Тема 1 Организация безопасного удаленного доступа

Лекция 4. Мониторинг инцидентов информационной безопасности

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

Учебные вопросы и цели занятия:

1. Инциденты информационной безопасности.
2. Общие принципы управления компьютерными инцидентами
3. Обнаружение событий ИБ и инцидентов ИБ

Вступительная часть

Обеспечение безопасности проходящего сетевого трафика и внимательное изучение входящего трафика являются критически важными аспектами сетевой безопасности. Защита граничного маршрутизатора, который подключается к внешней сети, – это важный первый шаг в обеспечении безопасности сети.

Защищая сеть, не менее важно защищать сами устройства. Это включает использование интерфейса командной строки Cisco IOS для внедрения проверенных способов физической защиты маршрутизатора и защиты административного доступа к маршрутизатору. Большинство сервисов маршрутизаторов включены по умолчанию. Некоторые из этих функций были включены изначально, но сейчас уже не нужны. На данном занятии рассматриваются несколько из этих сервисов, а также режим One-Step Lockdown команды auto secure, который может использоваться для автоматизации задач по защите устройств.

Аутентификация протокола маршрутизации – это обязательный лучший способ предотвращения спуфинга протокола маршрутизации. В этой главе мы также остановимся на аутентификации конфигурирования открытого протокола кратчайшего пути (Open Shortest Path First, OSPF) с шифрованием Message Digest 5 (MD5) и Secure Hash Algorithm (SHA). Плоскости управления, менеджмента и данных рассматриваются с точки зрения использования ограничения плоскости управления (Control Plane Policing, CoPP).

Первый учебный вопрос.
Инциденты информационной безопасности

Ни одна самая совершенная мера по снижению рисков ИБ не может полностью предотвратить возникновение в информационной среде событий, потенциально несущих угрозу деятельности организации. Сложность и разнообразие среды деятельности предопределяют наличие остаточных рисков ИБ вне зависимости от качества подготовки и внедрения мер противодействия. Также всегда существует вероятность реализации новых, не известных до настоящего времени, угроз ИБ. Неготовность организации к обработке подобного рода ситуаций может существенно затруднить восстановление нормального функционирования и потенциально усилить нанесенный ущерб от реализации инцидентов ИБ, оказывающих прямое или косвенное негативное воздействие на ее деятельность.

Первый учебный вопрос. Инциденты информационной безопасности

Таким образом, любой организации, серьезно относящейся к вопросам ОИБ, необходимо реализовать комплексный подход для решения следующих задач:

обнаружения, оповещения и учета инцидентов ИБ;

реагирования на инциденты ИБ, включая применение необходимых средств для предотвращения и уменьшения последствий и/или восстановления после нанесенного ущерба;

анализа и расследования произошедших инцидентов ИБ с целью извлечения уроков из них, планирования превентивных защитных мер и улучшения процесса управления инцидентами ИБ.

Решение всех этих задач можно получить, разработав и реализовав эффективный процесс управления инцидентами ИБ. Обобщенно рассматриваемые стандарты вводят определение события ИБ как идентифицированное появление определенного состояния актива организации (системы, сервиса или сети), указывающего на возможное нарушение ПБ или в работе средств защиты либо возникновение ранее неизвестной ситуации, которая может иметь отношение к ИБ.

Во-первых, для того чтобы событие ИБ имело место, необходимо, чтобы субъектом (или агентом) было совершено действие, направленное на какой-либо объект.

Во-вторых, данное определение события ИБ не делает различия между авторизованными и неавторизованными действиями. Обнаруживаемые события ИБ могут быть частью инцидента ИБ или иметь отношение к ИБ.

Первый учебный вопрос. Инциденты информационной безопасности

Иногда возникающие события ИБ являются частью шагов, предпринимаемых злоумышленником для получения какого-то несанкционированного ПБ организации результата. Эти события ИБ можно рассматривать как часть инцидента ИБ, а сам инцидент ИБ – как совокупность событий ИБ.

Инцидент ИБ – появление одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации операций деятельности и указывающих на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ для активов организации.

Первый учебный вопрос.
Инциденты информационной безопасности

Инциденты ИБ могут быть преднамеренными или случайными (например, являться следствием ошибки человека, неправильного функционирования технических средств или природных явлений) и могут вызываться различными источниками угроз ИБ. Их послед ствиями могут быть несанкционированные изменения информации, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение. Приведем примеры некоторых распространенных инцидентов ИБ:

Первый учебный вопрос.
Инциденты информационной безопасности

1. Отказ в обслуживании (denial of service, DoS) является достаточно большой категорией инцидентов ИБ, приводящих к сбоям в системах, сервисах или сетях, которые не могут продолжать работу с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям. Существует два основных типа таких инцидентов ИБ: уничтожение ресурсов и истощение ресурсов. Одни технические инциденты "отказ в обслуживании" могут со зодаваться случайно, например в результате ошибки в конфигурации, допущенной оператором, или из-за несовместимости прикладного ПО, а другие – преднамеренно.

1. Отказ в обслуживании (denial of service, DoS)

Типичными примерами таких преднамеренных инцидентов являются следующие:

- зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;
- передача данных в некорректном формате в систему, сервис или сеть в попытке нарушить нормальную работу;
- дновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать ее ресурсы (за медлить их работу, блокировать или разрушить).

1. Отказ в обслуживании (denial of service, DoS)

Цель намеренно инициируемых инцидентов "отказ в обслуживании" – разрушить систему или сервис, снизить производительность сети. Другие инциденты являются лишь побочными продуктами иной вредоносной деятельности. Например, некоторые наиболее распространенные методы скрытого сканирования и идентификации могут приводить к полному разрушению старых или ошибочно сконфигурированных систем или сервисов при их сканировании. Многие преднамеренные инциденты "отказ в обслуживании" часто выполняются анонимно (источник атаки неизвестен), поскольку злоумышленник обычно не получает какую-либо информацию от атакуемой сети или системы.

1. Отказ в обслуживании (denial of service, DoS)

Инциденты "отказ в обслуживании", создаваемые нетехническими средствами и приводящие к потере информации, сервиса и/или устройств обработки, могут вызываться следующими факторами:

- нарушениями систем физической защиты, приводящими к хищениям, преднамеренному нанесению ущерба или разрушению оборудования;
- случайным нанесением ущерба аппаратуре;
- экстремальными условиями окружающей среды, например высокой температурой (выход из строя кондиционера);
- неправильным функционированием или перегрузкой системы;
- неконтролируемыми изменениями в системе;
- неправильным функционированием аппаратного обеспечения и ПО.

2. **Сбор информации** включает действия, связанные с определением потенциальных целей атаки и получением представления о запущенных сервисах. Инциденты такого типа предполагают проведение разведки с целью определения:

наличия цели, представления об окружающей ее сетевой топологии и о том, с кем обычно эта цель связана для обмена информацией;

потенциальных уязвимостей цели или непосредственно окружающей ее сетевой среды, которые можно использовать для атаки.

2. **Сбор информации**

Типичными примерами атак, направленных на сбор информации техническими средствами, являются следующие:

- сбрасывание записей DNS (системы доменных имен) для целевого домена Интернета (передача зоны DNS);
- отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;
- зондирование системы с целью идентификации (например, по контрольной сумме файлов) операционной системы хоста;
- сканирование доступных сетевых портов на протокол пере дачи файлов системе с целью идентификации соответствующих сервисов (например, электронная почта, FTP, Web и т. д.) и версий ПО этих сервисов;
- сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов (горизонтальное сканирование).

2. **Сбор информации**

В некоторых случаях технический сбор информации расширяется до несанкционированного доступа (НСД), если, например, злоумышленник, отыскивая уязвимости, пытается также получить НСД. Обычно это осуществляется автоматическими средствами взлома, которые не только ищут уязвимости, но и пытаются использовать уязвимые системы, сервисы и/или сети.

2. **Сбор информации**

Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, приводят:

- к прямому или косвенному раскрытию или модификации информации;
- хищению интеллектуальной собственности, хранимой в электронной форме;
- нарушению учетности, например при регистрации учетных записей;
- неправильному использованию ИС (нарушение закона или политики организации).

Инциденты могут вызываться таким образом:

нарушениями физической защиты, приводящими к НСД к информации и хищению устройств хранения данных (например, ключи шифрования);

неудачно и/или неправильно сконфигурированными ОС по причине неконтролируемых системных изменений в системе или не правильного функционирования ПО или АО, приводящих к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

3. НСД включает инциденты, которые не вошли в первые две категории: несанкционированные попытки доступа в систему или неправильное использование системы, сервиса или сети. Некоторые примеры НСД с помощью технических средств включают в себя:

- попытки извлечь файлы, содержащие пароли;
- атаки переполнения буфера с целью получения привилегированного (например, на уровне системного администратора) доступа к сети;
- использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;
- попытки повысить привилегии доступа к ресурсам или ин формации по сравнению с теми, которые пользователь или администратор уже имеют легитимно.

3. НСД

Инциденты НСД, создаваемые нетехническими средствами, которые приводят к прямому или косвенному раскрытию или модификации информации, к нарушениям учетности или неправильному использованию ИС, могут вызываться следующими факторами:

- разрушением физической защиты с последующим НСД к информации;
- неудачно и/или неправильно сконфигурированной ОС вследствие неконтролируемых изменений в системе или неправильного функционирования ПО или АО, приводящих к результатам, подобным тем, которые описаны выше.

Первый учебный вопрос.
Инциденты информационной безопасности

Управление инцидентами ИБ – процесс, на вход которого подаются данные, полученные в результате сбора и протоколирования затрагивающих ИС событий ИБ, а на выход поступает информация о причинах произошедшего инцидента ИБ, нанесенном организации ущербе и мерах, которые необходимо принять для того, чтобы инцидент ИБ не повторился вновь. Таким образом, управление инцидентами ИБ направлено на совершенствование СОИБ организации. Кроме того, получаемые на выходе данные являются, по сути, единственным объективным источником определения вероятности реализации угроз ИБ при анализе рисков ИБ.

Первый учебный вопрос.
Инциденты информационной безопасности

Управление инцидентами ИБ – процесс, на вход которого подаются данные, полученные в результате сбора и протоколирования затрагивающих ИС событий ИБ, а на выход поступает информация о причинах произошедшего инцидента ИБ, нанесенном организации ущербе и мерах, которые необходимо принять для того, чтобы инцидент ИБ не повторился вновь. Таким образом, управление инцидентами ИБ направлено на совершенствование СОИБ организации. Кроме того, получаемые на выходе данные являются, по сути, единственным объективным источником определения вероятности реализации угроз ИБ при анализе рисков ИБ.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Для обнаружения компьютерных инцидентов используют результаты проводимого в организации мониторинга информационной безопасности, в рамках которого осуществляется сбор информации о событиях безопасности и иных данных мониторинга, необходимых для поиска признаков возможного возникновения компьютерных инцидентов. Такие признаки представляют собой совокупность зарегистрированных событий безопасности и иных данных мониторинга, а также условий, при которых такая совокупность зарегистрированных событий безопасности и иных данных мониторинга может свидетельствовать о возможном возникновении компьютерного инцидента. Для сбора событий безопасности и иных данных мониторинга и последующего поиска признаков возможного возникновения компьютерных инцидентов, как правило, применяют средства управления событиями информационной безопасности.

Такие средства позволяют осуществлять сбор, нормализацию, агрегацию событий безопасности и иных данных мониторинга и на основании настроенных правил (далее – правила регистрации признаков возможного возникновения компьютерных инцидентов) проводить автоматизированный анализ и корреляцию событий без опасности и иных данных мониторинга. Понятие "признак возможного возникновения компьютерных инцидентов" применяют в связи с тем, что средства управления событиями информационной безопасности фиксируют возникновение ситуации, которая может свидетельствовать о возникновении компьютерного инцидента, а не сам факт его возникновения.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Некоторые данные мониторинга используют только как аналитические при формировании правил регистрации признаков возможного возникновения компьютерных инцидентов. К таковым могут относиться данные об индикаторах компрометации, на основе которых возможно сформировать новое правило, предусматривающее анализ событий безопасности, ранее не использовавшихся в правилах регистрации признаков возможного возникновения компьютерных инцидентов. Другие данные мониторинга, в первую очередь данные о зарегистрированных событиях безопасности, используют непосредственно для обнаружения и регистрации компьютерных инцидентов как условия для правил регистрации признаков возможного возникновения компьютерных инцидентов.

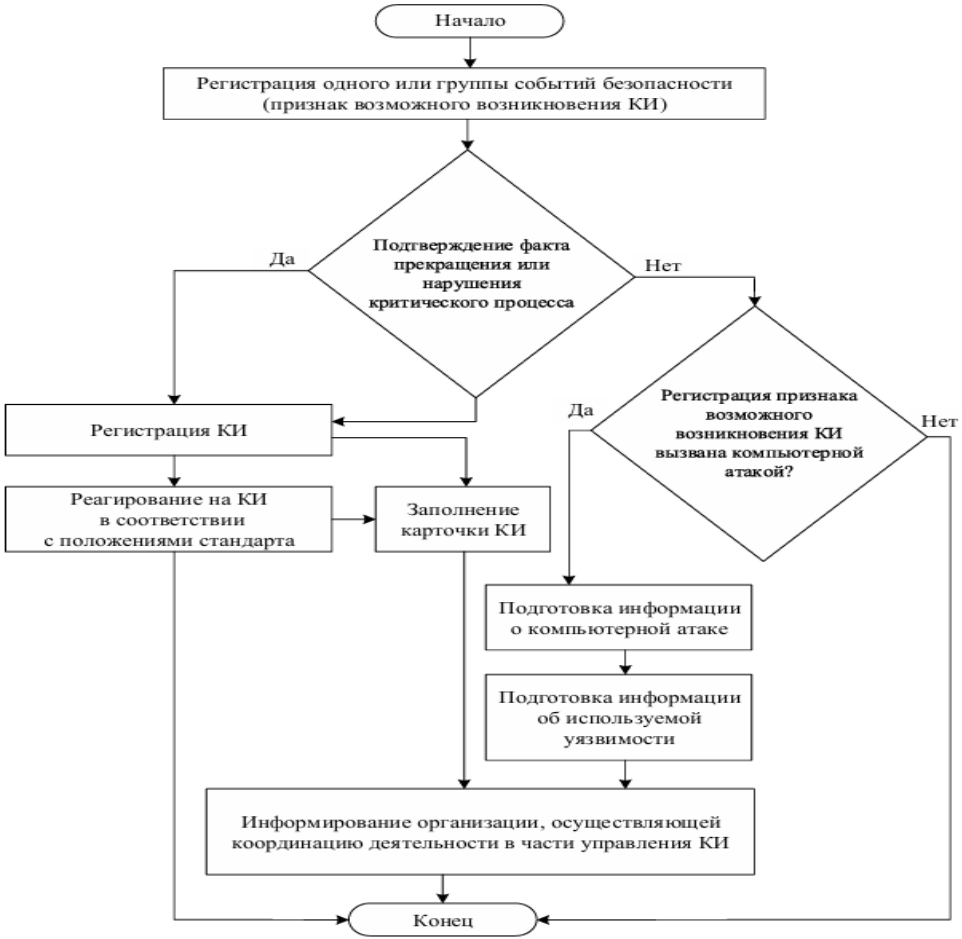
Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Для всех зарегистрированных признаков возможного возникновения компьютерных инцидентов необходимо проводить проверку факта их возникновения. Если в ходе проверки подтверждается факт возникновения компьютерного инцидента, то должна осуществляться его регистрация. Если в ходе проверки не может быть однозначно подтверждено отсутствие факта возникновения компьютерного инцидента, то также осуществляется его регистрация. При этом в ходе реагирования на компьютерный инцидент факт его возникновения может быть не подтвержден, что может являться основанием для его закрытия.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

На рисунке представлен общий подход к обнаружению и регистрации компьютерных инцидентов, реагированию на них и информированию организации, осуществляющей координацию деятельности в части управления компьютерными инцидентами. К компьютерным относятся инциденты, характеризующиеся наличием факта нарушения и (или) прекращения функционирования информационных ресурсов субъектов ГосСОПКА, сети электросвязи, используемой для организации взаимодействия информационных ресурсов, и (или) нарушения безопасности обрабатываемой в информационном ресурсе субъектов ГосСОПКА информации, необходимой для обеспечения критических процессов (ее конфиденциальности, целостности или доступности), в том числе произошедших в результате компьютерной атаки. При этом под прекращением или нарушением функционирования информационных ресурсов понимают приведение информационного ресурса в состояние, при котором он полностью или частично не может обрабатывать информацию, необходимую для обеспечения критических процессов, и (или) осуществлять управление, контроль или мониторинг критических процессов.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами



Общий подход к управлению компьютерными инцидентами

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Субъекты ГосСОПКА, являющиеся субъектами критической информационной инфраструктуры, определяют критические процессы в соответствии с законодательством Российской Федерации. Иные субъекты ГосСОПКА определяют критические процессы установленным в организации порядком. Для эффективного ведения деятельности по управлению компьютерными инцидентами в организации должны быть использованы не только средства управления событиями информационной безопасности, но и средства управления инцидентами, а также специализированные средства, предназначенные для обмена информацией о компьютерных атаках, компьютерных инцидентах и уязвимостях (средства обмена информацией).

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Средства управления инцидентами должны обеспечивать автоматизацию процесса реагирования на компьютерные инциденты. Средства обмена информацией следует использовать для взаимодействия с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами, и с иными внешними организациями. Обмен информацией и взаимодействие с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами, и с иными внешними организациями значительно повышают эффективность управления компьютерными инцидентами, так как в некоторых случаях компьютерные инциденты не могут быть разрешены организацией самостоятельно (собственными силами) или могут выходить за пределы зоны ответственности одной организации.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Использование структурированного подхода к управлению компьютерными инцидентами направлено на достижение следующих целей:

А. Повышение эффективности реагирования на компьютерные инциденты. Повышению эффективности реагирования на компьютерные инциденты способствуют планирование и распределение ресурсов подразделений организации, участвующих в деятельности по управлению компьютерными инцидентами, а также возможность совместного использования информации о зарегистрированных компьютерных инцидентах специалистами подразделения, ответственного за управление компьютерными инцидентами, специалистами смежных подразделений, участвующих в деятельности по управлению компьютерными инцидентами, а также организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Кроме того, управление компьютерными инцидентами предусматривает определение очередности реагирования на компьютерные инциденты с учетом их приоритетов и уровней влияния. Реагирование на компьютерные инциденты с учетом их приоритетов и уровней влияния позволяет исключить ситуации, в которых действия по реагированию проводят в режиме "быстрой реакции", когда компьютерные инциденты отрабатываются в порядке их регистрации, что может при вести к несвоевременному реагированию на инциденты, оказывающие наибольшее негативное влияние на информационные ресурсы.

Б. Снижение негативного воздействия на процессы организации. Деятельность по управлению компьютерными инцидентами в первую очередь направлена на снижение уровня потенциальных негативных последствий от компьютерных инцидентов для процессов, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям в сфере обеспечения обороны страны, безопасности государства и правопорядка, финансовым потерям или долгосрочным убыткам, возникающим из-за испорченной репутации и потери доверия к организации.

В. Предотвращение компьютерных инцидентов. Анализ данных, связанных с компьютерными инцидентами, проводимый в рамках деятельности по управлению компьютерными инцидентами, направлен на выявление закономерностей и тенденций произошедших ранее компьютерных инцидентов, информация о которых может быть использована для приобретения и накопления опыта, а также при разработке рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов с целью предотвращения их повторного возникновения.

Г. Обеспечение повышения осведомленности (информирования) в области управления компьютерными инцидентами. Деятельность по управлению компьютерными инцидентами предусматривает информирование специалистов, участвующих в управлении компьютерными инцидентами, с учетом полученного опыта.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Стадии управления компьютерными инцидентами

Структурированный подход к организации и ведению деятельности по управлению компьютерными инцидентами включает в себя четыре стадии:

- организация деятельности по управлению компьютерными инцидентами;
- обнаружение и регистрация компьютерных инцидентов;
- реагирование на компьютерные инциденты (включая фиксацию материалов, связанных с возникновением компьютерных инцидентов и установление причин и условий возникновения компьютерных инцидентов);
- анализ результатов деятельности по управлению компьютерными инцидентами.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Стадии управления компьютерными инцидентами

Стандарты [23–25] охватывают различные стадии управления компьютерными инцидентами:

1) [23] – все четыре стадии;
2) [24] – стадию организации деятельности по управлению компьютерными инцидентами;
3) [25] – стадии:

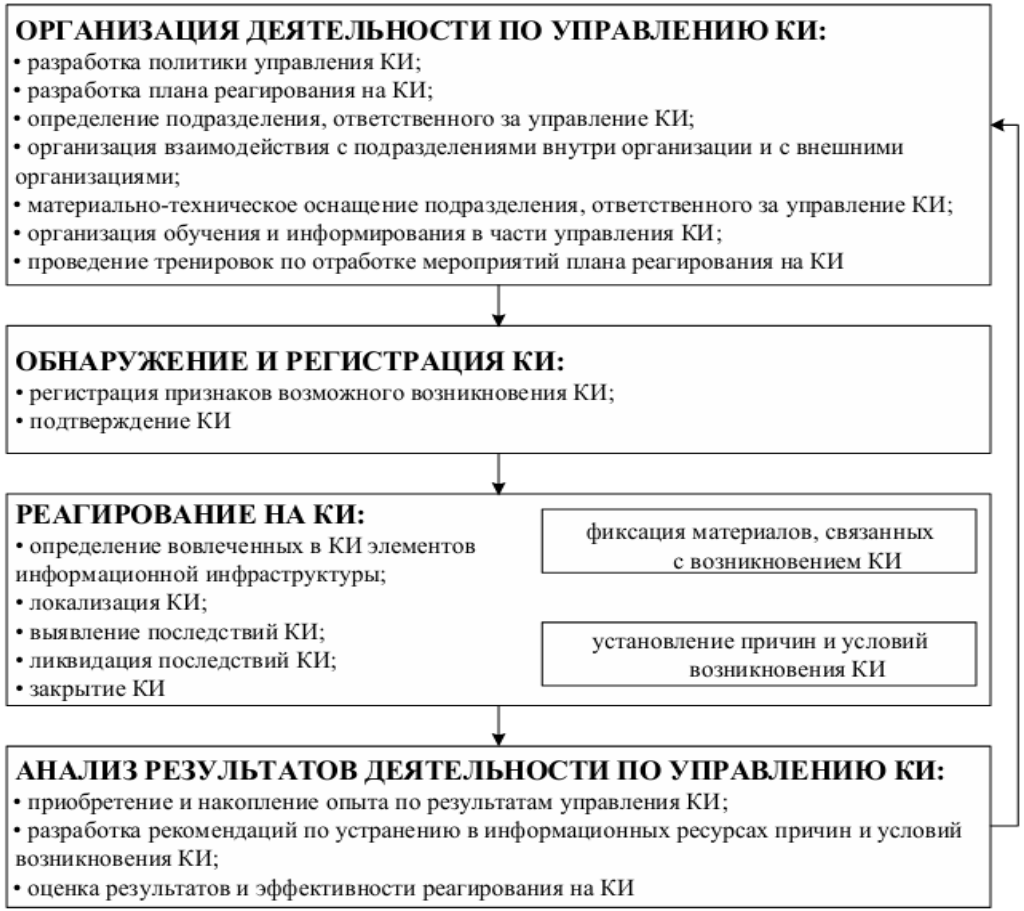
а) обнаружения и регистрации компьютерных инцидентов;

б) реагирования на компьютерные инциденты;

в) анализа результатов деятельности по управлению компьютерными инцидентами.

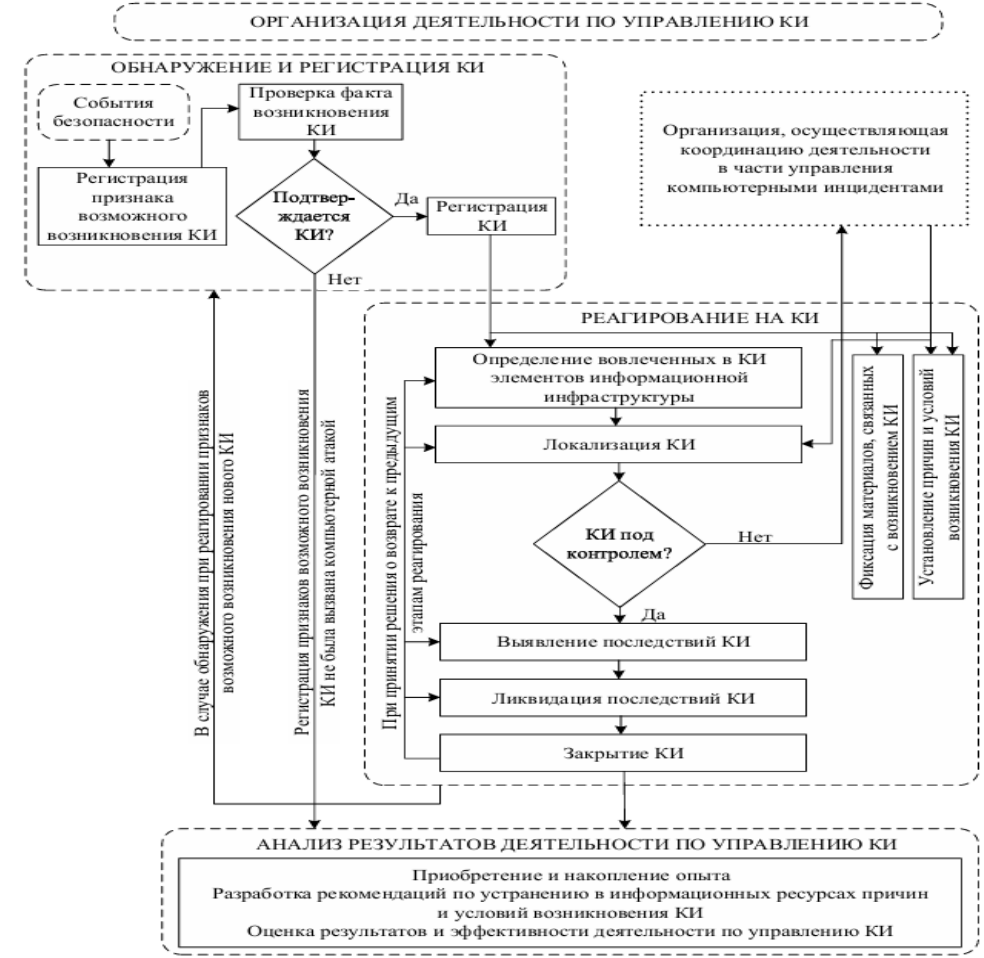
23. ГОСТ Р 59709–2022. Национальный стандарт Российской Федера ции. Защита информации. Управление компьютерными инцидентами. Термины и определения
24. ГОСТ Р 59710–2022. Национальный стандарт Российской Федера ции. Защита информации. Управление компьютерными инцидентами. Общие положения
25. ГОСТ Р 59711–2022. Национальный стандарт Российской Федера ции. Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами



Стадии управления компьютерными инцидентами

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами



Общий порядок ведения деятельности по управлению компьютерными инцидентами

Организация деятельности по управлению компьютерными инцидентами

Эффективное управление компьютерными инцидентами требует соответствующего планирования и подготовки. Для осуществления деятельности по управлению компьютерными инцидентами организация должна выполнить следующие мероприятия:

- разработать политику управления компьютерными инцидентами;
- разработать план реагирования на компьютерные инциденты;
- определить подразделение, ответственное за управление компьютерными инцидентами;
- обеспечить взаимодействие с подразделениями внутри организации и с внешними организациями;
- реализовать материально-техническое оснащение подразделения, ответственного за управление компьютерными инцидентами;
- организовать обучение специалистов в части управления компьютерными инцидентами;
- провести тренировки по отработке мероприятий плана реагирования на компьютерные инциденты.

Обнаружение и регистрация компьютерных инцидентов

Деятельность по обнаружению и регистрации компьютерных инцидентов основывается на результатах проводимого в организации мониторинга, в рамках которого осуществляется сбор информации о событиях безопасности и иных данных из различных источников.

В состав собираемых данных помимо информации о зарегистрированных событиях безопасности, как правило, входят инвентаризационные данные, данные о сетевой активности, новостные ленты, касающиеся текущей политической, социальной или экономической деятельности (обстановки), которая может повлиять на активность, связанную с компьютерными инцидентами, информация о тенденциях, связанных с компьютерными инцидентами, о новых векторах атак и текущих индикаторах атак (индикаторах компрометации).

Обнаружение и регистрация компьютерных инцидентов

Стадия управления компьютерными инцидентами "обнаружение и регистрация компьютерных инцидентов " состоит из двух последовательных этапов:

- регистрация признаков возможного возникновения компьютерных инцидентов;
- подтверждение компьютерных инцидентов.

Регистрация признаков возможного возникновения компьютерных инцидентов осуществляется как неавтоматизированным способом (специалистами подразделения, ответственного за управление компьютерными инцидентами, при самостоятельном анализе событий безопасности в ходе мониторинга или при получении соответствующей информации от работников организации), так и автоматизированным способом (с использованием средства управления событиями информационной безопасности) на основе правил регистрации признаков возможного возникновения компьютерных инцидентов.

Обнаружение и регистрация компьютерных инцидентов

При автоматизированном способе регистрации признака возможного возникновения компьютерных инцидентов информация о данном зарегистрированном признаке передается из средства управления событиями информационной безопасности в средство управления инцидентами, где автоматически формируется карточка признака возможного возникновения компьютерного инцидента. При неавтоматизированном способе регистрации признака возможного возникновения компьютерных инцидентов специалист подразделения, ответственного за управление компьютерными инцидентами, самостоятельно регистрирует данный признак в средстве управления инцидентами (заполняет карточку признака возможного возникновения компьютерного инцидента).

Обнаружение и регистрация компьютерных инцидентов

На этапе подтверждения компьютерных инцидентов проводится оценка информации, связанной с событиями безопасности, на основании которых был зарегистрирован признак возможного возникновения компьютерных инцидентов, для определения характера влияния на информационные ресурсы с целью принятия решения о регистрации компьютерного инцидента. При необходимости осуществляются сбор и внесение дополнительной информации. В случае подтверждения компьютерный инцидент регистрируется и создается карточка компьютерного инцидента.

Реагирование на компьютерные инциденты

Реагирование на компьютерные инциденты осуществляют специалисты подразделения, ответственного за управление компьютерными инцидентами, и специалисты смежных подразделений, участвующих в деятельности по управлению компьютерными инцидентами, входящие в состав рабочих групп реагирования на компьютерные инциденты. В ходе реагирования на компьютерный инцидент должны быть выполнены нижеперечисленные действия.

1. Определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры. Крайне важно определить полное множество элементов информационной инфраструктуры, вовлеченных в компьютерный инцидент, и внести эту информацию в карточку компьютерного инцидента.

Реагирование на компьютерные инциденты

2. На этапе локализации компьютерного инцидента специалисты подразделения, ответственного за управление компьютерными инцидентами, должны определить, находится ли компьютерный инцидент под контролем. Если компьютерный инцидент находится под контролем, то выполняются последующие этапы реагирования. Если компьютерный инцидент не находится под контролем или ожидается, что он окажет серьезное воздействие на критические процессы организации (приведет к серьезным последствиям), целесообразно направить обращения в организацию, осуществляющую координацию деятельности в части управления компьютерными инцидентами, об оказании содействия в реагировании на компьютерный инцидент. Компьютерный инцидент считается находящимся под контролем, если удалось принять меры, которые позволили предотвратить вовлечение в инцидент новых элементов информационной инфраструктуры и увеличение масштаба негативных последствий.

Реагирование на компьютерные инциденты

3. На этапе выявления последствий компьютерного инцидента выполняются процедуры по выявлению признаков негативного воздействия компьютерного инцидента на информационные ресурсы.

4. На этапе ликвидации последствий компьютерных инцидентов выполняются процедуры по восстановлению штатного функционирования информационных ресурсов и обрабатываемой им информации.

Реагирование на компьютерные инциденты

5. На каждой стадии реагирования на компьютерные инциденты специалисты, ответственные за реагирование на компьютерные инциденты (руководители рабочих групп реагирования на компьютерные инциденты), должны осуществлять проверку качества и достаточности выполненных действий по реагированию на компьютерный инцидент и при необходимости создавать задания на доработку выполненных действий, а также принимать решение о возврате на предыдущий этап реагирования.

Специалисты, ответственные за реагирование на компьютерные инциденты (руководители рабочих групп реагирования на компьютерные инциденты), осуществляют следующую деятельность:

- проведение проверки фактов возникновения компьютерных инцидентов с целью их подтверждения;
- регистрация компьютерных инцидентов в случае их подтверждения;
- контроль выполнения этапов реагирования на компьютерные инциденты.

Реагирование на компьютерные инциденты

При осуществлении контроля выполнения этапов реагирования на компьютерные инциденты специалист, ответственный за реагирование на компьютерный инцидент (руководитель рабочей группы реагирования на компьютерные инциденты), должен принимать решение о необходимости привлечения организации, осуществляющей координацию деятельности в части управления компьютерными инцидентами. Параллельно с действиями по реагированию, и даже после реакции на компьютерный инцидент, может проводиться фиксация материалов, связанных с возникновением компьютерного инцидента, а также установление причин и условий возникновения компьютерного инцидента. Их выполнение не влияет на закрытие компьютерного инцидента.

Реагирование на компьютерные инциденты

Помимо перечисленных этапов реагирования организация должна решать следующие ключевые задачи:

- определение принципа очередности реагирования на компьютерные инциденты с учетом уровня их влияния и приоритетов;
- обеспечение документирования всех действий вовлеченных сторон и, в частности, специалистов по компьютерным инцидентам;
- безопасное хранение зафиксированных материалов, связанных с возникновением компьютерных инцидентов (цифровых свидетельств) для установления причин и условий их возникновения;
- информирование о возникновении компьютерного инцидента и обмен информацией с организацией, осуществляющей координацию деятельности в части управления компьютерными инцидентами.

Вся собранная информация, относящаяся к компьютерному инциденту, должна быть отражена в карточке компьютерного инцидента и быть максимально полной. Это позволяет качественно проводить анализ результатов деятельности по управлению компьютерными инцидентами.

Анализ результатов деятельности по управлению компьютерными инцидентами

Заключительная стадия управления компьютерными инцидентами осуществляется после того, как компьютерный инцидент был закрыт. Анализ результатов деятельности по управлению компьютерными инцидентами включает в себя следующие этапы:

- приобретение и накопление опыта по результатам управления компьютерными инцидентами;
- оценка результатов и эффективности реагирования на компьютерные инциденты.

Анализ результатов деятельности по управлению компьютерными инцидентами

На основе оценки результатов и эффективности реагирования на компьютерные инциденты осуществляется (при необходимости) доработка (актуализация) документации в части управления компьютерными инцидентами.

На стадии анализа результатов деятельности по управлению компьютерными инцидентами организация также должна решать следующие ключевые задачи:

- информирование и обмен результатами деятельности по управлению компьютерными инцидентами с заинтересованными организациями (при необходимости);
- определение состава информации о компьютерных инцидентах, связанных с ними векторах атак и уязвимостях, которая может быть передана организациям, с которыми осуществляется взаимодействие, в целях предотвращения возникновения таких же компьютерных инцидентов в их информационной инфраструктуре.

Анализ результатов деятельности по управлению компьютерными инцидентами

На основе оценки результатов и эффективности реагирования на компьютерные инциденты осуществляется (при необходимости) доработка (актуализация) документации в части управления компьютерными инцидентами.

На стадии анализа результатов деятельности по управлению компьютерными инцидентами организация также должна решать следующие ключевые задачи:

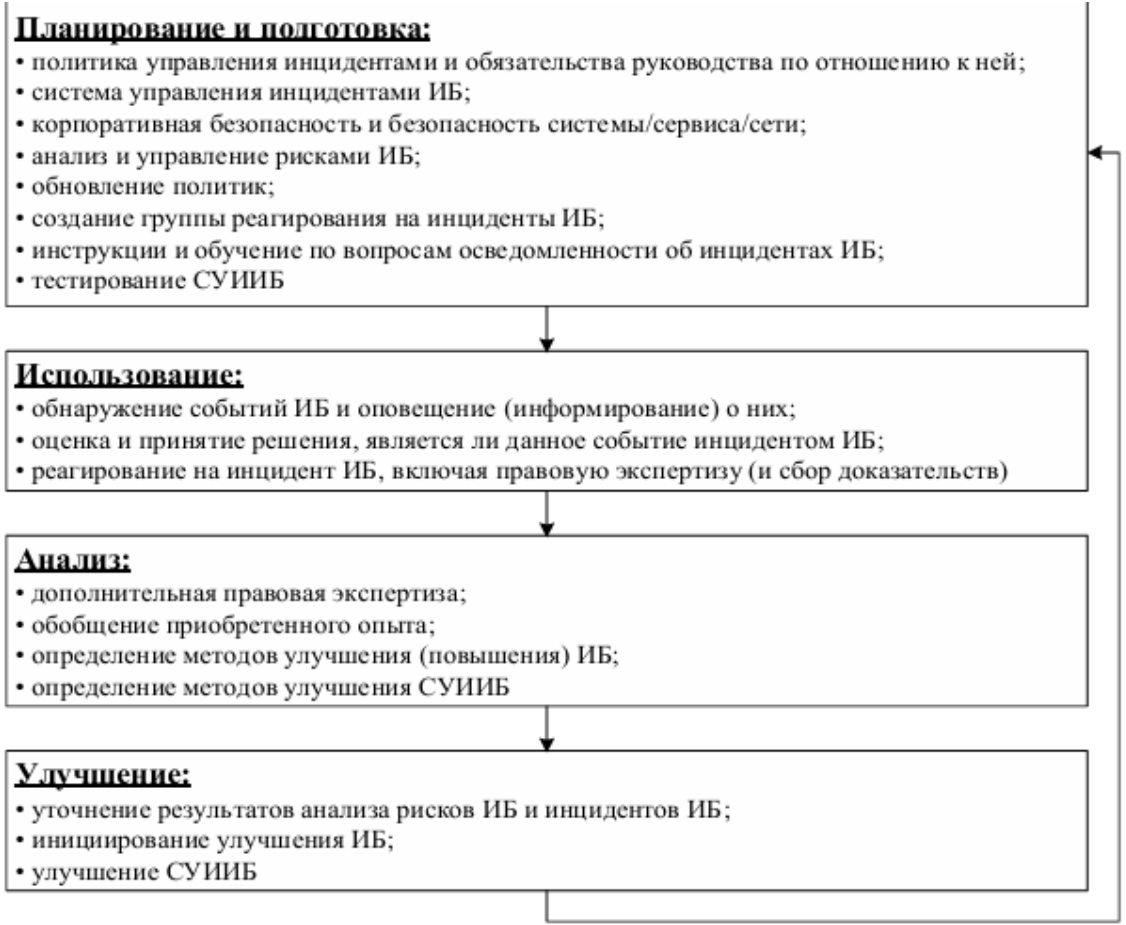
- информирование и обмен результатами деятельности по управлению компьютерными инцидентами с заинтересованными организациями (при необходимости);
- определение состава информации о компьютерных инцидентах, связанных с ними векторах атак и уязвимостях, которая может быть передана организациям, с которыми осуществляется взаимодействие, в целях предотвращения возникновения таких же компьютерных инцидентов в их информационной инфраструктуре.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами

Любая организация, использующая системный подход к управ лению инцидентами ИБ, построив и внедрив Систему управления инцидентами ИБ (СУИИБ) , в целом повышает устойчивость ее процессов деятельности и извлекает из этого значительные преимущества. Для достижения поставленных целей в соответствии с основными стандартами процесс управления инцидентами ИБ делится на четыре основных этапа:

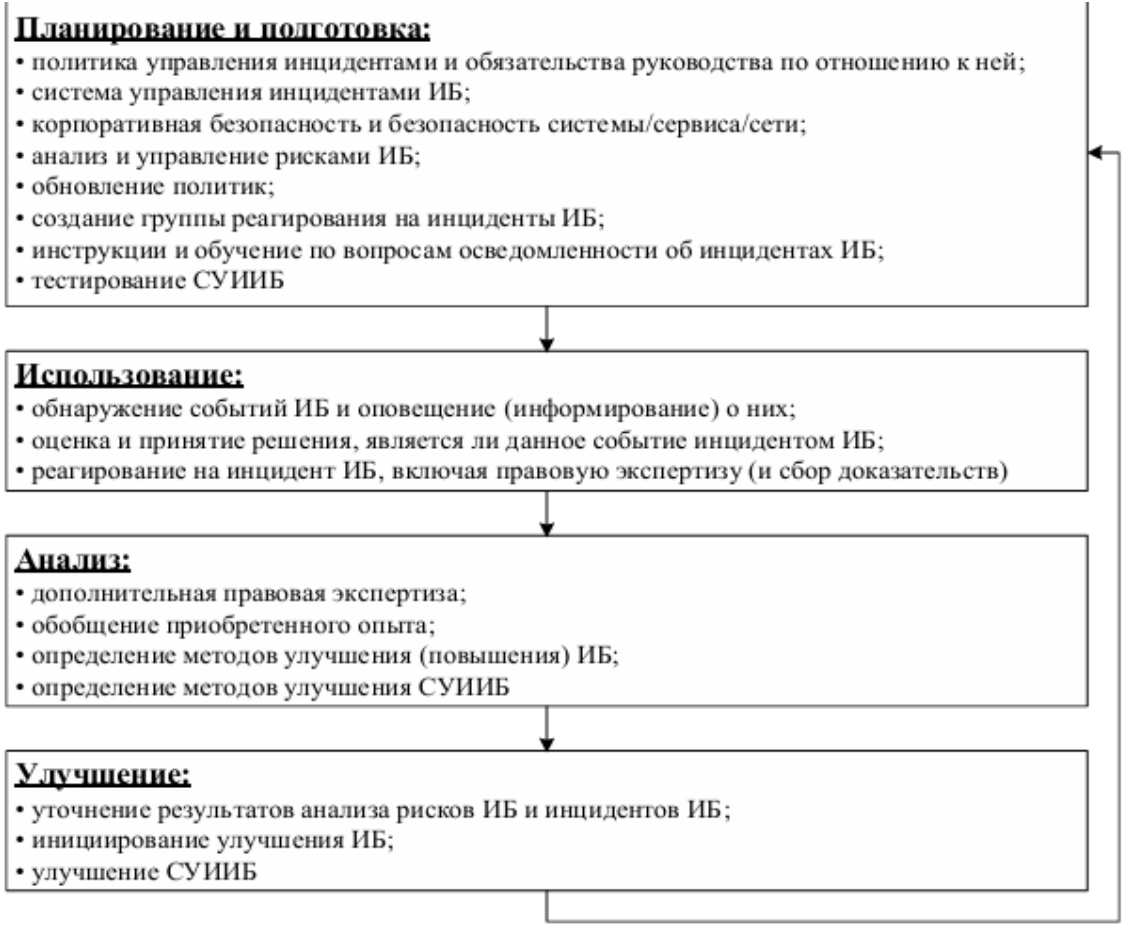
- планирование и подготовка,
- использование,
- анализ,
- улучшение.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами



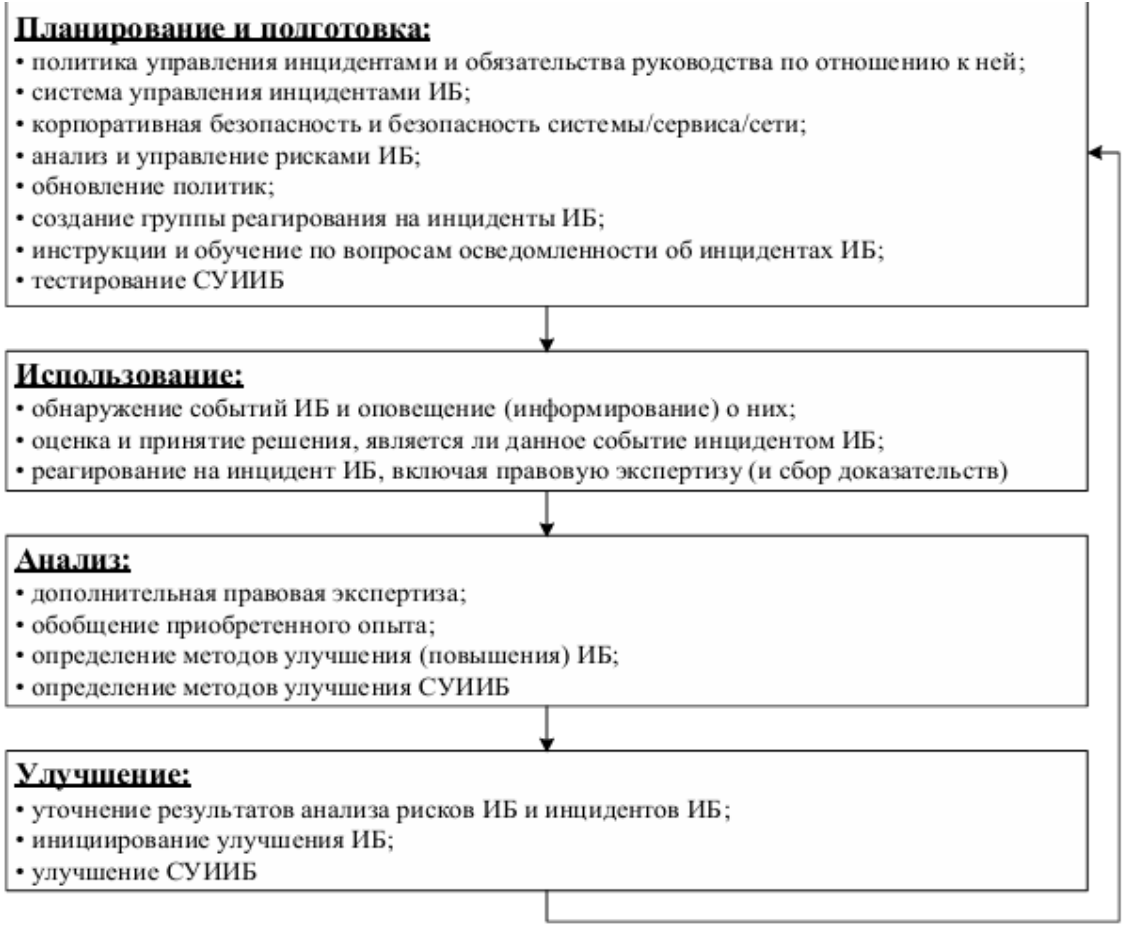
На этапе планирования и подготовки разрабатываются доку менты, регламентирующие процесс реагирования на инциденты ИБ, создается соответствующая организационная структура, выделяются людские и материальные ресурсы и проводится обучение персонала.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами



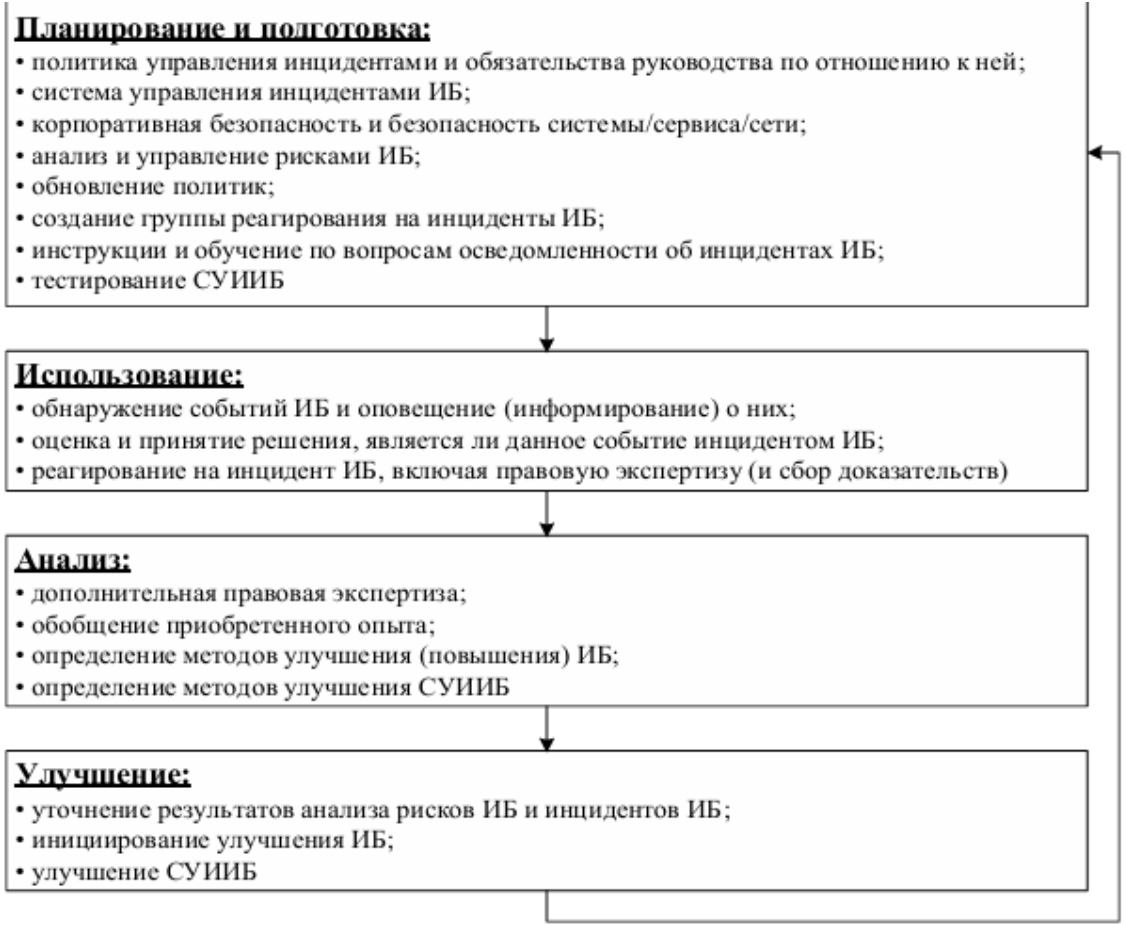
На этапе использования происходят обнаружение и оповещение о возникновении события ИБ, сбор информации о нем и его оценка, определяется, является ли данное событие инцидентом ИБ. Также происходят реагирование на инцидент ИБ и определение необходимости проведения расследования инцидента ИБ.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами



На третьем этапе проводятся анализ и расследование инцидента ИБ. На основе полученных результатов делаются выводы и составляются рекомендации по улучшению процессов ОИБ в целом и управления инцидентами ИБ в частности.

Второй учебный вопрос.
Общие принципы управления компьютерными инцидентами



На этапе улучшения (совершенствования) реализуются рекомендации, выработанные на этапе анализа.

Третий учебный вопрос.
Обнаружение событий ИБ и инцидентов ИБ

События ИБ обнаруживаются непосредственно лицом/лицами, заметившими что-либо, вызывающее беспокойство и имеющее технический, физический или процедурный характер. Обнаружение может осуществляться, например, детекторами огня/дыма или с по мощью охранной сигнализации путем передачи сигналов тревоги в заранее определенные места для дальнейшего осуществления человеком заранее спланированных действий. Технические события ИБ обнаруживаются автоматически, это могут быть сигналы тревоги, производимые средствами анализа записей журналов регистрации, МЭ, средствами обнаружения вторжений (СОВ), антивирусными программами.

Третий учебный вопрос.
Обнаружение событий ИБ и инцидентов ИБ

Разные категории пользователей осуществляют обнаружение инцидентов ИБ и событий ИБ разными способами. Так, специалисты подразделения ИБ могут обнаружить события ИБ и инциденты ИБ следующим образом:

- получая сообщения от средств защиты информации;
- изучая результаты проведения анализа защищенности активов организации с использованием инструментальных средств;
- анализируя журналы регистрации событий серверов, активного сетевого оборудования, прикладного ПО, БД и т. д.;
- просматривая данные систем видеонаблюдения и контроля доступа и т. д.

Сотрудники подразделений, ответственных за поддержание информационной инфраструктуры, обнаруживают инциденты ИБ путем осуществления регулярного мониторинга уязвимостей и угроз ИБ для ИС, за которые они ответственны. Основными источниками сведений для администраторов ИС являются:

- сайты и новостные рассылки производителей ПО;
- новостные сайты и рассылки третьих сторон;
- БД уязвимостей;
- сообщения о доступных обновлениях ПО;
- другие уведомления об уязвимостях, обновлениях или угрозах ИБ.

Третий учебный вопрос.
Обнаружение событий ИБ и инцидентов ИБ

Рядовые пользователи осуществляют обнаружение инцидентов ИБ посредством наблюдения за работой систем, сервисов и сетей, с которыми они работают, а также за работой других пользователей и служб организации. После того как инцидент ИБ (или событие ИБ, похожее на инцидент ИБ) был обнаружен, о нем сообщается по установленным каналам сотрудникам, ответственным за прием и обработку сообщений об инцидентах ИБ. Независимо от причины обнаружения события ИБ, лицо, заметившее нечто необычное или оповещенное автоматическими средствами, несет ответственность за инициирование процесса обнаружения и оповещения.

Обработка конкретного события ИБ зависит от того, что оно собой представляет, а также от последствий и воздействий, к которым это событие может привести. Принятие решения о способе обработки события ИБ для многих работников организации выходит за пределы их компетенции. Поэтому информирующий о событии ИБ сотрудник должен заполнить форму отчета таким образом, чтобы в ней было как можно больше информации, доступной ему в тот момент. При необходимости он связывается со своим руководителем. Желательно, чтобы форма отчета существовала в электронном виде (например, была прислана по электронной почте или представлена на веб-сайте организации) и ее можно было передать защищенным образом в надлежащую службу (работающую, по возможности, 24 ч в сутки, семь дней в неделю), а копию – руководителю ГРИИБ.

Обработка событий ИБ и инцидентов ИБ

Как отмечается в стандартах, обработка сообщений – важный элемент управления инцидентами ИБ, включающий в себя сортировку, определение типа события ИБ, типа и степени серьезности инцидента ИБ (если событие ИБ признается таковым) и т. д. Именно посредством эффективной реализации данного процесса можно понять, что именно происходит в организации и своевременно оценить потенциальное воздействие события ИБ на деятельность организации.

Обработка событий ИБ и инцидентов ИБ

Ответственный сотрудник, принявший сообщение о событии ИБ, производит его первоначальную оценку и определяет, является ли оно сообщением о событии ИБ, или об инциденте ИБ, или об уязвимости либо не относится к ИБ вовсе. Оценка производится на основе полученных сведений о событии ИБ, экспертного мнения принявшего сообщение специалиста и принятых в организации классификации инцидентов ИБ и шкалы их серьезности. Обычно инциденты ИБ делятся по типам, например, инциденты физической безопасности, программно-технические и т. д. Помимо этого, вводится классификация по степени серьезности, чтобы прежде всего оценить общую ситуацию, а также определить временные рамки и приоритеты реагирования на инциденты ИБ.

Обработка событий ИБ и инцидентов ИБ

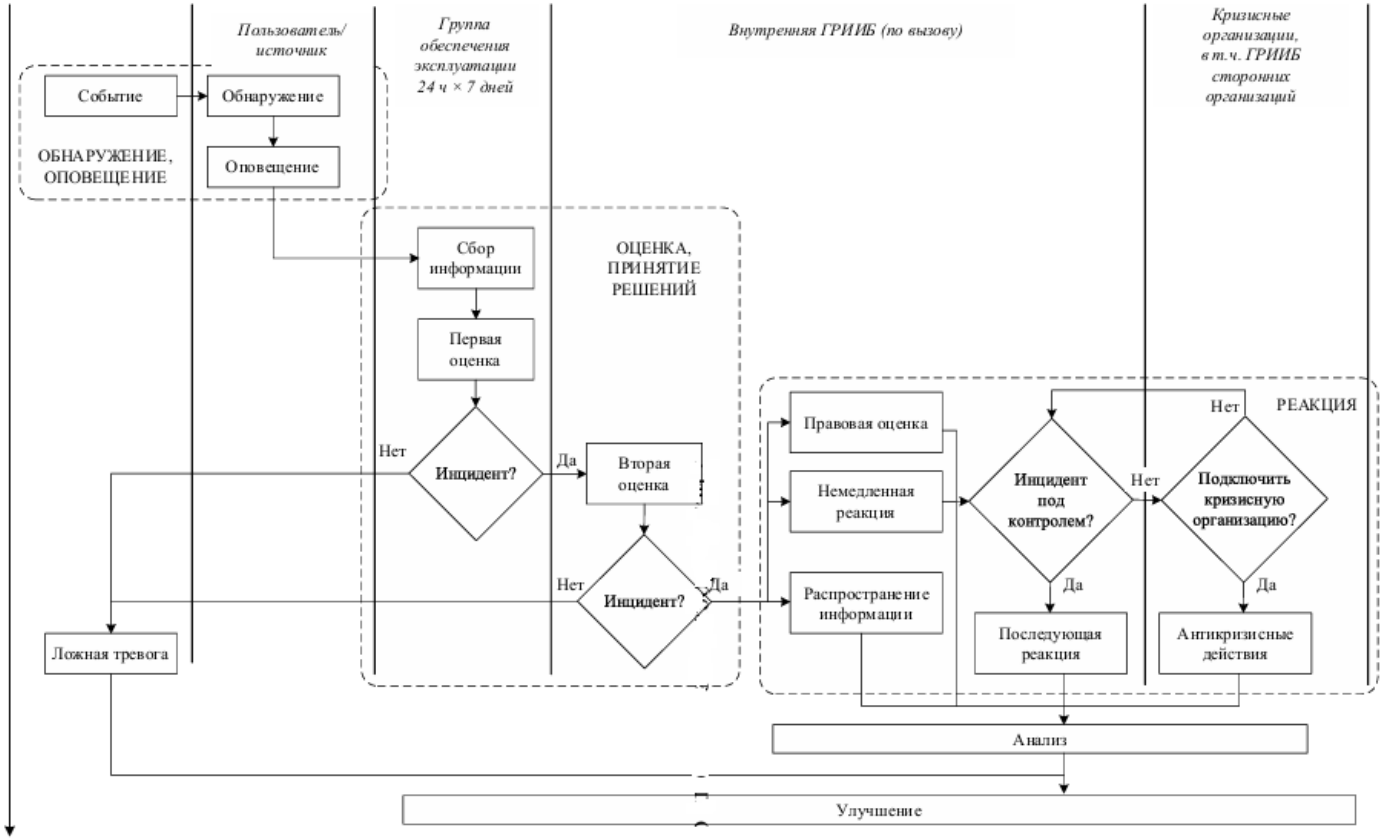
Если полученная информация не является событием ИБ, регистрирующий данное сообщение сотрудник, исходя из анализа сообщения, передает эту информацию на вход других процессов управления, которые кажутся ему наиболее подходящими.

Если полученная информация является просто событием ИБ (а не инцидентом ИБ), регистрирующий данное сообщение сотрудник фиксирует его в надлежащем виде. Тогда дальнейшая работа по событию ИБ в рамках процесса управления инцидентами ИБ не требуется.

Обработка событий ИБ и инцидентов ИБ

В случае отсутствия возможности возложить задачу приема и первичной обработки инцидентов ИБ на сотрудников подразделений ИБ для выполнения этой деятельности привлекаются сотрудники технической поддержки или даже те, кто не обладает глубокими знаниями в области ИБ. Однако тогда потребуется детальная проработка классификации инцидентов ИБ, а также разработка подробных памяток с примерами.

Третий учебный вопрос. Обнаружение событий ИБ и инцидентов ИБ



Последовательность операций обработки событий и инцидентов ИБ, реализуемых на этапе процесса управления инцидентами ИБ,

Первая оценка и предварительное решение по событию ИБ

Согласно разработанной в стандартах последовательности совершаемых в связи с обнаружением события ИБ действий, принимающее в группе обеспечения эксплуатации (ГОЭ) СУИИБ сообщения лицо подтверждает получение заполненной формы отчета, вводит ее в БДСИИБ и анализирует. Далее должностное лицо получает любые уточнения от сообщившего о событии ИБ и собирает другую требуемую дополнительную доступную информацию как от сообщившего о событии, так и из любого другого источника. Затем представитель ГОЭ проводит оценку для определения, подходит ли это событие под категорию инцидента ИБ или является ложным. Если событие ИБ определяется как ложное, форма отчета заполняется и передается ГРИИБ для записи в БД и дальнейшего анализа.

Первая оценка и предварительное решение по событию ИБ

Собранные на этом этапе информация и другие свидетельства могут потребоваться в будущем при дисциплинарном или судебном разбирательстве. Лицо/лица, выполняющие задачи сбора и оценки информации, должны хорошо знать требования к сбору и сохранению свидетельств инцидентов ИБ. Если событие ИБ определено как вероятный инцидент ИБ, а сотрудник ГОЭ имеет соответствующий уровень компетентности, то проводится его дальнейшая оценка. В результате могут потребоваться корректирующие действия, например идентификация дополнительных "аварийных" защитных мер и обращение за помощью в их реализации к соответствующему лицу.

Первая оценка и предварительное решение по событию ИБ

Событие ИБ может быть классифицировано по принятой в организации шкале серьезности как инцидент ИБ, причем значительный. Об этом информируется непосредственно руководитель ГРИИБ. Может потребоваться объявление "кризисной ситуации" и, как следствие, уведомление руководителя о возможной активизации плана безопасности с одновременным информированием руководителя ГРИИБ и высшего руководства. Однако наиболее вероятна ситуация передачи инцидента ИБ непосредственно в ГРИИБ для дальнейшей оценки и выполнения заранее запланированных действий.

Первая оценка и предварительное решение по событию ИБ

Независимо от того, каким будет следующий шаг, сотрудник ГОЭ заполняет форму отчета в описательном виде и по возможности характеризует следующее:

- что представляет собой инцидент ИБ;
- что явилось его причиной, чем или кем он был вызван;
- на что он влияет или может повлиять;
- фактическое или потенциальное воздействие (ущерб) инцидента ИБ на деятельность организации;
- указание на вероятную значительность/незначительность инцидента ИБ (по шкале серьезности, принятой в организации);
- как инцидент ИБ обрабатывался до этого времени и соответствующая оценка правильности и эффективности действий по реагированию на инцидент ИБ.

Первая оценка и предварительное решение по событию ИБ

Таким образом, материалы по инциденту ИБ, как правило, включают в себя:

- перечень всех активов организации, затронутых в инциденте ИБ;
- угрозы ИБ, реализованные против активов организации, и уязвимости, позволившие реализовать данные угрозы ИБ;
- предполагаемые источники угроз ИБ;
- действия и мотивацию злоумышленника;
- используемые для защиты затронутых активов СЗИ;
- действия, предпринятые по реагированию на инцидент ИБ.

Первая оценка и предварительное решение по событию ИБ

В первую очередь определяется, какое последствие может быть при потенциальном или фактическом негативном воздействии инцидента ИБ на деятельность организации в результате:

несанкционированного раскрытия информации;

несанкционированной модификации информации;

отказа от имеющейся информации;

недоступности информации и/или сервиса;

уничтожения информации и/или сервиса.

Примеры последствий: финансовые убытки/прерывание операций деятельности; ущерб коммерческим и экономическим интересам; ущерб информации, содержащей персональные данные; нарушение правовых и нормативных обязательств; сбои операций по управлению и операций деятельности; утрата престижа организации.

Первая оценка и предварительное решение по событию ИБ

Правильно проведенная оценка инцидента ИБ представляет следующие результаты:

- формируется заключение о защищенности затронутых активов, а также о причинах возникновения инцидента ИБ;
- определяется эффективность процесса реагирования на инциденты ИБ;
- оцениваются правильность и своевременность действий и решений сотрудников, ответственных за реагирование на инциденты ИБ;
- составляется заключение об ущербе, нанесенном инцидентом ИБ, включая материальный или репутационный ущерб, а также затраты на восстановление работоспособности активов, вовлеченных в инцидент ИБ, в полном объеме;
- формируется заключение об эффективности и правильности действий сотрудников, ответственных за активы, их администрирование и т. д., а также определяется, насколько точно выполнялись инструкции и предписания;
- вырабатываются рекомендации по предотвращению инцидентов ИБ в будущем и совершенствованию процедуры реагирования на инциденты ИБ.

Первая оценка и предварительное решение по событию ИБ

Для событий ИБ, отнесенных к инцидентам ИБ, используются соответствующие рекомендации по категорированию потенциальных или фактических воздействий для внесения их в отчет по инцидентам ИБ.

Если инцидент ИБ был разрешен, то отчет содержит детали предпринятых защитных мер (например, для предотвращения повторного появления подобного инцидента ИБ) и выводы.

После наиболее подробного, по мере возможности, заполнения форма отчета представляется ГРИИБ для ввода в БДСИИБ и после дующего анализа. Если расследование проводится больше недели, то обычно составляется промежуточный отчет.

Первая оценка и предварительное решение по событию ИБ

Сотрудник ГОЭ, оценивающий инцидент ИБ на основе руководств, содержащихся в документации СУИИБ, должен быть осведомлен о следующем:

- когда и кому направлять материалы об инциденте ИБ;
- при осуществлении всех действий, выполняемых ГОЭ, выполнять документированные процедуры контроля изменений.

При наличии проблем или подозрении о том, что существуют проблемы с установленными по умолчанию механизмами электронного оповещения (например, с электронной почтой), включая случаи атаки на ИС и считывания несанкционированными лицами отчета об инциденте ИБ, применяются альтернативные средства связи – курьеры, телефон, текстовые сообщения. Эти средства используются на ранних стадиях расследования, когда становится очевидным, что событие ИБ будет переведено в категорию инцидента ИБ, особенно того, который считается значительным.

Вторая оценка и подтверждение инцидента ИБ

В стандартах установлено, что в обязанности ГРИИБ входят вторая оценка и подтверждение ИБ или какое-либо другое решение относительно того, надо ли отнести событие ИБ к инциденту ИБ.
Принимающий отчеты сотрудник ГРИИБ осуществляет следующие действия:

- подтверждает получение формы отчета ГОЭ;
- вводит эту форму в БДСИИБ;
- обращается за уточнениями к ГОЭ;
- анализирует содержание отчета;
- собирает дополнительную необходимую информацию о со бытии ИБ (если она существует) от ГОЭ, заполнившего отчетную форму о событии ИБ лица или из какого-либо иного источника.

Вторая оценка и подтверждение инцидента ИБ

Если все еще есть какая-либо неопределенность относительно аутентичности инцидента ИБ или полноты полученной информации, то сотрудник ГРИИБ проводит вторую оценку для определения реальности или ложности инцидента ИБ.

Если инцидент ИБ определен как ложный, заполняется отчет о событии ИБ, добавляется в БДСИИБ и передается руководителю ГРИИБ. Копии отчета передаются ГОЭ, сообщившему о событии лицу, и местному руководителю.

Вторая оценка и подтверждение инцидента ИБ

Если инцидент ИБ определен как реальный, то сотрудник ГРИИБ, при необходимости привлекая коллег, проводит дальнейшую оценку с целью максимально быстро подтвердить:

- что представляет собой инцидент ИБ, что явилось его причиной, чем или кем он был вызван, на что он повлиял или мог повлиять, фактическое или потенциальное воздействие на деятельность организации, указание на вероятную значительность/незначительность инцидента ИБ (по принятой в организации шкале серьезности);
- предумышленную техническую атаку нарушителя на некоторую систему, сервис и/или сеть, например: глубину проникновения нарушителя и степень полученного контроля над системой, сервисом и/или сетью; данные об информации, к которой он получил доступ, были ли они скопированы, изменены или удалены; какое ПО было скопировано, изменено или разрушено;

Вторая оценка и подтверждение инцидента ИБ

- предумышленную физическую атаку нарушителя на любую ИС аппаратной части, сервиса и/или на сеть и/или на физическое месторасположение: масштабы прямых и косвенных последствий нанесенного физического ущерба (при отсутствии физической за щиты доступа); прямых и косвенных последствий в отношении инцидентов ИБ, косвенно созданных действиями нарушителя (к при меру, стал ли физический доступ возможным по причине пожара, является ли уязвимость ИС следствием неправильного функционирования ПО, линии связи или ошибки оператора);
- используемый до настоящего времени способ обработки инцидента ИБ.

Вторая оценка и подтверждение инцидента ИБ

При анализе потенциального или реального негативного воздействия необходимо подтвердить, какие последствия для деятельности организации повлек инцидент ИБ:

- несанкционированное раскрытие информации;
- несанкционированная модификация информации;
- отказ от имеющейся информации;
- недоступность информации и/или сервиса;
- разрушение информации и/или сервиса.

Для отнесения потенциальных или фактических воздействий к той или иной категории используются принятые в организации рекомендации, которые классифицируют их как инцидент ИБ, и результаты вносятся в отчет по инциденту ИБ.