RTM GROUP

Важное в защите персональных данных 2023

Уведомления и импортозамещение

Эксперт

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Евгений Царев

Управляющий RTM Group

Эксперт в области информационной безопасности и

ИТ-права (более 15 лет профессионального опыта)

Андрей Гончаров

Юрист в области информационной безопасности

Ведущий консультант по информационной безопасности

Профессиональный опыт в области IT-права с 2015 года

О компании RTM Group

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Работаем на всей территории России, Беларуси и Казахстана, и не ограничиваемся на этом. Головной офис компании находится в Москве, производственное подразделение базируется в Воронеже.

RTM Group ежегодно выполняет сотни проектов, делая свой вклад в стабильность и безопасность киберпространства, а также помогает провести анализ цифровых доказательств для судов и следственных органов.

ПРАВО 300

Входим в рейтинг «Pravo.ru-300» в отрасли Цифровая экономика.

АБИСС

Полноправный член «Ассоциации пользователей стандартов по информационной безопасности»

ТПП РФ

В реестре надежных партнеров торгово-промышленной палаты Российской Федерации

RTM GROUP

О чем пойдет речь

01 Уведомление регуляторов – реализация

02 Состав команды по реагированию

03 Технические средства

04 Какие СЗИ нужны на каждый УЗ? Что ушло, что осталось

05 453 приказ Минцифры

06 Советы

01. Уведомление регуляторов – реализация

1. Уведомление регуляторов – реализация

Все регуляторы создают каналы для оперативной связи с компаниями для получения различной информации в области:

- Отчетности
- Обмена оповещениями и распоряжениями
- Для оповещения в области инцидентов различного характера

1.1 Уведомление регуляторов – реализация

В случае обнаружения факта неправомерного распространения ПДн, оператор обязан направить 2 уведомления (ст. 21 Закона № 152-ФЗ):

1. Посылается в течении 24 часов с момента обнаружения;
2. В течении 72 часов с момента обнаружения.

1.2 Уведомление регуляторов – реализация

Само первичное оповещение должно содержать:

- Наименование оператора, ИНН оператора, адрес оператора
- Дату и время выявления инцидента
- Предполагаемые причины возникновения инцидента
- Описание содержания утекших ПДн
- Предполагаемый вред субъектам ПДн, который оценивается по единой методике оценки вреда (Приказ Роскомнадзора № 178)
- Перечень действий, которые на момент подачи оповещения (т.е. в течении первых 24 часов) уже были сделаны для локализации инцидента
- Дополнительная информация, например: источники получения информации о факте возникновения инцидента, дополнительные вложения
- Контактные данные для обратной связи

1.3 Уведомление регуляторов – реализация

- **Первичное** оповещение должно быть направлено сразу после обнаружения. Даже если вы узнали о своей утечки уже из новостей, его все равно требуется направить
- **Второе** оповещение направляется как дополнение к первому и содержит результаты внутреннего расследования инцидента

После направления оповещения выдается ключ и номер оповещения, с помощью которых в любое время оповещение можно дополнить

1.4 Уведомление регуляторов – реализация

Результаты внутреннего расследования должны содержать:

- Причину возникновения утечки
- Перечень технических недостатков и уязвимостей системы защиты, которые привели к возможности появления утечки
- Ответственных за утечку лиц
- Перечень мероприятий по устранению последствий инцидента
- Дополнительно можно включить сведения о планах по повышению уровня информационной безопасности

Оповещение РКН – это прямая обязанность операторов, указанная в 152-ФЗ, невыполнение которой добавит ответственности при расследовании причин утечки

1.5 Уведомление регуляторов – реализация

Для того чтобы корректно направить оповещение сотрудник должен:

- Знать перечень процессов компании и какие конкретно в них обрабатываются базы ПДн
- Знать содержание баз данных ПДн или иметь быстрый доступ к этому перечню
- Знать этапы реагирования на инциденты

1.6 Уведомление регуляторов (подводные камни)

На текущий момент обмен информацией об инцидентах производится через:

- Госсопку
- Электронные формы на сайте РКН
- ПО Банка России

02. Состав команды по реагированию

2. Состав команды по реагированию

Процесс реагирования на инциденты ИБ зависит от 2 факторов:

1. Зрелость системы менеджмента инцидентов
2. Функциональные возможность автоматизированных систем по реагированию на инциденты

Зрелость системы менеджмента – это компетенция сотрудников, наличие стандартных процедур реагирования, а также их фактическая результативность

2.1 Состав команды по реагированию

Реагирование должно приводить к следующим результатам:

- Определение причин возникновения и нарушителя
- Определение недостатков систем обработки информации и защиты информации
- Определение дальнейших решений по недопущению повторной утечки

2.2 Состав команды по реагированию

1. **Политика менеджмента инцидентов, в которую входят:**
    - Задачи и цели различных мероприятий по реагированию
    - Полномочия и обязанности сотрудников при реагировании
    - Описание правил взаимодействия различных отделов при возникновении инцидентов
2. **Методический материал для обучения сотрудников**
3. **Порядок тестирования самой системы по реагированию**

2.3 Состав команды по реагированию

Стандарты по реагированию на инциденты, в которых описываются все мероприятия, которые необходимо проводить для быстрого реагирования:

- ГОСТ 57580.1 Процесс 6
- ГОСТ 18044-2007
- ГОСТ Р ИСО МЭК 27002-2021
- ISO IEC 27035-3 2022
- ГОСТ Р 59709-2022
- ГОСТ Р 59710-2022
- ГОСТ Р 59711-2022
- ГОСТ Р 59712-2022

03. Технические средства

3. Технические средства

Технические средства защиты в рамках инцидентов выполняют следующие функции:

- Функции проактивной защиты, которые предотвращают утечки
- Функции обнаружения, расследования и журналирования
- Функции по защите информации

3.1 Технические средства: IRP

IRP-системы – предоставляет функционал для автоматизированного реагирования, а также функционал для автоматизации различных процедур.

IRP имеет следующий функциона:

- Обнаружение инцидента на основании признаков корреляции
- Исключение ложноположительных срабатываний
- Восстановление данных из резервных копий
- Оповещение ответственных лиц
- Составление стандартизированных отчетов

3.2 Технические средства: SOAR

SOAR-системы – обеспечивает оркестрацию всех средств защиты.

SOAR имеет следующий функционал:

- Обнаружение инцидента на основании признаков корреляции
- Идентификация и классификация угроз
- Удаленное управление средствами защиты
- Составление стандартизированных отчетов

3.3 Технические средства: Playbook

Помимо зрелых рыночных решений, могут применяться и самописные скрипты и алгоритмы.

Несертифицированные СЗИ применять для защиты ПДн запрещено

04. Какие СЗИ нужны на каждый УЗ? Что ушло, что осталось

4. Какие СЗИ нужны на каждый УЗ? Что ушло, что осталось

Требования				Решение
4-уз	3-уз	2-уз	1-уз	
Разграничение доступа				Доменная сеть
Контроль состава программного обеспечения				Средства доверенной загрузки
-		Защита машинных носителей и контроль переноса информации на машинные носители		DLP (Data Loss Prevention) – блокирование каналов передачи, контентный анализ, теневое копирование и пр.
Регистрация событий защиты				SIEM (Security information and event management) – система централизованного сбора логов. Сопрягается со всеми иными средствами защиты.
Антивирусная защита				Антивирусные средства (все)
-	-	Защита от сетевых атак		IPS/IDS (Intrusion prevention/Detection System) – мониторинг сетевого трафика, оповещение о сетевых атаках. У IPS – проактивная защита от сетевых атак
-	Поиск уязвимостей, контроль обновлений			Сканер уязвимостей
-	-	Целостность программного обеспечения + защита от спама, технологические меры		Антивирусы + DLP (Data Loss Prevention) – блокирование каналов передачи, контентный анализ, теневое копирование и пр.
-	-	Резервирование данных и инфраструктуры		Системы резервного копирования

4.1 Средства защиты вычислительной сети

- UTM решения
- Межсетевые экраны
- IPS/IDS системы
- Прокси
- VPN
- Иные выполняющие их функции продукты

4.2 Средства защиты вычислительной сети

Ушедшие решения:

- Cisco
- Fortigate

Доступные решения:

- Traffic Inspector Next Generation
- ViPNet
- BI.ZONE WAF
- Комплекс безопасности «Континент»
- Usergate
- Checkpoint

4.3 Антивирусные средства

Ушедшие решения:

- ESET

Доступные решения:

- Kaspersky
- Dr. WEB

По данным Коммерсантъ доля лидера рынка антивирусных средств— «Лаборатории Касперского» — выросла до 94% в штучном выражении в 2023 против 80% годом ранее

4.4 Разграничение доступа

- Avanpost IDM
- Active directory
- Функции линукс
- Соболь
- Secret NET

Контроллер Windows AD в совокупности с дополнительными службами могут обеспечить выполнение всех требований по разграничению доступа, однако потребуются дополнительные ТСЗИ для контроля целостности ПО и ОС

4.5 DLP

DLP системы защищают одновременно от умышленных сливов информации внутренним нарушителем, утечек по неосторожности или халатности, а также блокируют каналы утечки, по которым внешний нарушитель может вывести данные из инфраструктуры.

Ушедшие решения:

- DLP Zecurion
- DLP DeviceLock

Доступные решения:

- Стахановец
- InfoWatch Traffic Monitor
- Solar Dozor

4.6 SIEM

На отечественном рынке можно наблюдать следующие решения:

- RuSIEM
- Ankey SIEM
- MaxPatrol SIEM
- KOMRAD Enterprise SIEM

4.7 Сканеры уязвимостей

Сканеры уязвимостей – это незаменимый инструмент для периодических внутренних проверок защищенности.

В основном компании пользуются следующими сканерами:

- Maxpatrol
- Xspider
- Сканер-ВС

Все сканеры оперируют единой общей базой CWE, в которой как раз и собрана информация об уязвимостях. Основное направление развития таких средств – это расширение функциональных возможностей по устранению уязвимостей и пользовательского интерфейса

4.8 Гипервизоры

Ушедшие решения:

- VMware

Доступные решения:

- Numa vServer
- ROSA Virtualization

4.9 Замена зарубежных решений

Практически в каждой компании есть неподдерживаемые или несертифицированные СЗИ. С точки зрения законодательства их использование недопустимо, однако это все еще лучше, чем не защищать информацию вовсе.

Пример: Введение нового ПО – это хорошая возможность пересмотреть требования к функционалу этого ПО СЗИ, не может ли это или подобные решения выполнять дополнительные функции, которые ранее не были интегрированы.

Также, ввод новой системы – это повод провести инвентаризацию в своей инфраструктуре, нарисовать топологию, пересмотреть требования политики защиты и прочее.

Касательно требований к защите ПДн, можно обратиться к чек-листу, по которому производятся все плановые проверки, к мерам 21 приказа ФСТЭК.

05. 453 приказ Минцифры

5. 453 приказ Минцифры

Согласно новому приказу, аудит по ГОСТ 57580.1 для сегмента ЕБС проводится не раз в год, а **раз в 2 года**.

Основное нововведение – это требование по **ежегодному аудиту системы защиты персональных** данных для организаций, которые обрабатывают биометрию в целях аутентификации клиентов.

- МФЦ
- Банки
- Гос.органы
- Операторы региональных центров ЕБС

5.1 453 приказ Минцифры

- Все перечисленные организации, обрабатывающие биометрические персональные данные с целью аутентификации клиентов, обязаны проводить оценку соответствия требованиям по защите персональных данных по **21 приказу ФСТЭК**.

- Согласно требованиям 453 приказа, такая оценка должна проводиться **ежегодно** и с привлечением **лицензиата ФСТЭ**К в области технической защиты конфиденциальной информации.

- Привлекаемые компании должны иметь **лицензию** по видам работ б) д) и е) пункта 4 постановления правительства **РФ от 03.02.2012 №79**.

06. Советы для начала построения системы защиты ПДн

6. Советы для начала построения системы защиты ПДн

- Назначить ответственных лиц
- Ввести в действие политику обработки и защиты ПДн
- Провести инвентаризацию информационных активов и определить перечень ИСПДН
- Определить уровень защищенности ПДн
- Выбрать меры защиты ПДн в соответствии с определённым уровнем защищенности ПДн
- Составить дорожную карту совершенствования системы защиты ПДн

Данный перечень – обязательный минимум для старта построения корректной защиты ПДн, которые обрабатывает ваша Организация

RTM GROUP

Мероприятия

@it_law_security

Вебинар: Как белые хакеры помогают защититься от реальных угроз

19 сентября в 12:00

Вебинар: 757-П — новые требования для НФО от ЦБ

21 сентября в 12:00

Конференция: IT. Право. Безопасность. Online 2023

28 сентября в 10:00

Спасибо за внимание!

Готовы ответить на Ваши вопросы


+7 (495) 197-64-95


info@rtmtech.ru


https://rtmtech.ru


@RTM_Group


rtm.group


it_law_security