РЕГЛАМЕНТ
управления инцидентами информационной безопасности в ООО «Сатурн»

Москва 2018

Содержание

1 Информация о документе

1.1 Назначение документа

Настоящий Регламент управления инцидентами информационной безопасности в ООО «Сатурн» (далее – Регламент) определяет порядок управления инцидентами информационной безопасности в ООО «Сатурн» (далее – Общество).

1.2 Цель принятия документа

Настоящий Регламент принят в целях обеспечения безопасности персональных данных при их обработке в Обществе.

1.3 Область применения документа

Настоящий документ обязан знать и использовать члены Комиссии по обеспечению безопасности персональных данных.

1.4 Вводимые сокращения и термины

Таблица 1 — Перечень сокращений

Сокращение	Расшифровка сокращения
ИТ	информационные технологии
МЭ	межсетевой экран
НД	нормативный документ
ОС	операционная система
ПО	программное обеспечение

Таблица 2 — Перечень терминов

Термин	Определение термина
Владелец процесса	должностное лицо, управляющее процессом и несущее ответственность за результаты процесса.
Структурное подразделение	официально выделенная в организационной структуре Общества группа работников
Процесс	деятельность под управлением Владельца процесса, направленная на достижение эффективных результатов
Внешний процесс	процесс, являющийся внешним по отношению к рассматриваемому процессу. Внешние процессы могут быть двух категорий: а) бизнес-процессы Общества, б) бизнес-процессы сторонних организаций или физических лиц
Этап процесса	логически законченная часть процесса, используется для выделения в процессе основных составных частей процесса
Шаг процесса	логически законченная часть этапа процесса, используется для детализации этапа процесса
Вход	материальный или информационный объект или услуга, входящий в процесс (этап, шаг процесса)
Выход	материальный или информационный объект или услуга, являющийся результатом выполнения процесса (этапа, шага процесса)

Термин	Определение термина
Документ	информация в виде текста, звукозаписи или изображения с набором реквизитов, позволяющих ее идентифицировать
Поставщик	подразделение или должностное лицо, сторонняя организация, физическое лицо, предоставляющее входы процесса
Потребитель	подразделение или должностное лицо, сторонняя организация, физическое лицо, получающее результат выполнения процесса
Показатели процесса	показатели, характеризующие ход выполнения процесса, результаты процесса и удовлетворенность потребителей результатом процесса
Группа по расследованию инцидента информационной безопасности	работники, привлекаемые к расследованию инцидента информационной безопасности

1.5 Внешние нормативные и распорядительные документы

Таблица 3 — Внешние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 24.07.2014) «О персональных данных»

1.6 Внутренние нормативные и распорядительные документы

Таблица 4 — Внутренние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Положение об организации обработки персональных данных
2	Публичная политика обработки персональных данных
3	Регламент взаимодействия с уполномоченными органами в сфере обработки и обеспечения безопасности персональных данных

1.7 Пересмотр документа

Пересмотр настоящего Регламента должен осуществляться в следующих случаях, но не реже одного раза в три года:

– при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;

– при существенном изменении процессов обработки персональных данных Общества.

2 Выполнение процесса

2.1 Этапы процесса

Таблица 5 – Этапы процесса

№ п/п	Наименование этапа/шага процесса	Длительность и начало выполнения	Вход	Выход	Подразделение / Должность	
					Ответственный	Участвует
1	Создание группы по реагированию на инцидент информационной безопасности					
1.1	Анализ инцидента информационной безопасности	1 день	Вх. событие: Инцидент информационной безопасности	Произведена оценка риска инцидента ИТ-безопасности	Ведущий специалист по информационной безопасности и защите персональных данных	
1.2	Назначение руководителя группы по расследованию инцидента	1 день	Произведена оценка риска инцидента информационной безопасности	Назначен руководитель группы по расследованию инцидента информационной безопасности	Директор по информационной безопасности и специальным проекта	Ведущий специалист по информационной безопасности и защите персональных данных
1.3	Формирование группы по расследованию инцидента	1 день	Назначен руководитель группы по расследованию инцидента информационной безопасности	Сформирована группа по расследованию инцидента информационной безопасности	Руководитель группы по расследованию инцидента информационной безопасности	Директор по информационной безопасности и специальным проекта
2	Утверждение служебной записки по устранению инцидента информационной безопасности					
2.1	Разработка плана мероприятий по устранению инцидента информационной безопасности	1 день	Группа по расследованию инцидента информационной безопасности.	План мероприятий по устранению инцидента информационной безопасности	Группа по расследованию инцидента информационной безопасности	

№ п/п	Наименование этапа/шага процесса	Длительность и начало выполнения	Вход	Выход	Подразделение / Должность	
					Ответственный	Участвует
2.2	Создание служебной записки с планом мероприятий по устранению инцидента информационной безопасности	1 день	План мероприятий по устранению инцидента информационной безопасности	Служебная записка с планом мероприятий по устранению инцидента информационной безопасности	Руководитель группы по расследованию инцидента информационной безопасности	Владелец ИТ-системы
2.3	Подписание служебной записки о плане мероприятий по устранению инцидента информационной безопасности	1 день	Служебная записка о плане мероприятий по устранению инцидента информационной безопасности	Подписанная служебная записка о плане мероприятий по устранению инцидента информационной безопасности	Ведущий специалист по информационной безопасности и защите персональных данных	
3	Проведение мероприятий по устранению инцидента ИТ безопасности					
3.1	Принятие мер по устранению инцидента информационной безопасности	5 дней	Служебная записка с планом мероприятий по устранению инцидента информационной безопасности	Запротоколированные результаты действий по устранению инцидента информационной безопасности	Ведущий специалист по информационной безопасности и защите персональных данных	
3.2	Проведение повторного исследования информационной системы	1 день	Запротоколированные результаты действий по устранению инцидента информационной безопасности	Сведения о текущем состоянии ИТ системы	Группа по расследованию инцидента информационной безопасности	
3.3	Анализ и сопоставление результатов повторного исследования с исходными данными о инциденте	1 день	Сведения о текущем состоянии ИТ системы	Подтверждение устранения инцидента информационной безопасности	Группа по расследованию инцидента информационной безопасности	
3.4	Составление отчёта об инциденте информационной безопасности	1 день	Подтверждение устранения инцидента информационной безопасности	Отчёт о действиях, направленных на устранение инцидента информационной безопасности	Руководитель группы по расследованию инцидента информационной безопасности	Ведущий специалист по информационной безопасности и защите персональных данных

2.2 Продолжительность выполнения процесса

Продолжительность выполнения процесса с момента появления события «Инцидент информационной безопасности» и заканчивая событием «Составление отчёта об инциденте информационной безопасности» равна 14 рабочим дням.

2.3 Расширенное описание процесса

Этап 1. Создание группы по реагированию на инцидент информационной безопасности

Шаг 1.1. Анализ инцидента информационной безопасности

На данном шаге происходит анализ:

– угроз, которые реализует инцидент;

– степени влияния инцидента на бизнес-деятельность Общества;

– финансового ущерба;

– ущерба репутации Общества.

При этом берутся в расчёт:

– область охвата (количество узлов, на которые повлияло данный инцидент);

– степень влияния на узлы – объекты, подверженные инциденту.

При оценке степени риска события информационной безопасности следует руководствоваться Приложением 1 к настоящему Регламенту.

Срок исполнения шага – 1 день.

Шаг 1.2. Назначение руководителя группы по расследованию инцидента

На данном шаге производится назначение руководителя группы по расследованию инцидента информационной безопасности. Руководитель группы назначается из числа сотрудников УБиР.

Срок исполнения шага – 1 день.

Шаг 1.3. Формирование группы по расследованию инцидента

На данном шаге создаётся команда реагирования на инцидент информационной безопасности. Команда реагирования создаётся из числа сотрудников Управления безопасности и режима и ИТ.

Срок исполнения шага – 1 день.

Этап 2. Утверждение служебной записки по устранению инцидента информационной безопасности

Шаг 2.1. Разработка плана мероприятий по устранению инцидента информационной безопасности

На данном шаге происходит разработка плана мероприятий по устранению инцидента. План мероприятий должен включать:

– детальное описание инцидента;

– перечень уязвимых узлов;

– последовательность действий по устранению инцидента или направленных на уменьшение воздействия инцидента;

– перечень действий по оценке влияния этих мероприятий на систему в целом.

Перечень рекомендуемых мероприятий приведён в Приложении 2 к настоящему документу.

На данном шаге производится:

– анализ результатов сканирования ИТ систем, подверженных инциденту информационной безопасности;

– сравнение результатов сканирования от всех средств выявления уязвимостей;

– подтверждение найденных уязвимостей в результате сравнения версий, настроек ПО и ОС, определённых по результатам сканирования и версий, настроек ПО и ОС, фактически используемых в системе.

Срок исполнения шага – 1 день.

Шаг 2.2. Создание служебной записки с планом мероприятий по устранению инцидента информационной безопасности.

На данном шаге происходит подготовка и согласование служебной записки о плане мероприятий по устранению инцидента информационной безопасности. Служебная записка пишется на имя заместителя генерального директора – начальника Управления безопасности и режима. Служебная записка согласуется с владельцем ИТ-системы.

Срок исполнения шага – 1 день.

Шаг 2.3. Подписание служебной записки о плане мероприятий по устранению инцидента ИТ-безопасности

На данном шаге происходит подписание Руководителем по ИБ и ПДИТР УБиР служебной записки о плане мероприятий по устранению инцидента информационной безопасности.

Срок исполнения шага – 1 день.

Этап 3. Проведение мероприятий по устранению инцидента информационной безопасности

Шаг 3.1. Принятие мер по устранению инцидента

После разработки плана действий его необходимо привести в исполнение. При этом следует оценить:

– риск возникновения проблемы совместимости версий программного обеспечения;

– риск появления новых уязвимостей в информационной системе;

– трудоёмкость предварительное тестирование;

Срок исполнения шага – 6 дней.

Шаг 3.2. Проведение повторного исследования информационной системы

На данном шаге происходит проведение повторного исследования информационной системы.

Срок исполнения шага – 1 день с момента подтверждения совместимости исправлений.

Шаг 3.3. Анализ и сопоставление результатов повторного исследования с исходными данными об инциденте информационной безопасности

На данном шаге происходит подтверждение корректности внесённых в ИТ систему исправлений.

Срок исполнения шага – 1 день с момента подтверждения правильности исправлений.

Шаг 3.4. Составление отчета

На данном шаге формируется отчёт об инциденте информационной безопасности. Рекомендуемый формат отчёта приведён в Приложении 4 к настоящему документу.

Отчёт направляется заместителю генерального директора – начальнику Управления безопасности и режима.

Срок исполнения шага — 1 день с момента подтверждения правильности исправлений.

Приложение № 1.
Оценка степени риска события информационной безопасности

Степень риска	Характеристики
1	Единичные попытки сканирования, сбора информации в отношении узлов внутренней сети. Активность со стороны известных вирусов или червей на отдельных (изолированных) узлах.
2	Единичные попытки сканирования, сбора информации в отношении узлов внутренней сети. Попытки использования уязвимости, с большой долей вероятности присутствующей на узлах сети.
3	Большое число попыток сканирования, сбора информации. Неудачная попытка DoS-атаки или «взлома». Контролируемая активность со стороны известных вирусов или червей на значительном числе узлов сети. Активность со стороны новых вирусов или червей на отдельных (изолированных) узлах.
4	Попытка DoS-атаки или «взлома», оказавшая незначительное влияние на отдельные узлы. Частично успешная атака с легко устраняемыми последствиями. Трудно контролируемая активность со стороны известных вирусов или червей на значительном числе узлов сети. Незначительный риск потери репутации или финансовых потерь.
5	Удачная попытка DoS-атаки или «взлома», оказавшая значительное влияние на узлы корпоративной сети. Значительный риск потери репутации или финансовых потерь. Значительное распространение вирусов или червей, с трудом подлежащее контролю.

Приложение № 2.
Действия при обнаружении события информационной безопасности

Степень риска	Действия
1	Запись активности, связанной с инцидентом. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ.
2	Запись активности, связанной с инцидентом. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ. Блокировка взаимодействия с узлом нарушителя.
3	Запись активности, связанной с инцидентом. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ. Блокировка взаимодействия с узлом нарушителя.
4	Запись активности, связанной с инцидентом. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ. Блокировка взаимодействия с узлом нарушителя. Сбор доказательств для проведения расследования.
5	Запись активности, связанной с инцидентом. Обновление узлов, подверженных атаке. Обновление антивирусного ПО, изменение правил фильтрации на МЭ. Блокировка взаимодействия с узлом нарушителя. Сбор доказательств для проведения расследования. Выключение узлов или их изоляция.

Приложение № 3. Отчет об инциденте информационной безопасности

Дата возникновения инцидента	
Тип инцидента	
Описание инцидента	

Описание инцидента:

Контактная информация	
ФИО сотрудника, обнаружившего инцидент	
Подразделение	
Адрес e-mail	
Телефон	
Дополнительная контактная информация	
Объект атаки	
Имя хоста или IP-адрес	
Назначение компьютера (выполняемые функции)	
Источник атаки	
Имя хоста или IP-адрес	
Информирован ли владелец и/или провайдер владельца IP-адреса?	
Описание инцидента	
Дата	
Метод атаки	
Версии ОС и прикладного программного обеспечения на атакованном компьютере	
Использованные уязвимости	
Прочая информация	
Результат анализа	

Анализ инцидента информационной безопасности :

Какие угрозы реализует инцидент	
Степень влияния на бизнес-деятельность	
Финансовый ущерб	
Ущерб репутации Общества	

Описание хронологии инцидента:

Дата, время	Описание характера инцидента на момент времени

Группа расследования инцидента:

№	Должность	ФИО	Контактная информация

Принятые временные меры по уменьшению воздействия инцидента:

Принятые меры	Описание	Дата, время	ФИО сотрудника, принявшего меры

Принятые меры по устранению причин возникновения инцидента:

Принятые меры	Описание	Дата, время	ФИО сотрудника, принявшего меры