ГРУППА ЧТПЗ

Организация работы по противодействию утечкам информации с использованием DLP систем: кейсы и экономика

2020 год

Гусляев Георгий Александрович

ПРЕДПОСЫЛКИ ВНЕДРЕНИЯ DLP СИСТЕМЫ. ЧТО ЗАЩИЩАЕМ?

DATA LEAK PROTECTION или DATA LEKAGE PROTECTION - Предотвращение утечек информации, подлежащей защите, из корпоративной сети.

Что защищаем?

- ➢ Сведения составляющие коммерческую тайну
- ➢ Служебная тайна
- ➢ Секрет производства (Ноу-Хау)
- ➢ Сведения составляющие банковскую тайну
- ➢ Персональные данные
- ➢ И прочее и прочее (~50 видов)

Что важно защитить?

- Информацию, которая является для нас ценной и ее разглашение может нанести ущерб Обществу.
- Выполнить требования законодательства по защите информации.

ВЫСТРАИВАНИЕ ПРОЦЕССА ПРОТИВОДЕЙСТВИЯ УТЕЧКАМ

1.Определяем информацию, которую необходимо защищать.

2. Определяем, информационные активы в которых содержится информация подлежащая защите, регулируем доступ к ним.

ВЫСТРАИВАНИЕ ПРОЦЕССА ПРОТИВОДЕЙСТВИЯ УТЕЧКАМ

3. Определяем потенциальные каналы утечки информации.

Печать

Почта

IM

Облачные хранилища

СНИ

FTP

Интернет

4. Защищаемая информация должна всегда находится в пределах контролируемой зоны.

NGFW

Интеграция с межсетевым экраном

ВЫСТРАИВАНИЕ ПРОЦЕССА ПРОТИВОДЕЙСТВИЯ УТЕЧКАМ

5. Защищаемая информация должна иметь метку, для возможности ее идентификации DLP системой.

6. Классифицируем инциденты и настраиваем контрольные политики в DLP системе.

Что дальше?

ОРГАНИЗАЦИЯ РАБОТЫ. ОРГАНИЗАЦИОННО – РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ.

Правила работы пользователей

- ✓ Порядок работы пользователей в сети интернет;
- ✓ Порядок хранения и использования съемных носителей информации;
- ✓ Порядок использования электронной почты;
- ✓ Порядок работы в ЛВС Общества;
- ✓ и пр.

ОРГАНИЗАЦИЯ РАБОТЫ. ОРГАНИЗАЦИОННО – РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ.

Минимальные требования

- В ОРД регулирующих работу пользователей в ЛВС компании необходимо прописать:
  - ✓ Сотрудники обязаны использовать информационные ресурсы Общества и переданные Обществом в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения служебных обязанностей;
  - ✓ Обществом осуществляется контроль использования информационных ресурсов Общества, а также контроль использования технических средств обработки, хранения и передачи информации.

ВАЖНО!!! – с ОРД **под роспись** должны быть ознакомлены все сотрудники компании.

На пример, если речь идет о *Порядке работы с электронной почтой,* то у нас прописано:

Общество оставляет за собой право доступа к электронным сообщениям работников с целью их архивирования и централизованного хранения, а также мониторинга выполнения требований настоящего положения.

- Для официального использования результатов работы DLP системы рекомендуется издать приказ о ее введении в промышленную эксплуатацию.

ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА ПО УСТАНОВЛЕНИЮ РЕЖИМА КТ

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА ПО УСТАНОВЛЕНИЮ РЕЖИМА КТ

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, указанных мер.

Пример отказа в возбуждении уголовного дела: В ходе проведения проверки установлено, что документы, выполненные на листе бумаги, не содержат грифа «Коммерческая тайна» с указанием обладателя такой информации, в связи с чем режим коммерческой тайны считается не установленным, а значит права обладателя информации, составляющей коммерческую тайну, не возникли.

ОТВЕТСТВЕННОСТЬ

Корпоративная (дисциплинарная)

- Замечание
- Выговор
- Увольнение

Уголовная

ст. 183 УК РФ. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.
ст. 137 УК РФ Нарушение неприкосновенности частной жизни

ОТВЕТСТВЕННОСТЬ
ДАННЫЕ СТАТИСТИКИ ЗА 2019 ГОД

Показатель	Осуждено	Оправдано	Лишение свободы	Условное лишение свободы	Ограничение свободы	Штраф	Исправительные работы	Обязательные работы	Принудительные меры к невменяемым
Статья 183 часть 1 УК РФ	2	1	0	0	0	0	1	0	7
Статья 183 часть 2 УК РФ	7	0	0	1	0	2	2	0	10
Статья 183 часть 3 УК РФ	32	0	0	20	0	9	2	0	14
Статья 183 часть 4 УК РФ	0	0	0	0	0	0	0	0	0

ЭФФЕКТЫ

Case №1

Утечка конструкторской документации (собственные разработки)

Оценка ущерба:

- Количество работников * Период * Заработная плата
- Упущенная выгода

Информация отнесена к сведениям составляющим КТ, подаем заявление в полицию по 183 УК РФ.

ОАО "Альметьевский трубный завод"

СЕРТИФИКАТ КАЧЕСТВА № 466

Цех/ Дата выдачи: 14.02.08 Заказ/договор № 210 Вагон: 65499007

Грузополучатель: Ст. назначения:

и его адрес: Инкоты:

Наименование продукции: Трубы стальные электросварные

1. Сведения по трубам

№ п/п	Сорт	Марка стали	Размеры, мм: диаметр	Размеры, мм: толщ. стенки	Размеры, мм: длина	Масса нетто, кг: масса	Масса нетто, кг: нарезка	НТД
1	-	20	219	5,8	10	1008,86	0	10,417 ГОСТ 10705-80 Ч. 1
2	-	20	219	6,5	11	1130,01	0	28,43 ГОСТ 10705-80 Ч. 1
				ИТОГО	21	2138,87		38,847

2. Химический состав, %

№ п/п	Марка стали	C	Mn	Si	S	P	Примечание: метод
1	20 ГОСТ	0,18	0,65	0,17	0,012	0,012	ПОЗ
2	20 ГОСТ	0,18	0,65	0,17	0,012	0,012	ПОЗ
3	20 ГОСТ	0,20	0,70	0,18	0,014	0,021	ПОЗ
4	20 ГОСТ	0,20	0,70	0,18	0,014	0,021	ПОЗ

3. Механические свойства и технологические испытания

№ п/п	Дата	№ пл.	Предел прочности, кгс/мм2	Предел текучести, кгс/мм2	Относительное удлинение, %	Ударная вязкость, кгс/см2	Сплющивание	Раздача	Гидравлическое давление, кгс/см2
1	12.08	10	44	31	33	85	н.п.	Н.Р.	1,5
2	12.08	12	44	40	31	85	н.п.	Н.Р.	1,5
3	12.08	11	44	40	31	100	н.п.	Н.Р.	2,0
4	12.08	11	44	40	31	100	н.п.	Н.Р.	2,0

С дополнительным требованием:

- ОСТЬ неразрушающий контроль сварного соединения и основного металла трубы
- Сталь 20 - 10 Г2 ГОСТ 8731-74, ГОСТ 1050-88

Продукция сертифицирована в системе ГОСТ Р.

Система менеджмента качества сертифицирована на соответствие требованиям ИСО 9001:2000.

При перепечатке по вопросам качества ссылаться на номер сертификата качества

Тел.(8553) 26-08-00

Начальник ОТК Сертификатчик

Case №2

Несанкционированная передача сертификатов качества на трубную продукцию организациям занимающимся оборотом б/у и восстановленной трубной продукции

Оценка ущерба:

- Стоимость трубной продукции указанной в сертификате
- Упущенная выгода

Информация отнесена к сведениям составляющим КТ, подаем заявление в полицию по 183 УК РФ.

ЭФФЕКТЫ

Case №3
Утечка клиентской базы и информации по заказам
Оценка ущерба:

- Оценить сложно

Информация о клиентах и информация о их потребностях позволяет посредникам или конкурентам перехватывать клиентов, как следствие – снижение Выручки, снижение объемов продаж и т.д. (влияние на годовые показатели деятельности предприятия)

Case №4
Утечка персональных данных
Оценка ущерба:
Для общества – минимальный, у нас не GDPR
Для работника – административный штраф, либо лишение свободы на срок до 4 лет (ст. 137 УК РФ)

МАКСИМАЛЬНЫЙ ЭФФЕКТ
MONEY LOSS PREVENTION

Проведение расследований по инцидентам:

- Выявление взаимосвязей между фигурантами;
- Построение событийных графов получения информации фигурантами и принятия ими решений;
- Формирование массива данных, подтверждающего факт нарушения

Активный мониторинг. Выявление коррупционных признаков:

- Выявление признаков нарушения и аффилированности на этапе заключения сделок;
- Выявление фактов формирования мнимой конкурентной среды при проведении ТЗП;
- Обнаружение признаков подготовки закупочной процедуры под конкретного поставщика.

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ (АВТОМАТИЗИРОВАННЫЙ ПРОФАЙЛИНГ)

ГРУППА ЧТПЗ

Спасибо за внимание!

Вопросы?