Э. Э. Яндыбаева, И. В. Машкина

ОЦЕНКА АКТУАЛЬНОСТИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ЭЛЕКТРОННОЙ ТОРГОВОЙ ПЛОЩАДКИ

Информационная система электронной торговой площадки (ИС ЭТП) предназначена для проведения аукционов в электронной форме в сети Интернет. Проведение электронного аукциона требует участия оператора ЭТП, организатора аукциона и участников такого аукциона. Оператором ЭТП является юридическое лицо, которое владеет ИС ЭТП и обеспечивает проведение электронных аукционов в соответствии с законодательством РФ о контрактной системе в сфере закупок. Организатор аукциона — клиент ЭТП, заинтересованный в выполнении какого-либо объема работ, приобретении какого-либо продукта либо в продаже какого-либо товара посредством электронного аукциона и объявивший о проведении такого аукциона. Участник аукциона — клиент ЭТП, подавший заявку на участие в объявленном электронном аукционе.

При проведении электронного аукциона обязательным является использование электронной подписи. Каждый документ, отправляемый клиентом и администратором ЭТП, подписывается электронной подписью [1]. ИС ЭТП состоит из открытой и закрытой частей. Открытая часть ИС ЭТП доступна всем пользователям сети Интернет. Закрытая часть ИС ЭТП доступна зарегистрированным клиентам ЭТП и администраторам ЭТП, позволяет получить доступ к конфиденциальной информации и выполнять действия в соответствии с предоставленным уровнем доступа. Аутентификация происходит как по связке логин-пароль, так и по сертификату электронной подписи.

В Российской Федерации для государственных и муниципальных учреждений с 2011 г. проведение электронных аукционов на закупку товаров является обязательной процедурой [2]. Общая сумма объявленных электронных аукционов ежегодно составляет сотни миллиардов рублей. При этом главная роль отводится обеспечению информационной безопасности (ИБ) в системе электронных торгов, и актуальным вопросом является исследование угроз ИБ ИС ЭТП.

Авторами были выявлены следующие преднамеренные угрозы ИБ ИС ЭТП:

- хищение ключа электронной подписи;
- удаленное несанкционированное управление ключом электронной подписи;
- подмена документа при передаче его на подпись;
- хищение логина и пароля от личного кабинета;
- несанкционированный доступ к конфиденциальной информации, хранящейся на серверах ЭТП;
- срыв нормального функционирования сайта ЭТП.

Угроза хищения логина и пароля от личного кабинета и угроза несанкционированного доступа к конфиденциальной информации, хранящейся на серверах ЭТП, могут привести к следующим негативным последствиям: невыгодный контракт, проигранный аукцион, раскрытие конфиденциальной информации о составе участников аукциона, раскрытие конфиденциальной информации о клиентах ЭТП, попадание в реестр недобросовестных поставщиков и испорченная репутация клиента ЭТП. К таким же негативным последствиям могут привести угроза хищения ключа электронной подписи, угроза удаленного несанкционированного управления ключом электронной подписи и угроза подмены документа при передаче его на подпись. Дополнительно они могут привести к отказу в регистрации в ИС ЭТП и невозможности принятия участия в аукционе. Срыв нормального функционирования сайта ЭТП приводит к нарушению сроков проведения аукциона и, как следствие, к испорченной репутации оператора ЭТП.

В настоящей работе для моделирования угроз ИБ ИС ЭТП используется графическая нотация EPC (Event-Driven Process Chain, событийная цепочка процессов), ключевыми элементами которой являются События и Функции, связанные между собой логическими операциями [3]. Диаграмма процесса в EPC должна начинаться и заканчиваться Событием. За Функцией всегда должно следовать Событие. Для ветвления процесса используются логические отношения, описываемые символами «и» (/\), «включающее ИЛИ» (\/) и «исключающее ИЛИ» (XOR). EPC-модели угроз позволяют оценить причинно-следственные связи между возможными уязвимостями ИС ЭТП и их негативными последствиями для безопасности системы.

Разработано шесть EPC-моделей преднамеренных угроз ИБ ИС ЭТП, две из которых представлены на рис. 1 и 2, где ЭП — электронная подпись, УЦ — удостоверяющий центр, АРМ — автоматизированное рабочее место.

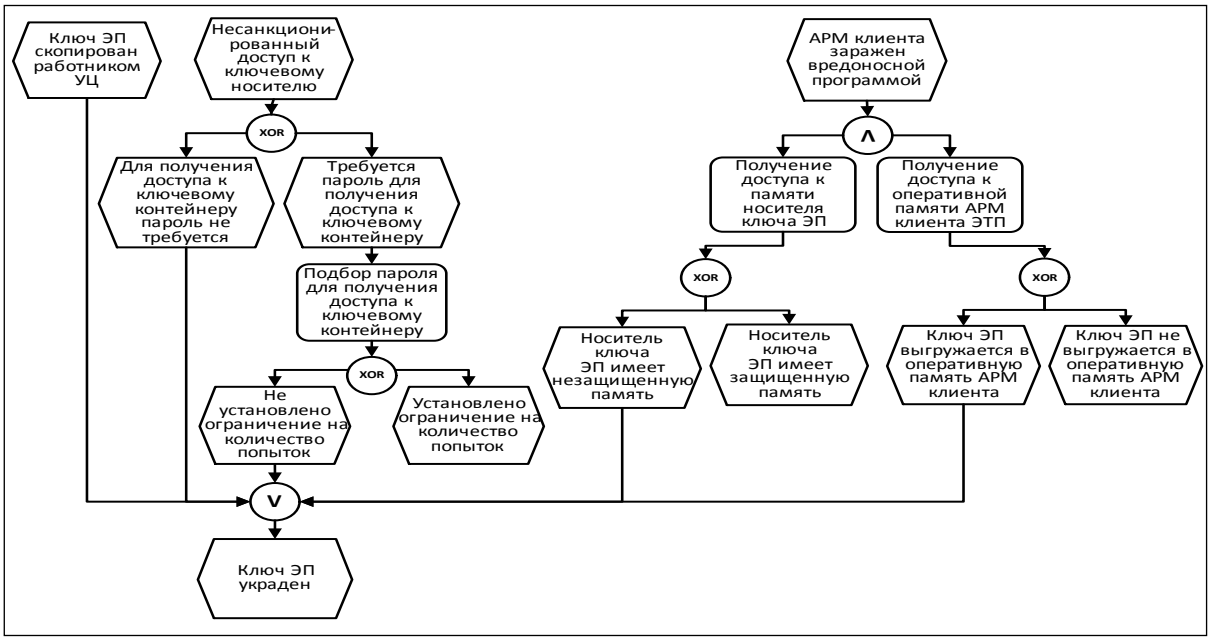

Рис. 1. EPC-модель угрозы хищения ключа электронной подписи

В настоящей работе с учетом положений теории вероятности проведена оценка вероятностей событий и активации функций для каждой разработанной EPC-модели угрозы. В соответствии с принципом недостаточного основания, если нет оснований предпочесть исход одного события другому, оба события следует считать равновероятными [4]. Поэтому в условиях отсутствия статистической информации о наступлении оцениваемых в EPC-моделях событий взаимоисключаемые события считались равновероятными. В том числе равновероятными считались наступление и ненаступление события.

Результаты расчета вероятностей событий в EPC-модели угрозы подмены документа при передаче его на подпись приведены в таблице 1.

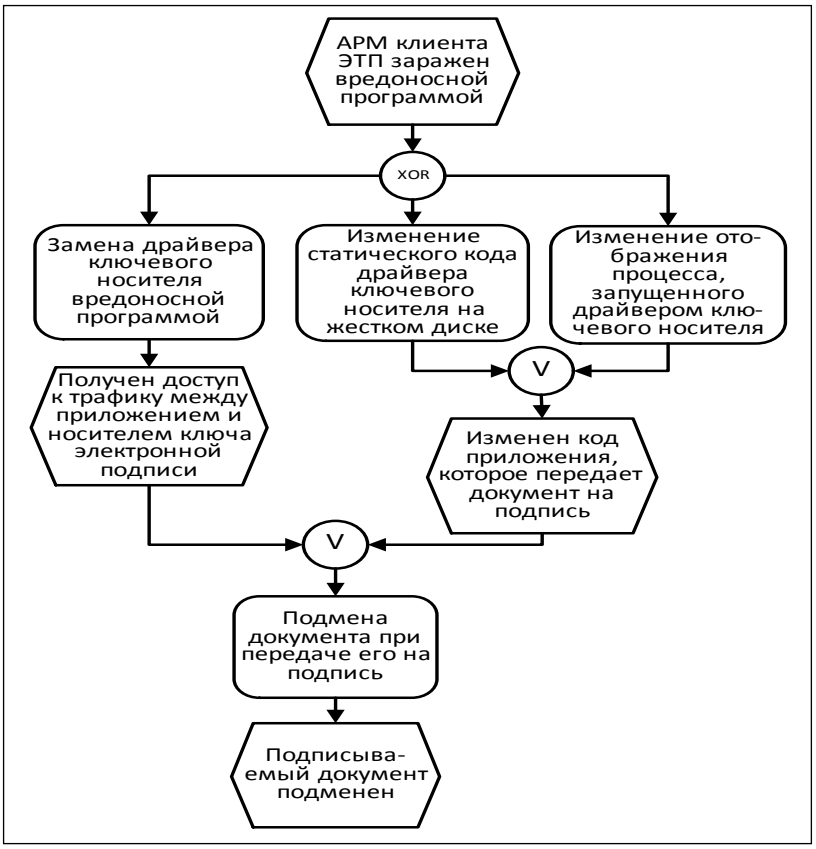

Рис. 2. EPC-модель угрозы подмены документа при передаче его на подпись

Таблица 1. Расчет вероятностей событий

Наименование события/ функции	**Вероятность**	**Пояснения**
АРМ клиента ЭТП заражен вредоносной программой (E1)	P(E1) = 0,5	Считаем равновероятными наступление и ненаступление данного события.
Замена драйвера ключевого носителя (F1)	P(F1) = P(E1) * P(F1|E1) = 0,5 * (1 : 3) = 0,17	Считаем F1|E1, F2|E1 и F3|E1 равновероятными.
Изменение статического кода драйвера ключевого носителя на жестком диске (F2)	P(F2) = P(E1) * P(F2|E1) = 0,5 * (1 : 3) = 0,17	Считаем F1|E1, F2|E1 и F3|E1 равновероятными.
Изменение отображения процесса запущенного драйвером ключевого носителя (F3)	P(F3) = P(E1) * P(F3|E1) = 0,5 * (1 : 3) = 0,17	Считаем F1|E1, F2|E1 и F3|E1 равновероятными.
Получен доступ к трафику между приложением и носителем ключа электронной подписи (E2)	P(E2) = P(F1) * P(E2|F1) = 0,17 * 0,5 = 0,09	Считаем равновероятными наступление и ненаступление события E2|F1.

Изменен код приложения, которое передает документ на подпись (E3)	P(E3) = P(F2 + F3)*P(E3|(F2 + F3)) = (0,17 + 0,17 – 0,17 * 0,17) * 0,5 = 0,16	Считаем равновероятными наступление и ненаступление события E3|(F2 + F3).
Подмена документа при передаче его на подпись (F4)	P(F4) = P(E2 + E3) = 0,09 + 0,16 – 0,09 * 0,16 = 0,24	
Подписываемый документ подменен (E4)	P(E4) = P(F4) = 0,24	

В таблице 2 приведены значения всех рассчитанных вероятностей успешной реализации угрозы.

Таблица 2. Значения вероятности успешной реализации угрозы

№	Угроза	Значение вероятности
	Хищение ключа электронной подписи клиента ЭТП / администратора ЭТП	0,25
	Удаленное несанкционированное управление ключом электронной подписи клиента ЭТП / администратора ЭТП	0,15
	Подмена документа при передаче его на подпись	0,24
	Хищение логина и пароля от личного кабинета клиента ЭТП / администратора ЭТП	0,34
	Несанкционированный доступ к конфиденциальной информации, хранящейся на серверах ЭТП, из сети Интернет	0,03
	Срыв нормального функционирования сайта ЭТП	0,41

Экспертным путем было установлено, что угроза актуальна, если рассчитанное значение вероятности успешной реализации угрозы больше или равно 0,25. Таким образом, актуальными угрозами ИБ ИС ЭТП являются: хищение ключа электронной подписи, хищение логина и пароля от личного кабинета, срыв нормального функционирования сайта ЭТП. Данные угрозы следует принять во внимание при разработке комплекса технических и организационных мер для их нейтрализации.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон РФ от 22 марта 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
2. Федеральный закон РФ от 21 июля 2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».
3. *Шеер А.-В.* ARIS — моделирование бизнес-процессов. Вильямс, Москва, 2000. — 175 с.
4. *Гнеденко Б. В.* Курс теории вероятностей: Учебник. Изд. 8-е, испр. и доп. М.: Едиториал УРСС, 2005. — 448 с.