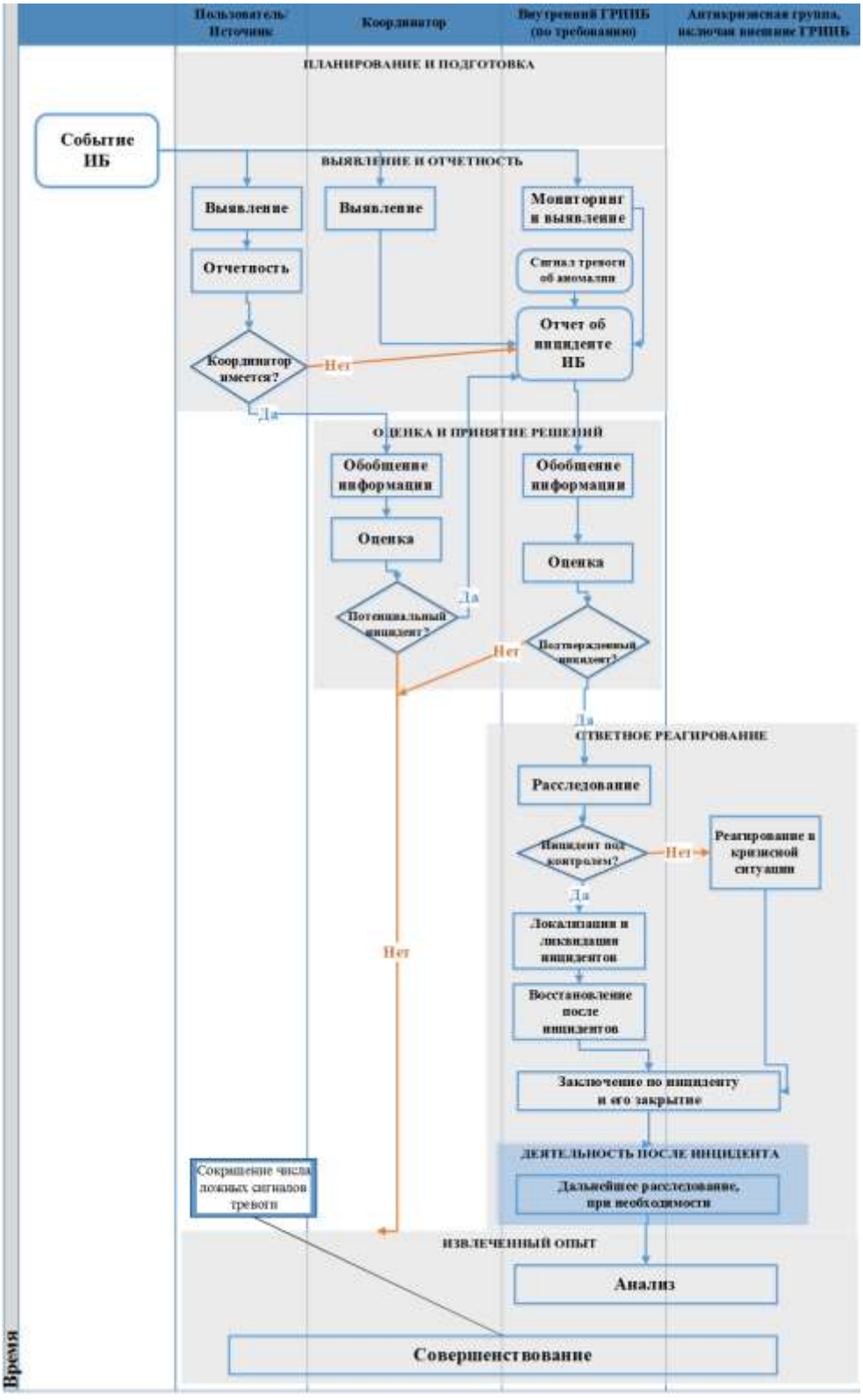

Рисунок 4 - Диаграмма потоков событий и инцидентов ИБ

5.2 Планирование и подготовка

Эффективное управление инцидентами ИБ требует надлежащего планирования и подготовки. Для принятия практичного и эффективного плана управления инцидентами ИБ организация должна завершить ряд следующих подготовительных мероприятий:

a) формулировка и разработка политики управления инцидентами ИБ с вовлечением высшего руководства в данный процесс;

b) обновление политик ИБ, в том числе связанных с управлением рисками, как на корпоративном уровне, так и применительно к системам, службам и сетям;

c) определение и документирование подробного плана управления инцидентами ИБ, включая вопросы связи и раскрытия информации;

d) создание ГРИИБ с соответствующей программой обучения, разработанной и предоставленной персоналу организации;

e) установление и поддержание соответствующих отношений и связей с внутренними и внешними организациями, которые непосредственно вовлечены в управление событиями, инцидентами и уязвимостями ИБ;

f) создание, внедрение и использование технических, организационных и операционных механизмов для поддержки плана управления инцидентами ИБ и деятельности ГРИИБ. Разработка и развертывание необходимых информационных систем для поддержки ГРИИБ, включая базу данных ИБ. Эти механизмы и системы предназначены для предотвращения возникновения инцидентов ИБ или уменьшения вероятности их возникновения;

g) разработка программы обучения и повышения осведомленности в области управления событиями, инцидентами и уязвимостями ИБ;

h) проверка использования плана управления инцидентами ИБ, его процессов и процедур.

По завершению этого этапа организация должна быть полностью подготовлена к надлежащему управлению инцидентами ИБ. В O‘z DSt 3387 приведено описание каждого из перечисленных выше видов деятельности, включая содержание документов политики и планирования.

5.3 Выявление и отчетность

Второй этап управления инцидентами ИБ включает в себя выявление событий ИБ, обобщение информации, связанной с ними, и отчетность по их возникновению и наличию уязвимостей ИБ с помощью ручных или

автоматических средств. На этом этапе события и уязвимости могут еще не классифицироваться как инциденты информационной безопасности.

Отчетность о событиях ИБ в соответствии с политиками отчетности организации позволяет, в случае необходимости, провести последующий анализ.

На этапе выявления и отчетности событий ИБ организация должна предпринять следующие основные действия:

a) мониторинг и регистрацию (протоколирование) системной и сетевой активности головной организации и подчиненных ей организаций;

b) выявление и отчетность о возникновении события ИБ или о наличии уязвимости ИБ, как вручную персоналом, так и автоматически;

c) обобщение информации о событии или уязвимости ИБ;

d) обобщение информации, влияющей на мероприятия по ИБ, из внутренних и внешних источников данных, включая журналы регистрации системной или сетевой активности, о текущей политической, социальной или экономической деятельности, тенденциях в отношении инцидентов, новых векторах атак, текущих индикаторах атак, новых стратегиях и технологиях по смягчению последствий атак;

e) обеспечение надлежащей регистрации всех действий, результатов и соответствующих принятых решений для последующего анализа;

f) обеспечение безопасного сбора и хранения цифровых доказательств и непрерывного мониторинга такого безопасного сохранения, в случае, если доказательства требуются для судебного преследования или внутренних дисциплинарных мер;

g) обеспечение соблюдения режима контроля за изменениями, позволяющего обновлять функции отслеживания и отчетности событий и уязвимостей ИБ, а также поддерживать базу данных ИБ в актуальном состоянии;

h) увеличение числа последующих проверок или принятых решений на протяжении всего этапа, по мере необходимости.

Вся собранная и обобщенная информация, относящаяся к событию или уязвимости ИБ, должна храниться в базе данных ИБ, управляемой ГРИИБ. Информация, указанная в отчетности во время каждого мероприятия, должна быть как можно более полной на текущий момент, что способствует принятию соответствующей оценки, решений и действий.

5.4 Оценка и принятие решений

Третий этап управления инцидентами ИБ включает в себя оценку информации, связанной с событиями ИБ, и принятие решения о том, классифицировать ли события как инциденты ИБ.

После выявления и отчетности события ИБ, на этапе «Оценка и принятие решений» организация должна выполнять следующие основные виды деятельности:

a) распределение ответственности за мероприятия по управлению инцидентами ИБ, включая оценку, принятие решений и действия посредством соответствующей иерархии персонала, с привлечением как сотрудников службы безопасности, так и других сотрудников;

b) предоставление для каждого уведомленного лица официальных процедур, которые должны соблюдаться, включая рассмотрение и изменение составленных отчетов, оценку ущерба и уведомление соответствующего персонала. Индивидуальные действия будут зависеть от типа и серьезности инцидента;

c) использование руководящих принципов для тщательной документации событий ИБ и последующих действий для инцидента ИБ, если событие ИБ классифицируется как инцидент ИБ;

d) обобщение информации, которая может включать в себя тестирование, измерение и другие данные по выявлению события ИБ. Тип и количество собранной информации будет зависеть от события ИБ, которое произошло;

e) проведение оценки обработчиком инцидентов для определения, является ли событие потенциальным или подтвержденным инцидентом ИБ или ложным сигналом тревоги. Ложный сигнал тревоги (то есть ошибочный допуск) указывает на событие, которое было представлено в отчетности как ненастоящее или не имеющее каких-либо последствий. ГРИИБ может провести проверку качества, чтобы убедиться, что обработчик инцидентов правильно обозначил инцидент;

f) обеспечение надлежащей регистрации всех действий, результатов и соответствующих принятых решений для последующего анализа, всеми вовлеченными сторонами, особенно ГРИИБ;

g) обеспечение соблюдения режима контроля за изменениями, позволяющего обновлять функции отслеживания и отчетности событий и уязвимостей ИБ, а также поддерживать базу данных ИБ в актуальном состоянии.

Вся собранная и обобщенная информация, относящаяся к событию или уязвимости ИБ, должна храниться в базе данных ИБ, управляемой ГРИИБ. Информация, указанная в отчетности во время каждого мероприятия, должна быть как можно более полной на текущий момент, что способствует принятию соответствующей оценки, решений и действий.

5.5 Ответное реагирование

Четвертый этап управления инцидентами ИБ предполагает ответное реагирование на инциденты ИБ в соответствии с действиями, определенными на этапе оценки и принятия решений. В зависимости от решений реагирование может быть немедленным, в режиме реального времени или близко к нему, а также включать в себя расследование ИБ.

После подтверждения инцидента ИБ и определения реагирования, на этапе «Ответное реагирование», организация должна выполнять следующие основные действия:

a) распределение ответственности за мероприятия по управлению инцидентами ИБ, включая оценку, принятие решений и действия посредством соответствующей иерархии персонала, с привлечением как сотрудников службы безопасности, так и других сотрудников;

b) предоставление для каждого уведомленного лица официальных процедур, которые должны соблюдаться, включая рассмотрение и изменение составленных отчетов, оценку ущерба и уведомление соответствующего персонала. Индивидуальные действия будут зависеть от типа и серьезности инцидента;

c) использование руководящих принципов для тщательной документации инцидента ИБ и последующих действий;

d) расследование инцидентов по мере необходимости и применительно к шкале классификации инцидентов ИБ. Изменение этой шкалы должно проводиться по мере необходимости. Расследование может включать в себя различные виды анализа для обеспечения более глубокого понимания природы инцидентов;

e) анализ со стороны ГРИИБ для установления факта нахождения инцидента ИБ под контролем и, в случае положительного результата - выполнение требуемого ответного реагирования. Если инцидент не находится под контролем или он может оказать серьезное воздействие на деятельность организации, выполнение антикризисных действий путем процесса эскалации до функции управления кризисом;

f) назначение внутренних ресурсов и определение внешних ресурсов для реагирования на инцидент;

g) увеличение числа последующих проверок или принятых решений на протяжении всего этапа, по мере необходимости;

h) обеспечение надлежащей регистрации всех действий, результатов и соответствующих принятых решений для последующего анализа, всеми вовлеченными сторонами, особенно ГРИИБ;

i) обеспечение безопасного сбора и хранения цифровых доказательств и непрерывного мониторинга такого безопасного сохранения, в случае, если

доказательства требуются для судебного преследования или внутренних дисциплинарных мер;

j) обеспечение соблюдения режима контроля за изменениями, позволяющего обновлять функции отслеживания и отчетности событий и уязвимостей ИБ, а также поддерживать базу данных ИБ в актуальном состоянии;

k) доведение информации о наличии инцидента ИБ и распространение любых соответствующих данных (например, информация об угрозах, атаках и уязвимостях) до других внутренних и внешних лиц или организаций в соответствии с планами организации и ГРИИБ по передаче информации и политиками раскрытия информации. Особенно важно уведомлять владельцев активов (определяемых во время анализа последствий), внутренние и внешние организации (например, другие ГРИИБ, правоохранительные органы, интернет-провайдеров и организации, предоставляющие информацию), которые могли бы помочь в управлении и разрешении (включая обнаружение, изучение и устранение последствий) инцидента. Обмен информацией может также принести пользу другим организациям, поскольку одни и те же угрозы и атаки часто затрагивают несколько организаций. Дополнительная информация об обмене информацией приведена в O‘z DSt ISO/IEC 27010;

l) инициирование деятельности после устранения последствий воздействия инцидента в зависимости от его характера и серьезности. Эта деятельность включает:

1) изучение информации, относящейся к инциденту;

2) изучение других соответствующих источников, таких как задействованный персонал;

3) обобщенный отчет о результатах изучения;

m) закрытие инцидента после его разрешения (включая обнаружение, изучение и устранение последствий) в соответствии с требованиями ГРИИБ или головной организации с уведомлением всех заинтересованных сторон.

Вся собранная и обобщенная информация, относящаяся к событию или уязвимости ИБ, должна храниться в базе данных ИБ, управляемой ГРИИБ. Информация, указанная в отчетности во время каждого мероприятия, должна быть как можно более полной на текущий момент, что способствует принятию соответствующей оценки, решений и действий, включая потенциальный последующий анализ.

5.6 Извлеченный опыт

Пятый этап управления инцидентами ИБ настает после разрешения (включая обнаружение, изучение и устранение последствий) инцидентов ИБ. Этот этап включает в себя изучение опыта (уроков) из того, каким образом были обработаны инциденты и уязвимости.

На этапе «Извлеченный опыт» организация должна выполнять следующие основные действия:

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

b) анализ, выявление и совершенствование реализации средств управления ИБ (новые или обновленные средства управления), а также политики управления инцидентами ИБ. Опыт можно извлечь из одного или нескольких инцидентов ИБ или сообщений об уязвимостях безопасности. Усовершенствованию способствуют количественные показатели, входящие в стратегию организации и указывающие направление инвестиций в средства управления ИБ;

c) анализ, выявление и совершенствование существующей системы определения и управления рисками ИБ организации;

d) анализ эффективности процессов, процедур, форматов отчетов и организационной структуры при реагировании, оценке и восстановлении после инцидента ИБ и обработки уязвимостей ИБ;

e) взаимодействие и обмен результатами анализа внутри доверенного круга лиц (по желанию организации);

f) определение совместного использования информации об инцидентах, связанных с ними векторов атак и уязвимостей организациями-партнерами для предотвращения схожих инцидентов в их среде. Дополнительная информация об обмене информацией приведена в O‘z DSt ISO/IEC 27010;

g) проведение на периодической основе комплексной оценки эффективности ГРИИБ.

Следует подчеркнуть, что операции по управлению инцидентами ИБ являются повторяющимися, следовательно, организация должна регулярно совершенствовать элементы ИБ. Такие усовершенствования должны следовать из анализа данных об инцидентах ИБ, ответном реагировании и уязвимостях ИБ.

O‘z DSt 3387 подробно описывает каждый из перечисленных выше видов деятельности.

Приложение А
(справочное)

Примеры инцидентов информационной безопасности и их причины

А.1 Атаки

А.1.1 Отказ в обслуживании

Атаки типа DoS (denial of service; отказ в обслуживании) и DDoS (distributed denial of service; распределенный отказ в обслуживании) - большие категории инцидентов, имеющие общую направленность. Такого рода инциденты являются причиной прекращения работы системы, службы или сети в полном объеме всех возможностей, чаще всего с полным отказом в доступе авторизованным пользователям. Существует два основных типа инцидентов DoS и DDoS, вызванных техническими средствами: ликвидация источника или зависание источника.

Некоторые типичные примеры намеренных технических инцидентов DoS и DDoS включают в себя:

- проверку с помощью пинг-запросов сетевой передачи с целью заполнения сетевого диапазона ответным трафиком;
- отправку данных в неизвестном формате в систему, службу или сеть, с целью ее выхода из строя или прерывания нормального функционирования;
- открытие нескольких санкционированных сессий с конкретной системой, службой или сетью, с целью исчерпания ее ресурсов (т.е., замедление, закрытие или сбой).

Такие атаки часто осуществляются посредством ботов, управляемых ботнетом - компьютерной сетью, запускающей вредоносный код. Ботнет - это централизованная командная и управляющая ботами сеть, регулируемая людьми. Ботнеты могут состоять из сотен и миллионов зараженных компьютеров.

Некоторые инциденты DoS технического характера могут быть вызваны случайно, например, неверной конфигурацией оператора или несовместимостью программного обеспечения, но, в большинстве случаев, они являются намеренными. Некоторые инциденты DoS технического характера запускаются преднамеренно с целью выведения из строя системы или службы, закрытия сети, в то время как другие являются побочными продуктами другой злонамеренной деятельности. Например, некоторые методы идентификации и скрытного сканирования могут вызывать выход из строя старых систем или систем и служб с неверной конфигурацией во время сканирования. Следует отметить, что многие инциденты DoS технического характера часто запускаются анонимно (т.е. источник атаки

сфальсифицирован), поскольку они обычно не зависят от злоумышленника, получающего какую-либо информацию из атакованной сети или системы.

Причинами инцидентов DoS нетехнического характера, заканчивающихся потерей информации, службы и/или материальных средств, могут быть:

- нарушения мер физической безопасности, заканчивающиеся кражей, преднамеренным повреждением или выведением из строя оборудования;
- случайные повреждения аппаратных средств (и/или мест их расположения) в результате пожара или наводнения;
- чрезвычайные условия окружающей среды, например, высокая рабочая температура (в результате сбоя работы кондиционера);
- системные сбои или перезагрузки;
- неконтролируемые изменения системы;
- сбои программного обеспечения или аппаратных средств.

A.1.2 Несанкционированный доступ

В целом, эта категория инцидентов состоит из попыток несанкционированного доступа и использования системы, службы или сети. Некоторые примеры инцидентов несанкционированного доступа технического характера включают в себя:

- попытки восстановить файлы паролей;
- атаки переполнения буфера обмена для получения привилегированного (например, на уровне системного администратора) доступа к объекту;
- использование уязвимостей протокола для захвата или перенаправления санкционированных сетевых подключений;
- попытки повышения существующего уровня привилегий на доступ к ресурсам или информации, которыми на законных основаниях владеет пользователь или администратор.

Инциденты несанкционированного доступа нетехнического характера, возникающие в результате прямого или косвенного раскрытия или модификации информации, нарушений подотчетности или неправильного использования информационных систем, могут быть вызваны:

- нарушениями мер физической безопасности в результате несанкционированного доступа к информации;
- плохой и/или неправильной настройкой конфигурации операционных систем из-за неконтролируемых системных изменений или сбоев программного обеспечения или аппаратных средств.

A.1.3 Вредоносные коды

Вредоносный код определяется как программа или часть программы, встроенная в другую программу с целью изменения ее первоначальной модели поведения, как правило, для выполнения потенциально опасных видов деятельности, таких как кража информации и персональных данных, уничтожение информации и ресурсов, DoS-атаки, спаминг и др. Атаки с применением вредоносного кода могут быть разделены на пять категорий: вирусы, черви, трояны, мобильные коды и смешанные категории. Изначально вирусы писались для получения уязвимой зараженной системы, однако в настоящее время для выполнения целевых атак используются и другие вредоносные коды. Иногда это происходит путем изменения существующего вредоносного кода и создания такой его разновидности, которая часто не распознается технологиями обнаружения вредоносного кода.

A.1.4 Злоупотребление

Инцидент подобного рода происходит, когда пользователь нарушает политику безопасности информационной системы организации. Подобные инциденты не являются атаками в строгом смысле этого слова, но часто отражаются в отчетах как инциденты и должны управляться ГРИИБ. Злоупотреблением может быть:

- загрузка и установка средств взлома;
- использование корпоративной электронной почты для спаминга или продвижения личного бизнеса;
- использование корпоративных ресурсов для создания несанкционированного веб-сайта;
- использование децентрализованной пиринговой сети для приобретения или распространения пиратских файлов (музыка, видео, программное обеспечение).

A.2 Сбор информации

В общих чертах, категория инцидентов сбора информации включает в себя виды деятельности, связанные с выявлением потенциальных целей и пониманием принципа работы служб, направленных на достижение этих целей. Этот тип инцидента предполагает ознакомление с информацией, с целью определения:

- наличия цели и понимания топологии окружающей ее сети, и того, с кем цель регулярно взаимодействует;
- потенциальных уязвимостей в целевой среде или непосредственно в сетевой среде, которые могут быть использованы.

Типичные примеры атак сбора информации технического характера включают в себя:

- сброс записей DNS (Domain Name System, система доменных имен) для целевого интернет-домена (передача зон DNS);

- пинг-запросы сетевых адресов для поиска действующих систем;

- проверку целевой системы для идентификации (например, с помощью отпечатков пальцев) хостинговой операционной системы;

- сканирование доступных сетевых портов системы с целью выявления сетевых служб (например, электронная почта, протокол передачи файлов, веб-службы и др.) и версий программного обеспечения этих служб;

- сканирование одной или нескольких известных уязвимых служб в диапазоне сетевых адресов (горизонтальное сканирование).

В некоторых случаях сбор информации технического характера распространяется на получение несанкционированного доступа, в случае, например, когда злоумышленник, в процессе поиска уязвимостей, предпринимает попытки получения несанкционированного доступа. Обычно это происходит с помощью автоматизированных средств, которые занимаются не только поиском уязвимостей, но и автоматически предпринимают попытки эксплуатации обнаруженных уязвимостей систем, служб и/или сетей.

Инциденты сбора информации, вызванные нетехническими средствами, приводят к:

- прямому или косвенному раскрытию или модификации информации;

- краже интеллектуальной собственности, хранимой в электронном виде;

- нарушениям подотчетности, например, в регистрации учетной записи;

- неправильной эксплуатации информационных систем (например, способами, противоречащими законодательству или политике организации).

Инциденты сбора информации могут быть вызваны:

- нарушениями мер физической безопасности в результате несанкционированного доступа к информации, а также кражи оборудования хранилища данных, содержащего конфиденциальные данные, например, ключей шифрования;

- плохой и/или неправильной настройкой конфигурации операционных систем из-за неконтролируемых системных изменений или сбоев программного обеспечения, или аппаратных средств, в результате чего внутренний или внешний персонал получает доступ к информации, на который у них отсутствуют полномочия;

- методами социальной инженерии, которая заключается в манипулировании людьми для выполнения ими несанкционированных действий (например, фишинга) или разглашении конфиденциальной информации.

Приложение B
(справочное)

Сведения о соответствии между O‘z DSt ISO/IEC 27001 и стандартами O‘z DSt 3386, O‘z DSt 3387

Таблица B.1

O‘z DSt ISO/IEC 27001	O‘z DSt 3386, O‘z DSt 3387
A.16 Управление инцидентами информационной безопасности	**O‘z DSt 3386** **4 Обзор** (для краткого обзора управления инцидентами ИБ)
A.16.1 Управление инцидентами информационной безопасности и его улучшение Цель: Обеспечить применение последовательного и эффективного подхода к управлению инцидентами ИБ, в том числе к обмену информацией о событиях и недостатках безопасности	**O‘z DSt 3386:** **5 Этапы** (для этапов управления инцидентами ИБ) **Приложение A (справочное) Примеры инцидентов информационной безопасности и их причины** **O‘z DSt 3387:** **Приложение A (справочное) Нормативно-правовые вопросы** **Приложение B (справочное) Примеры отчетов о событиях, инцидентах и уязвимостях информационной безопасности и образец формы отчета** **Приложение C (справочное) Примеры подходов к категоризации и классификации событий и инцидентов информационной безопасности**
A.16.1.1 Ответственность и процедуры Средство управления: Определение ответственности руководства и процедур по управлению инцидентами ИБ, обеспечивающих быстрое, эффективное и организованное реагирование на эти инциденты	**O‘z DSt 3386:** **5.2 Планирование и подготовка** **5.4 Оценка и принятие решений** a), b) **O‘z DSt 3387:** **4 Политика управления инцидентами информационной безопасности**

Продолжение таблицы В.1

O‘z DSt ISO/IEC 27001	O‘z DSt 3386, O‘z DSt 3387
	5 Обновление политики информационной безопасности **6 Разработка плана управления инцидентами информационной безопасности** **7 Создание группы реагирования на инциденты информационной безопасности** **8 Взаимодействие с другими подразделениями организации и другими организациями** **9 Организация технической и другой поддержки** **10 Разработка обучения и повышения осведомленности по инцидентам информационной безопасности**
A.16.1.2 Оповещение о событиях информационной безопасности Средство управления: Незамедлительное, насколько это возможно, оповещение руководства о событиях ИБ по соответствующим каналам	**O‘z DSt 3386** **5.3 Выявление и отчетность**
A.16.1.3 Оповещение о недостатках информационной безопасности Средство управления: Предъявление требования ко всему персоналу и всем работающим по договору о необходимости отмечать и сообщать о любых наблюдаемых или предполагаемых недостатках безопасности в системах или сервисах	**O‘z DSt 3386** **5.3 Выявление и отчетность**

Окончание таблицы B.1

O‘z DSt ISO/IEC 27001	O‘z DSt 3386, O‘z DSt 3387
A.16.1.4 Оценка событий информационной безопасности и принятие решений Средство управления: Оценка событий ИБ и принятие решения о том, следует ли их классифицировать как инциденты ИБ	**O‘z DSt 3386** **5.4 Оценка и принятие решений**
A.16.1.5 Реагирование на инциденты информационной безопасности Средство управления: Реагирование на инциденты ИБ в соответствии с документированными процедурами	**O‘z DSt 3386** **5.5 Ответное реагирование**
A.16.1.6 Изучение инцидентов информационной безопасности Средство управления: Использование знаний, полученных при выполнении анализа и устранении инцидентов ИБ, для уменьшения вероятности возникновения или влияния будущих инцидентов	**O‘z DSt 3386** **5.6 Извлеченный опыт** **O‘z DSt 3387** **12 Обобщение полученного опыта**
A.16.1.7 Сбор свидетельств Средство управления: Определение и применение процедур идентификации, получения и хранения информации, которая может служить в качестве свидетельства	**O‘z DSt 3386** **5.3 Выявление и отчетность** d), g) **5.4 Оценка и принятие решений** d), g) **5.5 Ответное реагирование** d), i), l)

Приложение С
(справочное)

Сведения о соответствии ссылочных международных стандартов государственным стандартам Республики Узбекистан

Таблица С.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

Окончание таблицы С.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего государственного стандарта Республики Узбекистан
ISO/IEC 27010:2012 Информационная технология. Методы обеспечения безопасности. Менеджмент обеспечения защиты информации между секторами и организациями	MOD	O‘z DSt ISO/IEC 27010:2015 Информационная технология. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью при коммуникациях между отраслями и между организациями
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 27035-2:2016 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Часть 2. Руководящие указания по планированию и разработке реагирования на инциденты	MOD	O‘z DSt 3387:2019 (ISO/IEC 27035-2:2016, MOD) Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2. Руководящие указания для планирования и подготовки к реагирова-
ISO/IEC 27037:2012 Информационные технологии. Методы обеспечения безопасности. Руководящие указания по идентификации, сбору, получению и сохранению цифровых данных	MOD	O‘z DSt ISO/IEC 27037:2017 Информационная технология. Методы обеспечения безопасности. Руководящие указания по идентификации, сбору, получению и сохранению цифровых доказательств

Окончание таблицы D.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего государственного стандарта Республики Узбекистан
ISO/IEC 27040:2015 Информационные технологии. Методы обеспечения безопасности. Безопасность хранения данных	MOD	O‘z DSt ISO/IEC 27040:2018 Информационная технология. Методы обеспечения безопасности. Безопасность хранения данных
ISO/IEC 27041:2015 Информационные технологии. Методы защиты. Руководство по обеспечению приемлемости и адекватности методов расследования	MOD	O‘z DSt 3361:2019 (ISO/IEC 27041:2015, MOD) Информационная технология. Методы обеспечения безопасности. Руководство по обеспечению пригодности и адекватности методов расследования
Примечание - MOD - модифицированная степень соответствия государственного стандарта Республики Узбекистан международному стандарту.		

Приложение D
(справочное)

Технические отклонения и объяснение причин их внесения

D.1 Наименование стандарта изменено в целях унификации согласно государственным стандартам по информационной безопасности.

D.2 По всему тексту слова «этот международный стандарт» заменены на «настоящий стандарт».

D.3 Стандарт оформлен с учетом требований O‘z DSt 1.6:2003.

D.4 В стандарт включены отдельные изменения и дополнения. Перечень внесенных модификаций и объяснение причин их внесения приведены в таблице D.1.

Таблица D.1

Раздел, пункт настоящего стандарта	Модификация	Объяснение
Предисловие	Исключено	В связи с тем, что содержит информацию только о разработке международного стандарта
Введение	Исключены ссылки на стандарты ISO/IEC 29147 и ISO/IEC 30111	В связи с тем, что носят информационно-справочный характер
Раздел 2	Международные стандарты заменены на соответствующие им государственные стандарты	В настоящее время действуют государственные стандарты в соответствии с приложением С
	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 27010 O‘z DSt ISO/IEC 27031	Перенесены из раздела «Библиография» в соответствии с приложением С. Ссылки по тексту стандарта на данные международные стандарты заменены соответствующими ссылками на государственные стандарты
Раздел 3	Исключена ссылка на стандарт ISO/IEC 27042	В связи с тем, что термин и его определение приводится в тексте настоящего стандарта

Окончание таблицы D.1

Раздел, пункт настоящего стандарта	Модификация	Объяснение
Приложение A	Исключено	В связи с тем, что содержит текст информационного характера, не относящийся к области применения настоящего стандарта
Приложение C	Дополнительно включены в текст стандарта	Приведены сведения о соответствии ссылочных международных стандартов государственным стандартам Республики Узбекистан
Приложение D		Содержит перечень технических отклонений и объяснение причин их внесения
Библиография	Исключена	Ссылки [1], [4], [5], [9] - [11], [13] исключены в связи с отсутствием ссылок на них в тексте оригинала международного стандарта
		Ссылки [2], [3], [6] - [8], [12], [14] исключены в связи с тем, что международные стандарты заменены на государственные стандарты в соответствии с приложением C и перенесены в раздел 2
		Ссылки [15] - [18] исключены в связи с исключением ссылок на них в тексте настоящего стандарта

ОКС 35.040

Ключевые слова: информационная безопасность, инцидент информационной безопасности, группа по реагированию на инциденты информационной безопасности, планирование, подготовка, выявление, отчетность, оценка, принятие решений, ответное реагирование, 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
№