



---

**Европейская экономическая комиссия**

Комитет по внутреннему транспорту

**Рабочая группа по таможенным вопросам,  
связанным с транспортом**

Группа экспертов по правовым аспектам компьютеризации процедуры МДП

Третья сессия

Женева, 16 и 17 мая 2017 года

Пункт 4 предварительной повестки дня

**Идентификация держателя и проверка целостности  
электронных сообщений для обмена данными**

**Идентификация держателя и проверка целостности  
электронных сообщений для обмена данными**

**Представлено правительством Российской Федерации\***

---

\* В данном документе воспроизводится без изменений текст, переданный секретариату.

## I. Актуальные угрозы информационной безопасности (при автоматизированной обработке)

<i>Угроза</i>	<i>Атака</i>	<i>Время проведения атаки</i>	<i>Объект атаки (местоположение атакуемого)</i>	<i>Субъект атаки (местоположение атакующего)</i>	<i>Код угрозы</i>
Модификация электронных документов (ЭД)	Изменение ПО	Вне процесса функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И1
			Почтовый сервер	Любая станция ЛВС → Сервер (через LOGIN SCRIPT) Почтовый сервер	
	Неправильный ввод ЭД	В процессе функционирования системы	Сервер	Любая станция ЛВС	И2
			Любая станция ЛВС	Эта же станция ЛВС	
Ввод несуществующего ЭД	Внедрение программной закладки	В процессе функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И3
			Почтовый сервер	Любая станция ЛВС → Сервер (через LOGIN SCRIPT) Почтовый сервер	
	Перехват ЭД	В процессе функционирования системы	Сервер	Любая станция ЛВС	И4
			Сервер	Любая станция ЛВС	
Изменение ПО	В процессе передачи данных	В процессе функционирования системы	Сеть передачи данных	Промежуточные узлы	И5
			Модем	Промежуточные узлы	
	Внедрение программной закладки	Вне процесса функционирования системы	В процессе функционирования системы	Любая станция ЛВС	Эта же станция ЛВС
Почтовый сервер				Любая станция ЛВС → Сервер (через LOGIN SCRIPT) Почтовый сервер	
Внедрение программной закладки	В процессе функционирования системы	В процессе функционирования системы	Сервер	Любая станция ЛВС	И3
			Любая станция ЛВС	Эта же станция ЛВС Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	

<i>Угроза</i>	<i>Атака</i>	<i>Время проведения атаки</i>	<i>Объект атаки (местоположение атакуемого)</i>	<i>Субъект атаки (местоположение атакующего)</i>	<i>Код угрозы</i>	
Нарушение конфиденциальности ЭД	«Ручной ввод»	В процессе функционирования системы	Почтовый сервер	Почтовый сервер	И6	
			Сервер Сервер Почтовый сервер	Любая станция ЛВС Любая станция ЛВС Любая станция ЛВС Почтовый сервер		
	Изменение ПО	В процессе передачи данных Аналогично предыдущему случаю	ЛВС	Любая станция ЛВС	И7	
			Сеть передачи данных Модем	Промежуточные узлы Промежуточные узлы		
	Внедрение программной закладки	Просмотр с экрана	В процессе функционирования системы	Любая станция ЛВС	Любая станция ЛВС	И8
				Почтовый сервер	Почтовый сервер	
	Перехват ЭД	В процессе функционирования системы	В процессе функционирования системы	ЛВС	Любая станция ЛВС	И4
				Сеть передачи данных Модем	Промежуточные узлы	И5
				Сервер	Любая станция ЛВС	И9
	Несанкционированное копирование	Вне процесса функционирования системы	В процессе функционирования системы	Любая станция ЛВС	Любая станция ЛВС	И3
Почтовый сервер				Почтовый сервер		
Отказ от факта получения ЭД	Изменение ПО	В процессе передачи данных Аналогично предыдущему случаю	Внешний тамож. орган	Внешний тамож. орган	И10	
			Почтовый сервер	Почтовый сервер		
Отказ от авторства ЭД Дублирование ЭД	Изменение ПО	Аналогично предыдущему случаю	Внедрение программной закладки	Аналогично предыдущему случаю	И16	
					И16	

<i>Угроза</i>	<i>Атака</i>	<i>Время проведения атаки</i>	<i>Объект атаки (местоположение атакуемого)</i>	<i>Субъект атаки (местоположение атакующего)</i>	<i>Код угрозы</i>
Потеря или уничтожение ЭД	«Повтор в сети»	В/Вне процесса функционирования системы	Сервер ЛВС Сеть передачи данных Модем	Любая станция сети Любая станция сети Промежуточные узлы	И12
	Перехват ЭД	В процессе функционирования системы	Сервер ЛВС Сеть передачи данных Модем	Любая станция сети Любая станция сети Промежуточные узлы	И4
	Несанкционированное копирование	Вне процесса функционирования системы	Сервер	Любая станция ЛВС	И9
	Изменение ПО	Аналогично предыдущему случаю			И11
НСД к АРМ системы электронного документооборота	Внедрение программной закладки				
	НСД	В/Вне процесса функционирования системы	Любая станция ЛВС Почтовый сервер Сервер Любая станция ЛВС	Эта же станция ЛВС Любая станция ЛВС → Сервер (через LOGIN SCRIPT) Почтовый сервер Любая станция ЛВС Любая станция ЛВС	И13
НСД к каналу передачи данных	НСД к каналу	В процессе функционирования системы	Любая станция ЛВС	Из внешней сети (Internet) Любая станция сети	И14
		В процессе передачи данных	Сеть передачи данных Модем	Промежуточный узел	И15
Нападение из внешней сети	Атака из внешней сети	В/Вне процесса функционирования системы	Сервер Станция сети Модем Маршрутизатор		И18

<i>Угроза</i>	<i>Атака</i>	<i>Время проведения атаки</i>	<i>Объект атаки (местоположение атакуемого)</i>	<i>Субъект атаки (местоположение атакующего)</i>	<i>Код угрозы</i>
Нарушение работоспособности процесса функционирования системы	Изменение ПО, изменение конфигурации аппаратных средств, внедрение программных закладок	В/Вне процесса функционирования системы	На всех технологических участках	На всех технологических участках	И17
Несанкционированное конфигурирование маршрутизаторов	Несанкционированное конфигурирование маршрутизаторов	В/Вне процесса функционирования системы	Маршрутизаторы	Любая станция сети передачи данных	И18

## II. Меры защиты от реализации угроз

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
И1	<ol style="list-style-type: none"> <li>1. Инструкция по внесению изменений в конфигурации ПО</li> <li>2. Инструкции пользователям</li> <li>3. Задание ответственности за нарушение установленных правил</li> <li>4. Инструкция по изменению полномочий пользователей</li> </ol>	<ol style="list-style-type: none"> <li>1. Разграничение доступа в помещения</li> <li>2. Физическая защита помещений</li> </ol>	<ol style="list-style-type: none"> <li>1. Запрет загрузки АРМ с гибких магнитных дисков</li> <li>2. Защита исполняемых файлов от изменения</li> <li>3. Замкнутая среда разрешенных для запуска программ для каждого пользователя системы</li> <li>4. Периодический контроль целостности исполняемых файлов и настроек программных средств</li> <li>5. Использование ЭЦП</li> <li>6. Регистрация событий</li> </ol>
И2	<ol style="list-style-type: none"> <li>1. Двойной контроль при вводе документов</li> <li>2. Контроль прохождения документов</li> <li>3. Инструкции пользователям</li> <li>4. Задание ответственности за нарушение установленных правил</li> </ol>	Нет	<ol style="list-style-type: none"> <li>1. Двойной контроль при вводе (при помощи ПО)</li> <li>2. Контроль прохождения документов (при помощи ПО)</li> <li>3. Регистрация событий</li> </ol>
И3	<ol style="list-style-type: none"> <li>1. Инструкция по внесению изменений в конфигурации ПО</li> <li>2. Инструкции пользователям</li> <li>3. Задание ответственности за нарушение установленных правил</li> </ol>	<ol style="list-style-type: none"> <li>1. Разграничение доступа в помещения</li> <li>2. Физическая защита помещений</li> </ol>	<ol style="list-style-type: none"> <li>1. Запрет загрузки АРМ с гибких магнитных дисков</li> <li>2. Защита исполняемых и системных файлов от изменения</li> <li>3. Замкнутая среда разрешенных для запуска программ для каждого пользователя системы</li> <li>4. Периодический контроль целостности системы</li> <li>5. Регистрация событий</li> <li>6. Использование средств обнаружения нарушений</li> </ol>
И4	<ol style="list-style-type: none"> <li>1. Инструкция по внесению изменений в конфигурации ПО</li> <li>2. Инструкции пользователям</li> <li>3. Задание ответственности за нарушение установленных правил</li> <li>4. Инструкция по изменению полномочий пользователей</li> </ol>	<ol style="list-style-type: none"> <li>1. Разграничение доступа в помещения</li> <li>2. Физическая защита помещений</li> </ol>	<ol style="list-style-type: none"> <li>1. Ограничение доступа к серверу по номеру сетевой карты</li> <li>2. Разрешение доступа к серверу только с защищенных рабочих станций</li> <li>3. Запрет одновременного доступа к серверу пользователей с одинаковым именем</li> <li>4. Преобразование информации</li> <li>5. Защита консоли сервера</li> <li>6. Регистрация событий</li> <li>7. Использование средств обнаружения нарушений</li> </ol>

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
И5	1. Договор с внешней организацией	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Преобразование информации 2. Использование ЭЦП 3. Контроль времени
И6	1. Инструкция по изменению полномочий пользователей 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил	1. Изоляция защищаемой системы от других систем	1. Ограничение доступа к ПК, серверу и т.п. 2. Разрешение доступа к серверу только с защищенных рабочих станций 3. Ограничение доступа к серверу по номеру сетевой карты 4. Запрет одновременного доступа к серверу пользователей с одинаковым именем 5. Регистрация событий 6. Использование средств обнаружения нападений
И7	1. Договор с внешней организацией	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Использование ЭЦП 2. Преобразование информации 3. Квотирование 4. Контроль времени
И8	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Хранитель экрана 2. Ограничение доступа к ПК 3. Разграничение доступа к ПК
И9	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Ограничение доступа к серверу по номеру сетевой карты 2. Разрешение доступа к серверу только с защищенных рабочих станций 3. Запрет одновременного доступа к серверу пользователей с одинаковым именем 4. Преобразование информации 5. Защита консоли сервера 6. Регистрация событий 7. Использование средств обнаружения нападений
И10	1. Договор с внешней организацией 2. Ведение архивов ЭД	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Регистрация событий 2. Использование ЭЦП

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
И11	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Изоляция защищаемой системы от других систем	1. Ограничение доступа к ПК 2. Разграничение доступа к ПК 3. Регистрация событий 4. Использование средств обнаружения нападений
И12	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил 3. Ведение архивов ЭД	1. Изоляция защищаемой системы от других систем	1. Квотирование 2. ЭЦП 3. Контроль времени 4. Регистрация событий
И13	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил 3. Инструкция по использованию СЗИ от НСД 4. Ограничение людей, имеющих право конфигурировать маршрутизаторы	1. Разграничение доступа в помещения 2. Физическая защита помещений 3. Изоляция защищаемой системы от других систем	1. Ограничение доступа к ПК, серверу 2. Разграничение доступа пользователей к ПК, серверу 3. Регистрация событий 4. Хранитель экрана 5. Изменение стандартного имени администратора системы защиты 6. Разрешение работы в сети только одного администратора системы защиты или администратора сети 7. Владелец всех исполняемых файлов в системе, а также критических настроек должен быть администратор системы защиты 8. Использование средств обнаружения нападений 9. Использование межсетевых экранов Использование антивирусных программ 10. Использование всех встроенных в маршрутизаторы средств защиты
И14	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Защита кабельной системы	1. Применение средств криптографической защиты информации
И15	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Защита кабельной системы	1. Применение средств криптографической защиты информации
И16	1. Инструкции пользователям 2. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Ограничение доступа к архиву ЭД 2. Резервное копирование 3. Использование антивирусных программ



<i>Код угрозы</i>	<i>Меры защиты</i>		
	<i>Организационные</i>	<i>Физические</i>	<i>Технические</i>
И17	Все меры	Все меры	Все меры
И18	<ol style="list-style-type: none"> <li>1. Инструкция по использованию каналов передачи данных</li> <li>2. Договор с внешней организацией</li> <li>3. Инструкции пользователям</li> <li>4. Задание ответственности за нарушение установленных правил</li> </ol>		<ol style="list-style-type: none"> <li>1. Ограничение числа используемых каналов передачи данных</li> <li>2. Физическая изоляция ПК для доступа в глобальные сети от АРМ системы ЭД</li> <li>3. Ограничение доступа к ПК, имеющим модемы</li> <li>4. Регистрация событий</li> <li>5. Использование средств обнаружения нападений</li> <li>6. Использование межсетевых экранов</li> <li>7. Использование всех встроенных в маршрутизаторы средств защиты</li> </ol>

ЛВС – Локальная вычислительная сеть

ПО – программное обеспечение

НСД – несанкционированный доступ

АРМ – автоматизированное рабочее место

ЭЦП – электронная цифровая подпись

ПК – персональный компьютер

СЗИ – средства защиты информации

АС – автоматизированные системы

### III. Неформальная модель нарушителя

*Нарушитель* - это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Система защиты должна строиться исходя из следующих предположений о следующих возможных типах нарушителей правил безопасности в системе:

а) *"Неопытный (невнимательный) пользователь"* - сотрудник организации, который может предпринимать попытки выполнения запрещенных операций, доступа к недоступным ему защищаемым ресурсам АС, ввода некорректных данных и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

б) *"Любитель"* - сотрудник организации, пытающийся преодолеть систему защиты без корыстных целей, с целью самоутверждения (из «спортивного интереса»). Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей и т.п. других пользователей), недостатки в построении системы защиты и доступные ему штатные (установленные на рабочей станции) программы (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства (отладчики, служебные утилиты), самостоятельно разработанные программы или стандартные дополнительные технические средства.

в) *"Внешний нарушитель (злоумышленник)"* - постороннее лицо или сотрудник организации, действующий целенаправленно из корыстных интересов или из любопытства и «спортивного интереса», возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома систем защиты, характерных для сетей общего пользования (сетей X.25 или сетей на основе IP-протокола), включая удаленное внедрение программных закладок и использование специальных инструментальных и технологических программ, используя имеющиеся слабости в системе защиты узлов сети АС.

г) *"Внутренний злоумышленник"* - сотрудник организации, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками организации. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как изнутри, так и извне - из сетей общего пользования.