В ТК ТС нет выделения основных формы таможенного контроля. Ст. 110 называет формы таможенного контроля, к которым относятся: 1) проверка документов и сведений; 2) устный опрос; 3) получение объяснений; 4) таможенное наблюдение; 5) таможенный осмотр; 6) таможенный досмотр; 7) личный таможенный досмотр; 8) проверка маркировки товаров специальными марками, наличия на них иденти 10) учет товаров, находящихся под таможенным контролем; 11) проверка системы учета товаров и отчетности по ним; 12) таможенная проверка.

Одинаковым является то, что при проведении таможенного контроля таможенные органы Таможенного союза, как и таможенные органы ЕС исходят из принципа выборочности и, как правило, ограничиваются только теми формами таможенного контроля, которые достаточны для обеспечения соблюдения таможенного законодательства таможенного союза и законодательства государств-участников таможенного союза, контроль за исполнением которого возложен на таможенные органы. При выборе объектов и форм таможенного контроля используется система управления рисками.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ РЕГУЛИРОВАНИЯ ПРАВОВЫХ ОТНОШЕНИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ТАМОЖЕННОГО СОЮЗА В РАМКАХ ЕВРАЗЭС

Сомов Ю.И., Российская таможенная академия, РФ

Актуальность – при создании Таможенного союза возникает необходимость в обмене информацией. Но когда дело касается конфиденциальной информации у объединяющихся сторон возникают определённые трудности: какой информацией можно делиться, как осуществлять допуск к ней, как будет обеспечиваться защита пользователями, какой возможен контроль и какая будет ответственность за нарушения безопасности информации в случае, когда у этой конфиденциальной информации предполагается несколько владельцев. В докладе будет представлен определённый взгляд на то, как решить эти проблемы, обеспечив устойчивое функционирование союза.

Порядок проведения исследований с целью определения основ правового регулирования отношений сторон, заключающих союз:

1. Моделирование ситуации объединённого конфиденциального информационного пространства.
2. Определение условий устойчивого состояния системы обмена конфиденциальной информацией.
3. Определение порядка вступления субъектов в объединённое конфиденциальное информационное пространство.

Моделирование

Наиболее значащими объектами системы (рис. 1) являются:

владелец информации;

информация;

«злоумышленник».

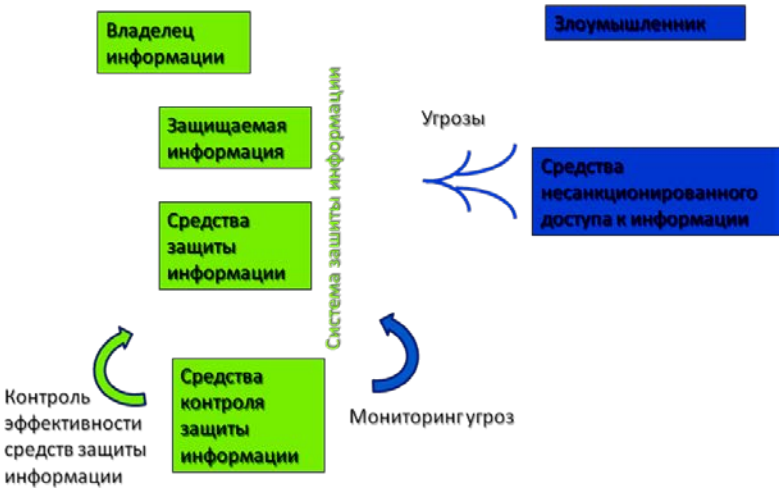

Рис. 1. Простая система защиты информации

Необходимо исследование особенностей каждого элемента и его связей с другими элементами.

В нашем случае определяется заинтересованность владельца информации защищать свои конфиденциальные сведения от доступа к ним «злоумышленников».

Показателем эффективности системы может быть выгода владельца информации от её применения для удовлетворения своих потребностей с учётом затрат. Если, например, выразить выгоду,

пользу от применения информации и затраты в деньгах, то можно записать формулу:

Выгода = Польза – Затраты.

Для информации исследуется способность удовлетворять потребности её владельца. Ценность конфиденциальности информации определяется ценностью потребляемого конкурентного ресурса (рис. 2).

Для случая, когда требуется совместное потребление конкурентного ресурса (рис. 3) и защиты его от «злоумышленников», объединяющиеся субъекты должны заключать между собой соответствующие договоры.

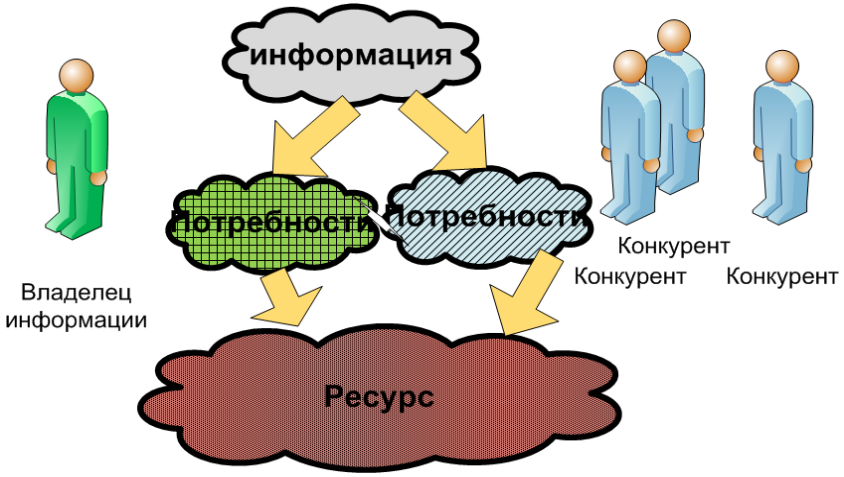

Рис. 2. Определение ценности конфиденциальности информации методом конкурентного ресурса

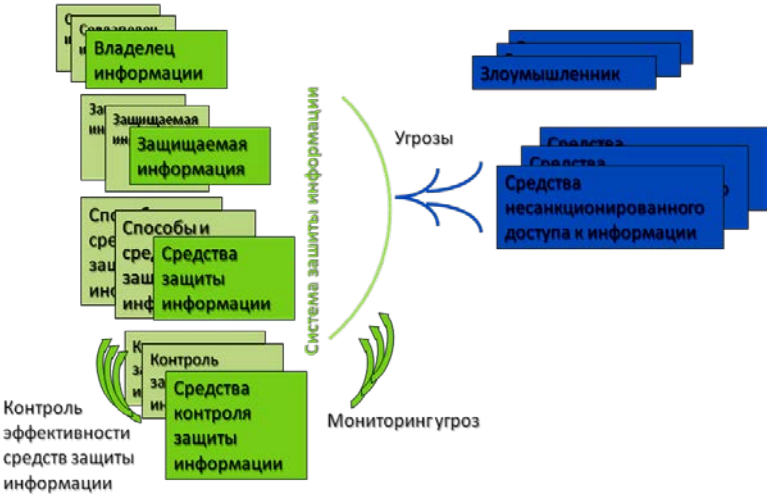

Рис. 3. Система защиты информации при множестве её владельцев

При заключении договоров об обмене конфиденциальной информацией необходимо определить решение следующих вопросов:

- определение единого подхода к отнесению информации к конфиденциальной и степень её конфиденциальности (создание перечней сведений, которые необходимо относить к конфиденциальным);
- определение общей модели угроз информационной безопасности;
- определение общих норм и требований по защите информации, в том числе относящихся к техническим средствам и системам;
- организация допуска сотрудников к общим конфиденциальным сведениям и к конфиденциальным (секретным) технологиям и средствам защиты информации;
- разработка (принятие) общих стандартов в области информационного взаимодействия и информационной безопасности;
- определение порядка проведения контроля выполнения и эффективности приятых мер по защите информации;
- определение общих правил ответственности за сохранность конфиденциальности информации;
- организация финансирования защиты информации.

Условия устойчивого состояния системы.

Система будет устойчивой при условии единого владельца информации (это может быть совместно созданный объединяющимися сторонами орган), который будет одинаково («равномерно») организовывать защиту информации от угроз по всему «периметру» и будет обеспечивать справедливость распределения ресурса между его потребителями. Этот владелец будет осуществлять допуск пользователей к конфиденциальной информации, определять порядок контроля и ответственности за нарушение требований её безопасности. В условиях использования современных информационно-телекоммуникационных систем такой владелец информации может быть верхним в иерархии удостоверяющим центром при применении объединёнными сторонами ЭЦП при документообмене.

Порядок вступления субъектов в объединённое конфиденциальное информационное пространство

Правовое регулирование отношений сторон, объединивших свое конфиденциальное информационное пространство, должно осуществляться соглашением, которым определяются условия устойчивого состояния системы.

Основные принципы принятия субъектов в объединение:

Порядок вступления новых субъектов в объединение не должен нарушать его стабильности.

Гарантией вступления нового члена может служить его залог, покрывающий возможный убыток других членов объединения при возникновении неисполнения им обязательств.

Возможно поэтапное вхождение нового члена в объединение, по мере его соответствия рамочным требованиям.

Возможно кредитование системы защиты информации более слабого члена объединения (быть может с применением страховых инструментов).

Приведённые выше рассуждения для абстрактной модели могут быть использованы при разработке соглашений в области защиты информации при создании Таможенного союза ЕврАзЭС.