План реагирования на инциденты информационной безопасности.

1. Введение

Управление инцидентами в ООО «АВС» (далее Компания) 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.

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. 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 24x7 за счет выявления событий ИБ или подозрительной активности служб и систем, приложений программ и оборудования 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 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.

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

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 в SIEM зарегистрирован в нерабочее время Администратора ИБ или ночное время, разрешение Инцидента переносится до момента выхода Администратор ИБ.

В случае если инцидент имеет высокий уровень критичности, то для разрешений Инцидента, обязательно созывается Группа реагирования на Инциденты, о чем дополнительно сообщается директору ИБ. Для всех остальных Инцидентов сбор Группы не является обязательным.

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).
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 SIEM (в виде логов) или другими способами, в случае если невозможно использовать встроенные функции SIEM.

В случае невозможности разрешения Инцидента в сроки 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.

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

Результаты расследования направляются Директору по ИБ.

4.3. Расследование Инцидентов

Директор 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.

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;
- Анализ действий нарушителя;
- Анализ действий по реагированию на Инцидент;
- Формирование рекомендаций по предотвращению инцидентов и совершенствованию процедуры реагирования.

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

При проведении расследования свыше недели руководству Компании представляется еженедельный отчет.

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.

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.