УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РЕГЛАМЕНТ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[ИБ-203]

(версия 1.2)

2018 г.

Оглавление

1. Введение **3**
2. Область применения **4**
3. Термины, определения и сокращения **4**
4. Управление инцидентами информационной безопасности **5**
4.1. Обнаружение событий ИБ 5
4.2. Разрешение Инцидентов 9
4.3. Расследование Инцидентов 14
5. Группа реагирования на инциденты информационной безопасности **19**
6. Порядок пересмотра Регламента и внесения изменений **20**

1. Введение

Управление инцидентами в Компании обеспечивается в соответствии с ГОСТ Р ИСО/МЭК ТО 18044:2007 (ISO/IEC TR 18044:2004 Information security incident management). Основными задачами процесса реагирования на Инциденты являются:

- защита прав Компании, установленных законом;
- защита репутации Компании;
- информирование, в установленные нормативными документами, сроки заинтересованных внешних организаций-контрагентов;
- минимизация нарушений порядка работы и повреждения данных информационных и телекоммуникационных систем Компании, восстановление в кратчайшие сроки работоспособности систем Компании при нарушении их работоспособности в результате инцидента;
- минимизация последствий нарушения конфиденциальности, целостности и доступности информации в ИС;
- координация реагирования на инцидент;
- подтверждение/опровержение факта возникновения инцидента ИБ;
- быстрое обнаружение и/или предупреждение подобных инцидентов в будущем;
- обеспечение сохранности и целостности доказательств возникновения инцидента, создание условий для накопления и хранения точной информации об имевших место инцидентах ИБ, о полезных рекомендациях;
- обучение персонала Компании действиям по обнаружению, устранению последствий и предотвращению инцидентов ИБ.

Правильно организованный процесс управления инцидентами характеризуется:

- четким определением ролей и ответственности всех специалистов за качественное и своевременное обнаружение и реагирование на инциденты;
- оперативным мониторингом эффективности принимаемых защитных мер;
- прозрачностью контроля эффективности работы сотрудников подразделений;
- эффективным взаимодействием специалистов в смежных подразделениях;
- глубоким анализом и превентивными мерами по улучшению состояния информационной безопасности.

2. Область применения

Настоящий регламент устанавливает правила по выявлению инцидентов информационной безопасности в Компании, обработке и реагированию на инциденты информационной безопасности и анализу произошедших инцидентов. Регламент является руководством для должностных лиц, владельцев информационных ресурсов и работников, в чьи функциональные обязанности входит обеспечение безопасности информационных систем, сервисов и обеспечивающих их телекоммуникационных инфраструктур.

На основе настоящего документа разрабатываются регламенты, инструкции и планы по разрешению конкретных нарушений информационной безопасности в информационных системах Компании.

3. Термины, определения и сокращения

Администратор ИС	Обеспечивает и отвечает за функционирование ИС
АРМ	Автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи
Владелец ИС	Лицо, уполномоченное размещать запросы на разработку, доработку, внедрение или приостановку функционирования ИС и сервисов, необходимых для решения бизнес-задач организации
ИБ	Информационная безопасность – комплекс организационных и технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации
Инцидент информационной безопасности	Единичное событие или ряд нежелательных и непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации бизнес-информации и угрозы информационной безопасности.
ИС	Информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием вычислительной техники
ИТ	Информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации с использованием средств вычислительной техники
Ответственный за эксплуатацию ИС	Обеспечивает функционирование ИС и отвечает за ее эксплуатацию перед Владельцем ИС. Организует работу

	Администратора ИС
ПК	Персональный компьютер
Пользователь	Работник Организации, использующий ресурсы информационной системы для выполнения своих должностных обязанностей
Событие информационной безопасности	Идентифицированный случай состояния системы, сервиса или сети, указывающий на возможное нарушение политики информационной безопасности или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности
Третья сторона	Лицо или организация, считающаяся независимой по отношению к Организации
SIEM	Комплекс управления инцидентами информационной безопасности

4. Управление инцидентами информационной безопасности

Управление инцидентами информационной безопасности, включает в себя:

- Обнаружение инцидентов ИБ;
- Разрешение инцидентов ИБ;
- Анализ или расследование инцидентов ИБ.

4.1. Обнаружение событий ИБ

Обнаружение инцидентов ИБ осуществляется в режиме 24х7 за счет выявления событий ИБ или подозрительной активности служб и систем, приложений программ и оборудования ПАК SIEM и контролируется Администратором ИБ.

В случае если Администратор ИБ выявил или заметил событие ИБ, вызвавшее (или способное вызвать) инцидент ИБ, или любую подозрительную активность, связанную с ИБ, он немедленно сообщает о данном Событии/Инциденте ИБ в ИБ или ОИБ по телефонам ***** или *****.

В качестве событий ИБ и/или подозрительной активности могут рассматриваться, в том числе следующие события:

- уязвимости в системном и/или прикладном ПО;
- трудности и проблемы при работе с ресурсами ИС (нештатном функционировании программных и аппаратных средств ИС, нарушения целостности информации и т.п.);
- неполадки средств и систем обеспечения жизнедеятельности помещений;

- подозрительные, неадекватные (не совместимые с должностными обязанностями) действия сотрудников Компании.

Администратор ИБ сообщает директору ИБ об обнаруженном событии и/или подозрительной активности, включая:

- в чем состоит обнаруженное событие и/или подозрительная активность;
- какие активы вовлечены в обнаруженное событие;
- есть ли вероятность распространения обнаруженного события.

Сообщив директору ИБ о событии, Администратор ИБ в случае необходимости проводит дополнительный сбор исходной информации. В случае если данное событие не было зарегистрировано в ПАК SIEM в ходе мониторинга событий автоматически, Администратор ИБ регистрирует его вручную в ПАК SIEM в качестве инцидента с минимальной критичностью, фиксируя в соответствующих полях информацию о событии.

На основе собранной о событии информации, статистики Инцидентов, а также своего экспертного мнения Администратор ИБ определяет является ли оно Инцидентом и принимает решение о необходимости дальнейших действий по данному событию.

В случае если событие не является Инцидентом, Администратор ИБ делает соответствующую отметку в ПАК SIEM.

В случае если событие является Инцидентом, Администратор ИБ создает запись в ПАК SIEM и осуществляет классификацию Инцидента.

Администратор ИБ проводит дополнительный анализ Инцидента (при необходимости) и определяет к какому типу инцидентов относится зарегистрированный Инцидент. Инциденты информационной безопасности классифицируются по следующим основным типам:

Табл. 1

Типы событий и инцидентов ИБ	Описание	Ответственный за разрешение инцидента
Административные	События и инциденты, связанные с административными нарушениями (в том числе нарушениями трудового распорядка и других корпоративных правил, а также с нарушениями сотрудниками правил ИБ)	Администратор ИБ при поддержке руководителей подразделений и руководителей высшего звена
Программно-технические	События и инциденты, связанные с работой программных и аппаратных средств, участвующих в бизнес-процессах, а также связанные с работой средств защиты информации. Программно-технические инциденты в качестве подтипов включают: Несанкционированные подключения и несанкционированный доступ к ресурсам; Атаки из внешних сетей; Вирусные атаки; Неавторизованное использование ресурсов.	Администратор АС, при поддержке Администратора ИБ и руководителей подразделений, чьи бизнес-процессы затронуты инцидентом
Связанные с конфиденциальной информацией	События и инциденты, связанные с несанкционированным доступом или подозрением на доступ к конфиденциальной информации и, как следствие, с компрометацией таких данных (или АС, содержащей данные)	Администратор ИБ

После определения типа инцидента администратор ИБ определяет критичность инцидента ИБ по шкале, приведенной в Таблице 2, исходя из следующих сведений:

- информации об инциденте;
- критичности активов, вовлеченных в инцидент;
- прогнозируемой степени влияния инцидента на ключевые свойства активов.

Табл. 2

Значение	Качественное значение	Целевое время разрешения	Описание
5	**Критичный**	**4 часа**	Инцидент, указывающий на событие, связанное с тем, что система была успешно атакована, затронуты критичные ресурсы Компании. Это может привести к системной компрометации или раскрытию очень важной информации, нарушению работы критически серверов, приводящих к недоступности сервисов и полному не предоставлению услуг. В этом случае планируются и реализуются корректирующие действия.
4	**Высокий**	**16 часов**	Инцидент указывает на событие, последствия которого могут привести к компрометации данных системы. Указанный инцидент должен быть исследован, по нему оперативно принимаются меры, с целью уменьшения риска, и снижения вероятности проведения успешной атаки. В этом случае планируются и реализуются корректирующие действия.
3	**Умеренный**	**48 часов**	Инцидент потенциально может привести к системной компрометации. Возможно применение компенсирующих мер.
2	**Низкий**	**72 часа**	Инцидент, символизирует собой низкие риск или предупреждения. В этом случае, например, знание некоторых конфигураций может быть интересным, и в последствии, может потенциально привести к компрометации данных системы. Компенсирующих мер, в принципе, не требуется. Риск в этом случае может быть принят.

Значение	Качественное значение	Целевое время разрешения	Описание
1	**Очень низкий**	**96 часов**	Инцидент, связанный с событием, представляющим интерес к системе, но не представляющим угрозу безопасности системы. К ним относятся, как правило, события информационного характера. К данной категории относятся так же инциденты административного типа, связанные с нарушениями трудового распорядка и других корпоративных правил, не связанных с ИС. Компенсирующих мер, не требуется. Риск принимается.

После определения типа и критичности инцидента ИБ администратор ИБ определяет есть ли аналогичные события ИБ или связанные инциденты ИБ, которые необходимо включить в формируемую квитанцию (Ticket). Поиск аналогичных событий ИБ или связанных инцидентов ИБ администратор ИБ осуществляет в системе ПАК SIEM.

По результатам формирования окончательных записей администратор ИБ инициирует разрешение инцидента(-ов) ИБ, зафиксированных в ПАК SIEM.

4.2. Разрешение Инцидентов

Действия по решению Инцидентов зарегистрированных событий производятся в рабочее время, согласно графика работы Администратора ИБ.

В случае если инцидент имеет высокий уровень критичности (4 или 5), то для разрешений Инцидента, обязательно созывается Группа реагирования на Инциденты, о чем дополнительно сообщается директору ИБ. Группа реагирования на Инциденты и ее задачи описаны в разделе 5 настоящего Положения.

В случае если в квитанции (Ticket) ПАК SIEM закреплено несколько инцидентов, разного уровня критичности, то Группа реагирования на Инциденты, для работы по данным квитанциям ПАК SIEM, созывается на усмотрение директора ИБ и СП.

Для всех остальных Инцидентов сбор Группы не является обязательным.

Администратор ИБ по сведениям из ПАК SIEM, таблиц IP адресов определяет сотрудников, ответственных за активы, вовлеченные в Инцидент:

Для инцидентов со значением критичности 1–3, Администратор ИБ в соответствии с типом инцидента и перечнем ответственных за администрирование и поддержку, затронутых активов, назначает в ПАК SIEM Ответственного за разрешение Инцидента из числа администраторов затронутых активов или руководителя подразделения и оповещает его об этом по телефону. В случае если по данной схеме невозможно назначить Ответственного за разрешение Инцидента (например, ввиду отсутствия администратора или руководителя подразделения), Администратор ИБ

руководствуется схемой действий, используемой для инцидентов со значением критичности 4 – 5.

Для Инцидентов со значением критичности 4-5 – Администратор ИБ сообщает по телефону директору ИБ и СП и составляет на его имя служебную записку, в которой кратко описывает Инцидент. В случае если не требуется созыв Группы реагирования на Инциденты, сообщает кандидатуру на роль Ответственного за разрешение Инцидента или сообщает о необходимости созыва Группы реагирования на Инциденты, в том числе сведения о необходимом составе Группы, который включает, ответственных за активы, вовлеченные в инцидент, директора ИБ и СП, администраторов по направлениям, владельцев бизнес-процессов, вовлеченных в инцидент. Директор ИБ направляет служебную записку заместителю генерального директора по безопасности, директору ИТ и назначает Ответственного за разрешение Инцидента или инициирует созыв Группы реагирования на Инциденты, о чем уведомляет Администратора ИБ.

В случае если инцидент в ПАК SIEM зарегистрирован в нерабочее время Администратора ИБ или ночное время, разрешение Инцидента переносится до момента выхода Администратор ИБ.

В случае если Группа реагирования на Инциденты не созывается, Администратор ИБ на всем протяжении процесса разрешения Инцидента, по мере необходимости, осуществляет контроль действий Ответственного за разрешение Инцидента и оказывает необходимую поддержку.

Администратор ИБ назначив Ответственного за разрешение Инцидента или участников Группы, в ПАК SIEM открывает доступ к сведениям об инциденте, о чем отдельно уведомляет Ответственного или членов Группы реагирования на Инцидент по телефону. В случае если требуется созыв Группы реагирования на Инцидент, администратор ИБ сообщает ID-Ticket инцидента в ПАК SIEM Руководителю Группы.

Ответственный за разрешение Инцидента повторно определяет активы, вовлеченные в инцидент, и владельцев этих активов (для инцидентов, которые были заведены в ПАК SIEM вручную).

Ответственный за разрешение Инцидента оповещает владельцев бизнес-процессов и активов, затронутых инцидентом, об инциденте по телефону и инструктирует их по порядку работы в сложившейся ситуации (для инцидентов критичности 3-5 в обязательном порядке, для инцидентов критичности 1-2 на усмотрение Ответственного за разрешение Инцидента). В случае сбора Группы реагирования на Инциденты владельцев бизнес-процессов и активов, затронутых инцидентом, аналогичным образом оповещает Администратор ИБ.

При наступлении события, связанного с компрометацией конфиденциальной информации, в частности, персональных данных, сведений о конструкторской документации, финансовой информации или АС, содержащих такие данные, Администратор ИБ немедленно ставит об этом в известность директора ИБ, который должен координировать проведение разрешения данного инцидента, внутреннего

расследования, обеспечить в течение 24 часов информирование Компании о данном событии, а также координацию работ по информированию вовлеченных структурных подразделений.

Ответственный за разрешение Инцидента или Группа, в случае ее созыва, проводит повторную классификацию Инцидента на основе имеющихся сведений об Инциденте. Уточнение классификации Инцидента производится с использованием тех же шкал, что представлены в Таблицах 1 и 2 настоящего документа.

В случае возникновения разногласий по определению степени критичности инцидента при работе Группы реагирования Инцидента в качестве критичности инцидента принимается максимальная из оценок критичности, выданная участниками Группы.

В случае если инцидент имеет наивысшую степень критичности и/или затрагивает критически важные активы Компании или третьих сторон Руководитель Группы уведомляет Руководство Компании, которое принимает решение о необходимости обращения в правоохранительные органы по поводу произошедшего Инцидента. Группа, совместно с СБ осуществляют взаимодействие с правоохранительными органами и обеспечивают сохранение свидетельств Инцидента.

Ответственный за разрешение Инцидента или Группа, в случае ее созыва, проверяет существует ли типовой план разрешения для данного инцидента. В случае наличия типового плана Ответственный за разрешение Инцидента анализирует его, и при необходимости вносит коррективы и руководствуется им при разрешении данного инцидента.

В случае отсутствия типового плана разрешения инцидента, Ответственный за разрешение Инцидента или Группа, на основе анализа данных об Инциденте осуществляет планирование действий по реагированию на Инцидент (включая описание действий, необходимых для разрешения инцидента, сроки выполнения данных действий, ответственных за выполнение данных действий). Для инцидентов критичности 4 и 5 разрабатывается более подробный план мероприятий.

При планировании действий по разрешению инцидента учитываются следующие сведения об инциденте:

- кем или чем Инцидент был вызван (например, явилась ли возможность физического доступа следствием умышленных действий сотрудников, был ли Инцидент следствием ошибки оператора/администратора и т.п.);
- на что Инцидент повлиял, мог или может повлиять, каково его воздействие на бизнес-процессы Компании;
- в случае осуществления компьютерной/физической атаки выясняются детали (как глубоко нарушитель ИБ проник в ИС, что он может контролировать, какие данные и ресурсы, подверглись атаке и каковы её последствия).

Действия по разрешению инцидента могут включать (но не ограничиваются):

- мониторинг развития Инцидента;
- идентификацию источника угрозы ИБ;
- отключение (изоляцию) части ИС, сервисов, сегментов комплекса ИС на время внедрения защитных мер;
- отключение физически повреждённых устройств;
- дублирование ресурсов ИС, затронутых Инцидентом;
- восстановление работоспособности компонентов ИС, сервисов, сегментов комплекса ИС (с применением «патчей», заменой скомпрометированных элементов ИС резервными и т.п.);
- копирование системных журналов и важной информации, включая описания сервисных команд, использованных при выполнении дублирования;
- проверку информации, которая могла быть изменена, по резервным копиям;
- проверку целостности журналов систем;
- проверку целостности и работоспособности программных и технических средств, вовлеченных в инцидент;
- анализ правовых и договорных требований (отчётности и др.), которые должны быть выполнены в Компании, в случае компрометации ИС, произошедшей в результате данного Инцидента, а также выполнение мер по их соблюдению.

Для инцидентов, связанных с компрометацией конфиденциальной информации, в частности, персональных данных, сведений о конструкторской документации, финансовой информации или АС, содержащих такие данные, необходимо запланировать и выполнить следующие действия:

- не подключаться к скомпрометированным системам, в том числе с административными привилегиями и не изменять существующие пароли;
- не выключая скомпрометированные компьютеры, отключить их от телекоммуникационных сетей;
- сохранить все доступные протоколы работ;
- создать резервную копию скомпрометированной системы для облегчения проведения дальнейшего расследования;
- протоколировать все выполняемые действия;
- осуществлять мониторинг всех систем обработки и передачи данных;
- оповестить все вовлеченные стороны:
- контрагентов (при необходимости);
- правоохранительные органы (при необходимости);
- действовать в соответствии с требованиями и рекомендациями нормативных документов международных платежных систем.

В случае компрометации АС Ответственными за АС совместно с владельцами

данных АС должны быть запланированы и выполнены следующие действия:

- зафиксировать время наступления компрометации;
- определить способ компрометации;
- оценить нанесенный АС ущерб;
- внести изменения в настройки программных и технических средств и/или внесение изменений в процессы и меры обеспечения ИБ, блокирующие повторные попытки действий, приведших к компрометации, удалить вредоносное ПО и сменить все пароли АС, которые могли быть скомпрометированы, после чего восстанавливается штатный режим работы всех систем;
- определить перечень скомпрометированных данных и систем, перечень контрагентов, затронутых данным событием;
- в соответствии с установленными платежными системами правилами и двухсторонними договорами с контрагентами произвести уведомление о наступившем событии вовлеченных лиц;
- определить перечень выводимых из обращения данных (например, криптографические ключи, данные о держателях карточек, карточки и т.д.), вывести указанные данные из обращения и произвести действия по замене этих данных и карточек;
- после проведения всего комплекса мероприятий, связанных с компрометацией, восстановить нормальную работу Компании. Все протоколы работы АС, свидетельства и документы должны быть переданы в ДБиИТ.

Ответственный за разрешение Инцидента или Группа, осуществляют действия по разрешению инцидента в соответствии с запланированными мероприятиями.

По ходу разрешения Инцидента, Ответственный за разрешение Инцидента фиксирует свои действия по разрешению инцидента в ПАК SIEM (в виде логов) или другими способами, в случае если невозможно использовать встроенные функции ПАК SIEM.

В случае невозможности разрешения Инцидента в сроки, заданные для инцидентов данной степени критичности (Таблица 2), Ответственный за разрешение Инцидента уведомляет директора ИБ и директора ИТ, которые принимают решение о дальнейших действиях по разрешению Инцидента.

По результатам разрешения инцидента Ответственный за разрешение Инцидента в случае сбора Группы – Администратор ИБ, оповещает владельцев бизнес-процессов и активов, затронутых инцидентом, об успешном завершении разрешения Инцидента и дает рекомендации по дальнейшей работе с затронутыми инцидентом ресурсами. В случае если в ходе инцидента были затронуты активы третьих сторон, директор ИБ аналогичным образом оповещает ответственных сотрудников со стороны третьих сторон (в соответствии с перечнем контактов).

По результатам разрешения Инцидента Ответственный за разрешение Инцидента сообщает об этом Администратору ИБ и передает все материалы по данному инциденту (логи, документы, появившиеся в ходе разрешения инцидента и т.д.).

Администратор ИБ изучает материалы, переданные ему Ответственным за разрешение Инцидента и передает их директору ИБ, который принимает решение о закрытии инцидента. В случае если директор ИБ не может самостоятельно принять решение о закрытии инцидента, он обращается к заместителю генерального директора по безопасности, который принимает окончательное решение.

После закрытия Инцидента Администратор ИБ формирует необходимый отчет с использованием средств ПАК SIEM.

Результаты расследования направляются Директору по ИБ.

4.3. Расследование Инцидентов

Заместитель генерального директора по безопасности Компании на основании Отчета об инциденте принимает решение о необходимости анализа или расследования инцидента и выбирает один из следующих видов расследования:

- Служебное расследование Инцидента – предполагает сбор сведений об инциденте и его причинах, нарушителях/злоумышленниках, проводится сотрудниками СБ. Материалы, полученные в ходе служебного расследования, не могут быть использованы для передачи в качестве доказательств в судебном разбирательстве.
- Расследование с привлечением правоохранительных органов – проводится в случае необходимости обеспечения доказательной силы материалов/доказательств инцидента в рамках судебных разбирательств, а также в случае нарушения статей 272-274 УК РФ.

В случае если требуется проведение расследования с привлечением правоохранительных органов директор ИБ обращается к руководству Компании, которое принимает окончательное решение о типе расследования. Привлечение правоохранительных органов к расследованию Инцидента ИБ описано в разделе 6 настоящего Положения.

4.3.1. Служебное расследование Инцидентов

Служебное расследование Инцидентов проводится с целью определения нарушителей ИБ для возмещения причиненного ущерба и предотвращения подобных инцидентов в дальнейшем.

Служебное расследование проводится сотрудниками СБ с привлечением сотрудников профильных подразделений и, при необходимости, руководителей подразделений, вовлеченных в инцидент. При необходимости, для проведения служебного расследования могут привлекаться сотрудники сторонних организаций.

Сотрудники СБ, в рамках проведения служебного расследования инцидента

информационной безопасности, осуществляют следующие процедуры:

Сбор и анализ первоначальных сведений об инциденте, включающих:

- сообщения от технических средств (СЗИ, серверов, активного сетевого оборудования и др.);
- сообщения от сотрудников Компании (пользователей, администраторов АС/ИБ и т.д.);
- сбор доказательств по инциденту (журналов регистрации событий серверов, рабочих станций, сетевого активного оборудования, средств защиты информации, копий жестких дисков и других данных, собранных на предшествующих этапах);
- данные, зафиксированные системами контроля доступа и видеонаблюдения;

Определение значимости инцидента на основе следующих данных:

- оценки критичности ресурсов, вовлеченных в инцидент;
- риска реализации угроз в отношении данных ресурсов;
- защищенности ресурсов.

Анализ действий нарушителя, включающий в себя следующее:

- анализ журналов регистрации событий СЗИ и программно-технических средств, вовлеченных в инцидент;
- опрос сотрудников Компании;
- изучение данных систем видеонаблюдения и контроля доступа;
- анализ средств и методов, используемых нарушителем.

Анализ действий по реагированию на Инцидент, включающий:

- анализ собранных доказательств по инциденту (журналов регистрации событий серверов, рабочих станций, сетевого активного оборудования, средств защиты информации, копий жестких дисков и других данных, собранных на предшествующих этапах);
- анализ действий, предпринятых сотрудниками Компании по разрешению инцидента;
- опрос сотрудников Компании;
- изучение данных систем видеонаблюдения и контроля доступа;
- контроль текущего состояния информационной безопасности ИС;

Формирование рекомендаций по предотвращению инцидентов и совершенствованию процедуры реагирования, включающее:

- определение последствий инцидента с указанием всех ресурсов, затронутых инцидентом, и предварительного ущерба, нанесенного инцидентом;
- анализ эффективности мер по реагированию на инцидент с указанием ресурсов, используемых для реагирования на инцидент;

- формирование рекомендаций по изменению процедур реагирования на инциденты, разработке дополнительных документов в части реагирования на инциденты и выделению дополнительных ресурсов, внесению изменений в существующие меры обеспечения ИБ, проведению дополнительного анализа рисков ИБ.

В результате СБ:

- определяет причины инцидента;
- определяет перечень ресурсов, вовлеченных в инцидент, и их критичность,
- осуществляет экспертную оценку нанесенного ущерба;
- формирует сведения о нарушителе и используемых им средствах;
- определяет процедуры реагирования на инциденты (по возможности производит оценку указанной процедуры);
- оценивает правильность и своевременность действий и решений Ответственного за разрешение Инцидента (или Группы);
- вырабатывает рекомендации по предотвращению инцидентов и совершенствованию процедуры реагирования, в том числе по проведению обучения сотрудников Компании.

В качестве мероприятий по устранению причин инцидентов и предотвращения повторений могут применяться следующие меры:

- проведение анализа рисков и выбор адекватных мер обеспечения ИБ;
- проверка защищенности и выявление уязвимостей программно-технических средств ИС специализированными средствами (сканеры безопасности);
- выявление потенциальных каналов утечки информации;
- обучение сотрудников Компании;
- проведение тестирования процедур реагирования на инциденты и тренировок;
- материальное стимулирование сотрудников.

По результатам служебного расследования Инцидента СБ формирует отчет об анализе Инцидента в свободной форме, который включает следующие сведения:

- дату составления отчета;
- краткое описание инцидента;
- оценку ущерба от инцидента;
- причины произошедшего инцидента;
- меры по предотвращению инцидентов, предпринятые до начала инцидента, во время инцидента и после инцидента.
- оценку действий сотрудников Компании во время инцидента ИБ;

- ответственных (организаторы и исполнители) за произошедший инцидент, если в ходе расследования это удалось выяснить, описание предпринятых ими действий и причин, приведших к этому;
- оценку целесообразности (возможности) проведения действий по привлечению к ответственности и компенсации нанесенного ущерба;
- действия нарушителей в привязке к использованным уязвимостям и реализованным угрозам, приведшим к инциденту;
- рекомендации по предотвращению инцидентов и совершенствованию процедуры реагирования, в том числе по проведению обучения сотрудников Компании.

По окончании служебного расследования все собранные по инциденту материалы передаются на хранение директору ИБ. Материалы должны храниться в сейфе директора ИБ.

Директор ИБ согласовывает отчет об анализе Инцидента с директором ИТ и представляет отчет заместителю генерального директора по безопасности. Заместитель генерального директора по безопасности принимает решение о выполнении рекомендаций, изложенных в отчете и назначает ответственных для выполнения рекомендаций, изложенных в отчете, из числа сотрудников Компании.

В случае необходимости директор ИБ, на основании отчета, формирует служебную записку руководству Компании с указанием виновных в инциденте и понесенного ущерба, включая заключение о целесообразности привлечения виновных к ответственности.

При проведении расследования свыше недели руководству Компании представляется еженедельный отчет.

4.3.2. Расследование с привлечением правоохранительных органов

Решение по обращению в правоохранительные органы принимается руководством Компании.

Заместитель генерального директора по безопасности согласовывает с генеральным директором Компании, обращение в правоохранительные органы и вместе с Ответственным по контактам с правоохранительными и судебными органами осуществляет дальнейшее взаимодействие с органами следствия и дознания, а также оказывают практическую помощь членам следственно-оперативной группы при производстве отдельных следственных действий и оперативно-розыскных мероприятий.

Ответственный по контактам с правоохранительными и судебными органами отвечает за сбор всех сообщений об инцидентах.

Взаимодействие Ответственного по контактам с правоохранительными и судебными органами может происходить в случае, если критичность инцидента соответствует уровню 4 и выше. При этом должна быть получена исчерпывающая

информация, касающаяся следующих сведений:

- критичности активов, вовлеченных в инцидент;
- прогнозируемой степени влияния инцидента на ключевые свойства активов;
- другой доступной информации.

При взаимодействии с правоохранительными и судебными органами может быть передана информация, касающаяся инцидента:

- дата и время его фиксации;
- ресурс ИС, безопасность которого может быть нарушена;
- вид, способ воздействия на ресурс;
- сведения о нарушителе (внутренний/внешний, предположения о квалификации);
- сведения об эффективности реагирования СЗИ (успешность отражения атак или попыток атак).

По требованию правоохранительных и судебных органов Ответственный по контактам с правоохранительными и судебными органами осуществляет:

- сохранение журналов регистрации событий серверов, рабочих станций, сетевого активного оборудования, средств защиты информации, копий жестких дисков и других данных на отторгаемые носители;
- получение сохраненных записей системы видеонаблюдения и контроля доступа;
- получение данных опроса пользователей и администраторов ИС Компании.

Ответственный по контактам с правоохранительными и судебными органами после получения данных указанных в п. 8.5 обобщает материалы Группы реагирования на Инциденты ИБ, и по решению руководства Компании предоставляет их в распоряжение правоохранительных и судебных органов.

Сбор свидетельств и доказательств по инциденту ИБ выполняется сотрудниками правоохранительных и судебных органов.

По окончании расследования заместитель генерального директора по безопасности Компании получает все необходимые заключения и передает полученные сведения руководству безопасности Компании.

Руководство Компании, на основании расследования правоохранительных органов принимает решение об обращении по факту Инцидента ИБ в суд. Решение по обращению в судебные органы принимается руководством Компании.

Ответственный по контактам с правоохранительными и судебными органами, на основании имеющейся информации, оформляет необходимые документы для обращения в судебные органы, и осуществляет взаимодействие с правоохранительными и судебными органами.

Для всех участвующих во взаимодействии с правоохранительными и судебными органами представителей Компании основными целями является содействие в полном и окончательном расследовании инцидента, раскрытие возможных пособников злоумышленника и, при наличии на то оснований, возбуждение уголовного дела в отношении лиц, совершивших злонамеренные действия.

5. Группа реагирования на инциденты информационной безопасности

Создание и состав Группы реагирования на инциденты ИБ утверждается Приказом генерального директора Компании или директором предприятия, входящего в состав Компании. В Группе реагирования на инциденты ИБ определяется Ответственный по контактам с правоохранительными и судебными органами;

Основными целями деятельности Группы реагирования на инциденты ИБ являются:

- организация работ и привлечение квалифицированного персонала для учета, реагирования, анализа инцидентов и минимизации их последствий;
- обеспечение необходимой координации и управления процессом реагирования на инциденты;
- обеспечение должного уровня информирования руководства и должностных лиц;
- обеспечение максимального снижения последствий инцидентов, как в материальной сфере, так и для репутации предприятия.

В состав Группы включаются представители следующих подразделений:

- СБ;
- ИТ;
- юридического департамента;
- владельцы активов и бизнес-процессов, вовлеченных в Инцидент.

При необходимости к работе Группы привлекаются сотрудники профильных подразделений и внешние эксперты для оказания поддержки обеспечения правовой, административной, экспертной и технологической деятельности.

Директор ИБ, назначается руководителем Группы.

Руководитель Группы реагирования на инциденты ИБ должен:

- иметь полномочия в рамках своей компетенции по принятию немедленных решений, касающихся инцидентов ИБ;
- иметь особую (вне нормальных бизнес-отношений) линию (способ) для информирования руководства Компании;
- иметь возможность привлекать к работе Группы специалистов для реагирования/расследования инцидентов ИБ в требуемой области.

6. Порядок пересмотра Регламента и внесения изменений

Настоящий Регламент пересматривается:

- при изменении законодательства РФ и нормативных актов регуляторов ИБ (ФСБ России, ФСТЭК России) (в т.ч. Политики информационной безопасности Компании);
- после изменений структуры информационной системы и применения новых технологий передачи, хранения и обработки информации
- после проверки соответствия ИБ (аудит, самооценка ИБ);
- после анализа произошедших инцидентов ИБ;
- по результатам анализа рисков ИБ (с учётом предложений владельцев информационных активов);
- по результатам анализа данных базы событий и инцидентов ИБ, но не реже одного раза в 2 (два) года после утверждения предыдущей редакции Регламента реагирования на инциденты Компании.

В процессе пересмотра настоящего Регламента директор ИБ обеспечивает проведение тестирования процедур по реагированию на инциденты ИБ, предусмотренных настоящим Регламентом, при этом оцениваются:

- оперативность взаимодействия членов Группы между собой, а также с другими работниками при передаче информации об инцидентах ИБ;
- состояние технических средств, предназначенных для сбора и анализа свидетельств инцидента ИБ;
- наличие и полнота процедур системы управления инцидентами ИБ (способствующих обнаружению инцидента ИБ и реагированию на него; по восстановлению ИС после идентификации и локализации инцидента ИБ), а также эффективность передачи информации об инциденте ИБ (обнаружение, оповещение, реагирование).

По результатам тестировании процедур по реагированию на инциденты ИБ в свободной форме сотрудником ИБ формируется «Протокол тестирования процедур по реагированию на инциденты ИБ», включающий сведения о проведенном тестировании, заключения о результатах тестирования.

По результатам тестирования процедур по реагированию на инциденты проводится внеплановое обучение сотрудников Компании.

Пересмотр Регламента производится ДБиИТ. Измененный Регламент выносится на рассмотрение и утверждение руководства Компании.