**Общество с ограниченной ответственностью «Компания «АБС»»**

**План реагирования на инциденты информационной безопасности.**

**1. Введение**

1.1 Настоящий План реагирования на инциденты информационной безопасности (далее ПРИИБ) устанавливает руководящие принципы для обеспечения сохранения конфиденциальности, сохранности и целостности как собственных данных, так и данных находящихся в распоряжении и операционном управлении ООО «Компания «АВС»» (далее Компания);

1.3 ПРИИБ применяется к информации или информационным системам находящимся:

* На локальных серверах Компании, а также облачных хранилищах принадлежащих или арендуемых Компанией;
* В web-приложениях Компании, а также в социальных сетях и мессенджерах в распоряжении Компании;
* На устройствах клиентов Компании (приложения, обеспечивающие доступ клиентов в личный кабинет «Партнёр-API»);

1.4 ПРИИБ поменяется также ко всей прочей исходящей информации, связанной с операционной деятельностью Компании (в том числе деловая переписка, обмен информации с государственными структурами);

1.3 ПРИИБ составлен в соответствии с:

* Федеральным законом «О защите персональных данных» № 152-ФЗ;
* Федеральным законом «Об информации, информационных технологиях и о защите информации" № 149-ФЗ»;
* Постановлением Правительства РФ № 1119 «Об утверждении Правил разработки, утверждения и реализации планов реагирования на инциденты в области информационных технологий»;
* Межотраслевыми рекомендациями по обеспечению безопасности информации (МРБИ) - разработанные ФСТЭК России;
* ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» - международным стандартом по управлению информационной безопасностью.

**2. Определения**

2.1 Инцидент информационной безопасности - непредвиденное событие, которое может нанести ущерб или иметь потенциальное воздействие на конфиденциальность, целостность или доступность информации или информационных систем;

2.2 Инцидентом считается любое несанкционированное руководством Компании действие в отношении информации и информационных систем Компании вне зависимости от степени физического, коммерческого или репутационного ущерба, причиненного Компании или Клиентам Компании;

2.3 Наиболее распространенными инцидентами являются: разрушение (отключение) внутренней системы безопасности данных, кибератака, утечка информации, несанкционированный доступ к информации и информационным системам, внедрение вирусов, фишинговая атака, DDoS-атака, а также действия в отношении сотрудников или клиентов Компании, носящие признаки манипулирования сознанием или применения социальной инженерии.

**3. Основные принципы управления Инцидентом**

3.1 Инцидент требует немедленного реагирования и устранения проблемы, чтобы минимизировать потенциальные негативные последствия для Компании или ее клиентов;

3.2 Управление Инцидентами включает в себя:

* Предотвращение Инцидента;
* Выявление (обнаружение) Инцидента;
* Реагирование на Инцидент
* Ликвидация воздействия Инцидента;
* Восстановление (информации и информационных систем, репутации) после Инцидента;
* Оценка и покрытие ущерба нанесенного Инцидентом;
* Расследование причин Инцидента, применение мер ответственности к виновным и поощрения отличившихся при ликвидации Инцидента;
* Разбор и обучение персонала Компании и клиентов на примере Инцидента.

**4. Организационные основы ПРИИБ и базовые положения в качестве мер по предотвращению Инцидента**

4.1 Организационные основы ПРИИБ:

* Начальник департамента автоматизации создает и возглавляет группу быстрого реагирования (ГБР) на Инциденты ИБ состоящую из действующих сотрудников Компании (сетевые администраторы, системные администраторы) с назначением дежурного ГБР и распределением сотрудников по секторам контроля;
* Начальник департамента автоматизации создает и возглавляет группу по расследованию инцидентов, куда по мере необходимости могут быть включены сотрудники юридического отдела, сотрудники физической безопасности и сотрудники прочих служб по согласованию с руководством Компании;
* Начальник департамента автоматизации является ответственным за соблюдение ПРИИБ, ее актуализацию и обновление по мере необходимости;
* Начальник департамента кадров является ответственным за систему оплаты сверхурочно и вне рабочего времени для обеспечения ПРИИБ;
* Начальник планово-экономического отдела является ответственным за подготовку бизнес-планов внедрения мероприятий ПРИИБ с указанием сроков внедрения и объема денежных средств необходимых на внедрение;
* Финансовый директор является ответственным за оценку бизнес-плана внедрения ПРИИБ, утверждение бюджета мероприятий ПРИИБ и включение его в финансовый план Компании;
* Начальник административно-хозяйственного отдела обеспечивает закупку материалов и выполнение строительных и ремонтных работ по обеспечению мероприятий ПРИИБ в плане физических мер безопасности;
* Начальник юридического департамента является ответственным за правовое сопровождение мероприятий ПРИИБ;
* Начальник отдела маркетинга и PR является ответственным за оценку репутационных рисков компании, а также за проведение мероприятий, направленных на минимизацию репутационных издержек Компании в случае Инцидентов ИБ;
* Руководство и координация всех служб по внедрению и реализации ПРИИБ возлагается на Заместителя генерального директора по безопасности.

4.2 Базовый положения ПРИИБ:

4.2.1 Обеспечение парольной защиты:

* Требование использования сложных паролей, включающих комбинацию цифр, букв верхнего и нижнего регистров, а также специальных символов.
* Регулярная смена паролей и запрет повторного использования предыдущих паролей.
* Введение многофакторной аутентификации для повышения безопасности доступа к системам и приложениям.

4.2.2 Обеспечение регулярного обновления и патчинга программного обеспечения:

* Установка автоматических обновлений для операционных систем, прикладного программного обеспечения и антивирусных программ.
* Регулярное сканирование и обновление всех уязвимых программных компонентов.

4.2.3 Обеспечение безопасности сети:

* Использование брандмауэров и интрузионных обнаружений для мониторинга и защиты сетевого трафика.
* Разделение сетей на отдельные зоны с различными уровнями доступа и защиты.
* Регулярный аудит сетевой инфраструктуры для выявления уязвимостей и недопустимых настроек.

4.2.3 Обучение сотрудников:

* Проведение обучающих программ по информационной безопасности для всех сотрудников, включая осведомление о социальной инженерии, фишинге, использовании электронной почты и веб-безопасности.
* Повышение осведомленности о существующих угрозах и методах защиты данных.

4.2.4 Обеспечение регулярного резервного копирования данных:

* Разработка и реализация плана регулярного резервного копирования данных.
* Проверка работоспособности процедур восстановления после сбоя или инцидента.
* Мониторинг и анализ событий:
* Установка системы мониторинга и анализа событий для обнаружения потенциальных инцидентов ИБ.
* Анализ журналов событий и регулярное отслеживание необычной активности и попыток несанкционированного доступа.

4.2.5 Проведение регулярных аудитов и тестирования:

* Проведение регулярных аудитов информационной безопасности для выявления уязвимостей и оценки соответствия политике ИБ.
* Проведение пентестинга (тестирования на проникновение) для идентификации слабых мест в системе и обеспечения их устранения.
* Установка антивирусных и анти-малварных программ:
* Регулярное обновление и сканирование всех компьютеров и серверов для обнаружения и предотвращения вирусов, вредоносного ПО и других угроз.

4.2.6 Организация управления доступом:

* Применение принципа наименьших привилегий, предоставление доступа только к необходимым ресурсам и функциям.
* Четкое и актуальное управление пользователями и их правами доступа.

4.2.7 Установка физических мер безопасности:

* Защита физического доступа к серверным комнатам, центрам обработки данных и другим критическим инфраструктурным объектам.
* Использование видеонаблюдения, контроля доступа и других физических мер безопасности.

4.2.8 Сотрудничество с внешними экспертами:

* Регулярная оценка и аудит информационной безопасности компании внешними специалистами.
* Получение консультаций и рекомендаций от профессионалов в области информационной безопасности.

4.2.9 Тренировки по плану реагирования:

* Регулярные тренировки и учения по плану реагирования, для целей готовности сотрудников Компании к эффективному реагированию на возможные инциденты ИБ.
* Информационная работа среди сотрудников и клиентов Компании с освещением возможных угроз и выработки определенного алгоритма действий при возникновении Инцидента.

**5. Реагирование на Инцидент**

5.1 Постоянное выполнение положений ПРИИБ

* В Компании на постоянной основе должны выполняться все положения ПРИИБ (п. 4.2) на высочайшем уровне качества и ответственности;
* Все сотрудники Компании, так или иначе связанные с выполнением положений ПРИИБ должны обладать необходимыми компетенциями, регулярно проходить учебу, повышение квалификации и переподготовку при внедрении новых способов и мер реагирования на Инциденты.

5.2 Обнаружение инцидента

Сотрудник Компании или Клиент обнаруживший инцидент, должен немедленно уведомить дежурного сотрудника ГБР по «горячей линии», который в свою очередь незамедлительно уведомляет начальника департамента автоматизации и принимает меры по реагированию на Инцидент;

5.3 Реагирование на инцидент

* Изолируются системы, подвергшиеся воздействию;
* Анализируется степень воздействия Инцидента для определения его характеристик и механизмов распространения;
* Применяются меры по обезвреживанию или устранению воздействия Инцидента
* Применяются меры по восстановлению нормальной работы систем подвергшихся воздействию.

5.4 Координация действий

Начальник департамента автоматизации координируют действия ГБР, по мере необходимости привлекает системных администраторов, команду по расследованию инцидентов и сотрудников юридического отдела, отдела маркетинга и PR, которые выполняют свои обязанности в соответствии с назначенными задачами.

5.5 Оповещение руководства

* Начальник департамента автоматизации как можно скорее оповещает заместителя генерального директора по безопасности о произошедшем инциденте и предоставляет как можно более полную информацию о возможных последствиях и предпринятых мерах;
* В свою очередь заместителя генерального директора по безопасности доводит до сведения генерального директора информацию о произошедшем Инциденте и возможной степени его воздействия на работу Компании

5.7 Анализ и предпринимаемые действия

* Команда по расследованию инцидентов проводит анализ инцидента, определяет его источник и причины;
* Команда по расследованию инцидентов разрабатывает рекомендации для усиления системы безопасности и предотвращения подобных инцидентов в будущем.

5.8 Правовая оценка

Юридический отдел оценивает возможные правовые последствия инцидента и координирует действия в соответствии с законодательством о защите данных и информационной безопасности.

5.9 Репутационная оценка

Отдел маркетинга и PR оценивает возможные репутационные последствия инцидента, координирует действия по освещению Инцидента в СМИ и проводит PR-акции в зависимости от степени воздействия Инцидента на репутацию Компании.

5.10 Заключительные решения

* По мере выполнения ПРИИБ и устранения последствий Инцидента под руководством заместителя генерального директора формируется заключительный акт о произошедшем Инциденте, где оценивается степень готовности Компании к подобного рода Инцидентам, скорость реакции на Инцидент, время на нейтрализацию Инцидента и восстановление нормальной работы Компании, материальный и репутационный ущерб нанесенный Инцидентом;
* На основании созданного документа Заместитель генерального директора по безопасности принимает решение об обновлении ПРИИБ и внедрению новых положений, направленных на недопущение в будущем подобных Инцидентов.

**6. Заключительные положения**

6.1 План реагирования на инциденты информационной безопасности (ПРИИБ) является обязательным для всех сотрудников Компании «АБС» в рамках их компетенций;

5.3 ПРИИБ должен регулярно обновляться и приводиться в соответствие с актуальными требованиями и стандартами;

5.4 Ответственность за подготовку технической и административной документации, разработанной в целях реализации ПРИИБ, а также неукоснительное выполнение всех технических и административных мероприятий, направленных на выполнение ПРИИБ возложить на Заместителя генерального директора по безопасности Петрова Б.В.;

Генеральный директор Иванов А.Г.

Приложение 1

**План реагирования на DDos-атаку**

**1. Обнаружение и анализ:**

1.1 Обеспечить постоянное дежурство подготовленных сотрудников группы быстрого реагирования (ГБР), отвечающих за реагирование на Инцидент;

1.2 Обеспечить бесперебойную работу «горячей линии» для связи с дежурным сотрудником ГБР;

1.3 Обеспечить бесперебойную работу систем и оборудования:

* Средств мониторинга сетевого трафика для обнаружения аномального поведения, увеличения трафика или необычных запросов;
* Мониторинга системы журналирования (логов) для обнаружения подозрительной активности или нестандартных событий;
* Системы защиты от DDoS (например, фильтры, IDS/IPS) для выявления атак;
* Проактивного мониторинга новых уязвимостей и известных методов DDoS-атак.

**2. Локализация, ликвидация угрозы:**

*В работе по локализации и ликвидации угрозы принимают участие сотрудники ГБР под руководством начальника департамента автоматизации, но при необходимости привлекаются дополнительные сотрудники*

2.1 Определить и локализовать источники DDoS-трафика, например, по IP-адресам или характеристикам пакетов;

2.2 Оперативно отреагировать на обнаруженную атаку путем настройки маршрутизаторов и брандмауэров для фильтрации и блокирования вредоносного трафика;

2.3 Связаться с интернет-провайдером для сотрудничества и установления защитных мер на уровне сети;

2.4 Запустить систему защиты от DDoS, для обнаружения и блокировки вредоносного трафика;

2.5 Провести с командой разработки ПО обновление веб-приложений для устранения уязвимостей, которые могут быть использованы злоумышленниками для запуска DDoS-атак.

**3. Восстановление системы:**

*В восстановлении системы принимают участие сотрудники, которых назначает начальник департамента автоматизации, здесь могут быть как сетевые администраторы, системные администраторы, разработчики ПО, специалисты прочих департаментов (клиентский, бухгалтерия, планово-экономический, маркетинга и PR) в зависимости от тех участков информация которых пострадала в результате Инцидента*

3.1 Проверить инфраструктуру и системы на наличие повреждений и восстановление их работоспособности;

3.2 Восстановить соединение с интернетом и проверить стабильность сетевой инфраструктуры;

3.3 Проверить работоспособность и доступность веб-приложений и сервисов Компании;

3.4 Восстановить базы данных и файлы, которые были повреждены в результате атаки;

3.5 Провести тесты нагрузки и исправление любых выявленных проблем.

**4. Меры, принимаемые после Инцидента:**

*Под непосредственным руководством заместителя генерального директора Компании по безопасности проводятся мероприятия:*

4.1 Оформить заключительный акт по Инциденту, включающий описание атаки, ее влияние на бизнес, принятые меры и результаты восстановления;

4.2 Провести анализ причин и последствий DDoS-атаки, с целью предотвращения подобных инцидентов в будущем;

4.3 Обновить политику безопасности и процедуры для улучшения защиты от DDoS-атак;

4.4 Обучить сотрудников о поведении и реагировании на подобные инциденты;

4.5 Провести аудит безопасности для выявления уязвимостей и улучшения системы защиты.