Informal document WP.30/GE.2 (2016) No. 3

Distr.: General
9 December 2016

Russian only

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, 12 и 13 декабря 2016 года
Пункт 5 предварительной повестки дня
Рассмотрение вопроса о конфиденциальности данных

Представлено правительством Российской Федерации

Актуальные угрозы информационной безопасности (при автоматизированной обработке)

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

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атакующего)	Код угрозы
Ввод несуществующего ЭД	Изменение ПО	Вне процесса функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И1
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	Любая станция ЛВС	
	Внедрение программной закладки	В процессе функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И3
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	Любая станция ЛВС	
	«Ручной ввод»	В процессе функционирования системы	Сервер	Любая станция ЛВС	И6
			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			ЛВС	Любая станции ЛВС	
		В процессе передачи данных	Сеть передачи данных	Промежуточные узлы	И7
			Модем	Промежуточные узлы	
Нарушение конфиденциальности ЭД	Изменение ПО	Аналогично предыдущему случаю			
	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	ЛВС	Любая станция ЛВС	И4
		В процессе передачи данных	Сеть передачи данных	Промежуточные узлы	И5

			Модем		
	Несанкционированное копирование	Вне процесса функционирования системы	Сервер	Любая станция ЛВС	И9

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атакующего)	Код угрозы
Отказ от факта получения ЭД	Изменение ПО	В процессе функционирования системы	Любая станция ЛВС	Любая станция ЛВС	И3
			Почтовый сервер	Почтовый сервер	
		В процессе передачи данных	Внешний тамож. орган	Внешний тамож. орган	
Отказ от авторства ЭД	Аналогично предыдущему случаю				И10
Дублирование ЭД	Изменение ПО	Аналогично предыдущему случаю			И16
	Внедрение программной закладки				
	«Повтор в сети»	В/Вне процесса функционирования системы	Сервер	Любая станция сети	И12
			ЛВС	Любая станция сети	
			Сеть передачи данных	Промежуточные узлы	
			Модем		
Потеря или уничтожение ЭД	Перехват ЭД	В процессе функционирования системы	Сервер	Любая станция сети	И4
			ЛВС	Любая станция сети	
			Сеть передачи данных	Промежуточные узлы	
			Модем		
	Несанкционированное копирование	Вне процесса функционирования системы	Сервер	Любая станция ЛВС	И9
	Изменение ПО	Аналогично предыдущему случаю			И11
	Внедрение программной закладки				
НСД к АРМ системы электронного документооборо	НСД	В/Вне процесса функционирования системы	Любая станция ЛВС	Эта же станция ЛВС	И13
				Любая станция ЛВС → Сервер (через LOGIN SCRIPT)	

та			Почтовый сервер	Почтовый сервер	
				Любая станция ЛВС	
			Сервер	Любая станция ЛВС	
			Любая станция ЛВС	Из внешней сети (Internet)	

Угроза	Атака	Время проведения атаки	Объект атаки (местоположение атакуемого)	Субъект атаки (местоположение атакующего)	Код угрозы
НСД к каналу передачи данных	НСД к каналу	В процессе функционирования системы	ЛВС	Любая станция сети	И14
		В процессе передачи данных	Сеть передачи данных	Промежуточный узел	И15
			Модем		
Нападение из внешней сети	Атака из внешней сети	В/Вне процесса функционирования системы	Сервер		И18
			Станция сети		
			Модем		
			Маршрутизатор		
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

Меры защиты от реализации угроз

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
И1	1. Инструкция по внесению изменений в конфигурации ПО 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил 4. Инструкция по изменению полномочий пользователей	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Запрет загрузки АРМ с гибких магнитных дисков 2. Защита исполняемых файлов от изменения 3. Замкнутая среда разрешенных для запуска программ для каждого пользователя системы 4. Периодический контроль целостности исполняемых файлов и настроек программных средств 5. Использование ЭЦП 6. Регистрация событий
И2	1. Двойной контроль при вводе 2. Контроль прохождения документов 3. Инструкции пользователям 4. Задание ответственности за нарушение установленных правил	Нет	1. Двойной контроль при вводе (при помощи ПО) 2. Контроль прохождения документов (при помощи ПО) 3. Регистрация событий
И3	1. Инструкция по внесению изменений в конфигурации ПО 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Запрет загрузки АРМ с гибких магнитных дисков 2. Защита исполняемых и системных файлов от изменения 3. Замкнутая среда разрешенных для запуска программ для каждого пользователя системы 4. Периодический контроль целостности системы 5. Регистрация событий 6. Использование средств обнаружения нападений
И4	1. Инструкция по внесению изменений в конфигурации ПО 2. Инструкции пользователям 3. Задание ответственности за нарушение установленных правил 4. Инструкция по изменению полномочий пользователей	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

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
И5	1. Договор с внешней организаций	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 организаций	1. Разграничение доступа в помещения 2. Физическая защита помещений	1. Использование ЭЦП 2. Преобразование информации 3. Квитирование 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 организаций 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	1. Изоляция защищаемой системы от других	1. Ограничение доступа к ПК 2. Разграничение доступа к ПК

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
	нарушение установленных правил	систем	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. Квитирование 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. Владельцем 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 марщрутизаторы 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

Код угрозы	Меры защиты		
	Организационные	Физические	Технические
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
И17	Все меры	Все меры	Все меры
И18	1. Инструкция по использованию каналов передачи данных 2. Договор с внешней организацией 3. Инструкции пользователям 4. Задание ответственности за нарушение установленных правил		1. Ограничение числа используемых каналов передачи данных 2. Физическая изоляция ПК для доступа в глобальные сети от АРМ системы ЭД 3. Ограничение доступа к ПК, имеющим модемы 4. Регистрация событий 5. Использование средств обнаружения нападений 6. Использование межсетевых экранов 7. Использование всех встроенных в маршрутизаторы средств защиты

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

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:

1. ***"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.

2. ***"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.

3. ***"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.

4. ***"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.