УДК 004.056.5; 004.738.5

АНАЛИЗ ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Минзов Анатолий Степанович[1], Бородина Александра Алексеевна[2]

[1]Профессор, доктор технических наук;
ГБОУ ВО МО «Университет «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, д.19;
e-mail: 9083083@rambler.ru.

[2]Студент;
ГБОУ ВО МО «Университет «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, д. 19;
e-mail: bo.alexandraa@gmail.ru.

В данной статье проведен анализ требований по обеспечению информационной безопасности систем электронной коммерции.

Ключевые слова: система электронной коммерции (СЭК), информационная безопасность (ИБ), политика безопасности, угрозы СЭК, аудит ИБ, статистика инцидентов СЭК, модель угроз СЭК, методы защиты СЭК, требования по обеспечению ИБ СЭК.

ANALYSIS OF REQUIREMENTS FOR INFORMATION SECURITY OF ELECTRONIC COMMERCE SYSTEMS

Minzov Anatoliy[1], Borodina Alexandra[2]

[1]Professor, Doctor of Technical Sciences;
Dubna State University,
Institute of the system analysis and management;
141980, Moscow reg., Dubna, 19 University st.;
e-mail: 9083083@rambler.ru.

[2]Student;
Dubna State University,
Institute of system analysis and management;
Moscow reg., Dubna, 19 University st.;
e-mail: bo.alexandraa@gmail.ru.

The article defines the requirements for information security of electronic commerce systems.

Keywords: electronic commerce systems (ECS), information security (IS), security policy, threats of ECS, audit of IS, incident statistics of ECS, threat model of ECS, protection methods of ECS, requirements for IS of ECS.

Введение

В настоящее время происходит стремительное развитие информационных технологий и сети Интернет. Все это сформировало информационную среду, которая воздействует на все сферы человеческой деятельности. Особенно, возрастает интерес к системам электронной коммерции (СЭК). Электронная коммерция – технология, которая обеспечивает цикл операций: заказ товара (услуги), проведение платежей, доставка товара (выполнение услуги). Но для нормального функционирования системы электронной коммерции, необходимо обеспечить ее защищенность. Ведь воздействие на систему электронной коммерции может привести не только к потере информации, но и может быть нанесен ущерб владельцам или пользователям информации, а также может привести к большим финансовым потерям.

1. Анализ современных требований к СЭК на основе нормативных документов

1.1 Системы электронной коммерции (понятие, схема взаимоотношений)

В настоящее время электронная коммерция представляет собой комплексную интернет-ориентированную систему, которая дает возможность автоматизировать взаимосвязи и отношения экономического субъекта и его внешнего окружения. Электронная коммерция – область, включающая в себя транзакции (финансовые и торговые), которые осуществляются с помощью компьютерных технологий. Системам электронной коммерции (СЭК) необходимо обеспечивать высокий уровень защищенности, с целью нормального функционирования и избежания:

- потери информации;
- нанесения ущерба владельцам или пользователям информации;
- больших финансовых потерь.

К системам электронной коммерции относят следующее:

- *Electronic Data Interchange* (*EDI*) – электронный обмен информацией;
- *Electronic Funds Transfer* (*EFT*) – электронное движение капитала;
- *e-trade* – электронную торговлю;
- *e-cash* – электронные деньги;
- *e-marketing* – электронный маркетинг;
- *e-banking* – электронный банкинг;
- *e-insurance* – электронные страховые услуги.

В данной статье будут рассматриваться взаимоотношения между системой электронной коммерции и потребителем – *Business-To-Consumer* (*B2C*).

B2C – концепция построения коммерческих взаимоотношений между СЭК (*Business*) и потребителем (*Consumer*). Это понятие применяется для описания деятельности, которую ведет предприятие. Оно показывает, что продажа предприятием товаров или предоставление услуг направлена исключительно на конечного потребителя. Особенности данной концепции:

- более короткий цикл продаж;
- эмоциональное принятие решений о покупке;
- менее тесное взаимоотношение продавца и покупателя.

Самый распространенный инструмент в СЭК – интернет-магазин.

На рис. 1 представлены отношения между объектами:

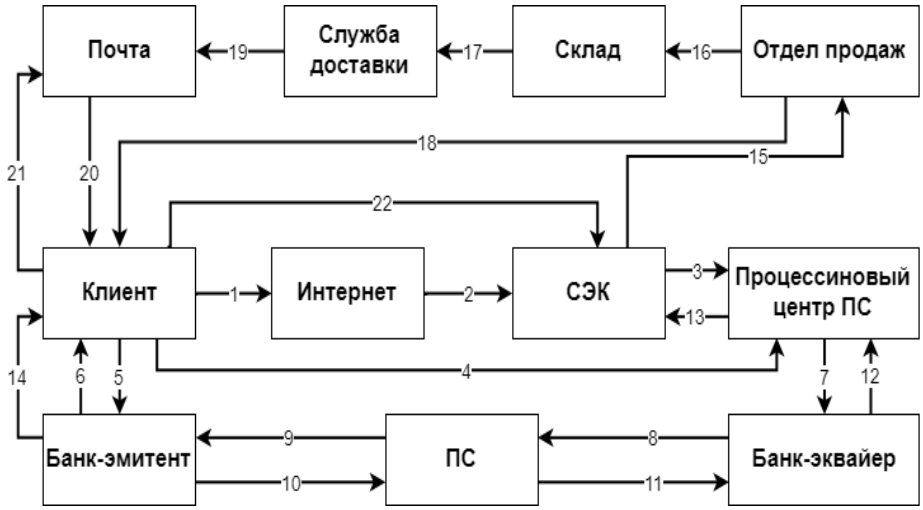

Рис. 1. Схема интернет-эквайринга

Безналичная оплата в системах электронной коммерции (СЭК) происходит следующим образом:

1. Клиент заходит в поисковую систему в Интернете и вводит наименование необходимого ему товара.
2. Выполняется поиск, и Клиенту представляется список интернет-магазинов (СЭК), где есть этот товар. Следовательно, Клиент перенаправляется на сайт выбранного им интернет-магазина.
3. Клиент выбирает себе товар, выбирает необходимые ему параметры этого товара. Данные о заказе, а именно, номер заказа, магазина, сумма и так далее, регистрируются интернет-магазином, и направляются в Процессинговый центр платежной системы (Процессинговый центр ПС).
4. Далее Клиент перенаправляется на страницу авторизации Процессингового центра, где предоставляет свои сведения по карте.
5. Также Клиент перенаправляется на защищенную страницу Банка-эмитента, для того, чтобы подтвердить пароль.
6. Клиент получает пароль, вводит его на странице Банка-эмитента, нажимает кнопку подтвердить.
7. Из Процессингового центра поступает запрос на авторизацию в Банк-эквайер.
8. Из Банка-эквайера, в свою очередь, поступает запрос на авторизацию в Платежную систему (ПС).
9. Платежная система отправляет запрос в Банк-эмитент.
10. В Банке-эмитенте проверяется остаток по счету Клиента. Он блокирует необходимую сумму, если она есть на счете, и посылает в Платежную систему ответ с разрешением (отказом) оплаты.
11. Платежная система сообщает о проведении транзакции Банку-эквайеру.
12. А Банк-эквайер передает эту информацию Процессинговому центру.
13. Далее в Интернет-магазин поступает информация от Процессингового центра об успешном проведении транзакции (или отказе).
14. Банк-эмитент уведомляет Клиента о совершении покупки.
15. Далее Интернет-магазин отправляет информацию в Отдел продаж о том, что товар оплатили, а также параметры этого товара, чтобы можно было формировать заказ.
16. Данные о заказе Отдел продаж отправляет на Склад.
17. Со Склада данный товар поступает в Службу доставки с информацией о месте доставки и отправляется Клиенту.

18. Клиент в свою очередь получает информацию от Отдела продаж, что товар отправлен, а также о его сопровождении и доставке.
19. Товар доставляется на Почту.
20. Почта отправляет извещение Клиенту о том, что товар доставлен.
21. Клиент приходит на Почту с паспортом и предоставляет извещение с его личными данными для того, чтобы ему получить товар.
22. Клиент на сайте Интернет-магазина подтверждает получение товара, а также по желанию может оставить свой отзыв.

Выделяют недостатки процесса интернет-эквайринга:

- привлечение различных мошенников;
- недоверие со стороны клиента к товару, который продается через интернет;
- ожидание доставки;
- невозможность лично посмотреть и потрогать товар и так далее.

Для того, чтобы понять какие меры нужно предпринимать для обеспечения безопасности, нужно понять, что именно угрожает.

Для анализа угроз, которые могут возникнуть при процессе интернет-эквайринга, была использована база данных угроз и уязвимостей сайта *fstec.ru*. Проанализировав угрозы и уязвимости, можно сделать вывод о том, что все опасности связаны с перехватом информации, введением вредоносного кода, из-за недостаточного обеспечения информации. Объектами воздействия в основном становятся сетевое программное обеспечение, сетевой трафик. И результат этих атак проявляется в нарушении конфиденциальности, целостности и доступности.

Также можно отметить, что все эти угрозы происходят удаленно от объектов воздействия. Удаленное воздействие можно назвать социальной инженерией. Социальная инженерия – это когда хакеры, нарушители несанкционированно получают доступ к какой-либо информации, не используя при этом технические средства.

То есть, социальная инженерия, например, при заражении вредоносными программами хакер пытается разнообразными способами убедить пользователя совершить какое-либо действие, для того чтобы запустить незнакомую программу на выполнение. В большинстве случаев от пользователя требуется установить некоторую программу или посетить какой-либо *Web*-сайт.

Обычно это происходит через электронную почту, службу мгновенных сообщений, одноранговые сети.

Схемы атак мошенников могут быть разные. Рассмотрим некоторые сценарии относительно представленной выше схемы интернет-эквайринга.

1. Фрод. - вид мошенничества в области информационных технологий, в частности, несанкционированные действия и неправомочное пользование ресурсами и услугами в сетях связи. Относительно схемы интернет-эквайринга, этот вид мошенничества может проявляться на различных этапах.

2. Кардинг – это когда производится операция с использованием платежной карты или ее реквизитов, и она не подтверждается ее держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров (либо непосредственно, либо через «трояны» и «черви»).

Кардинг может всречаться на 5 и 6 тапах схемы интернет-эквайринга, то есть между клиентом и банком-эмитентом.

3. Фишинг – это создание мошенниками сайта, который будет пользоваться доверием у пользователя, например — сайт, похожий на сайт банка-эмитента, через который и происходит похищение реквизитов платежных карт

На 4-м (клиент-процессинговый центр) и 5-м (клиент-банк-эмитент) этапах данной схемы можно проследить этот вид мошенничества.

4. Снифферы (анализатор трафика по признакам обращения к банковской ПС) — это программы, перехватывающие весь сетевой трафик. Например, если у злоумышленника есть доступ к одной сетевой машине, и он установил там сниффер, то в скором времени все пароли будут ему предоставлены.

5. «Злоумышленник посередине» – простая схема мошенничества. Нарушитель ставить себя в цепь обмена сообщениями между двумя пользователями, и перехватывает их сообщения. Но, ему также необходимо выдавать себя за каждую сторону.

1.2 Анализ статистики инцидентов

Анализ статистики инцидентов СЭК будет рассматриваться согласно [5].

Статистику провела компания *InfoWatch*, которая занимается разработкой решений для защиты бизнеса от внутренних угроз ИБ.

По статистике 2016 года данной компании были сделаны следующие выводы:

1. Было зарегистрировано 1556 случаев утечки конфиденциальной информации, что составляет на 3,4% больше, чем в 2015 году. При этом 61,8% утечек произошли по вине внутреннего нарушителя, а 38,2% по вине внешнего (рис. 2):

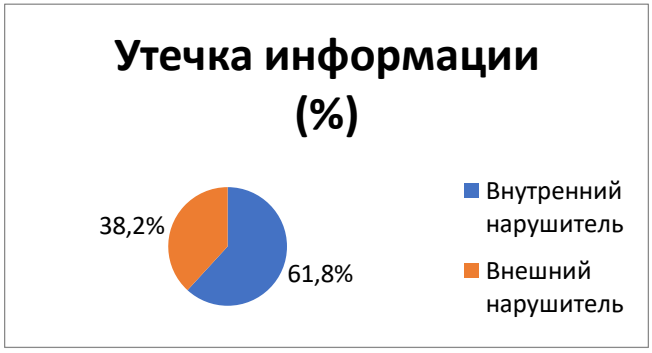

Рис. 2. Утечка информации относительно воздействия на систему [5]

2. Были выделены следующие виновники утечек (рис.3):

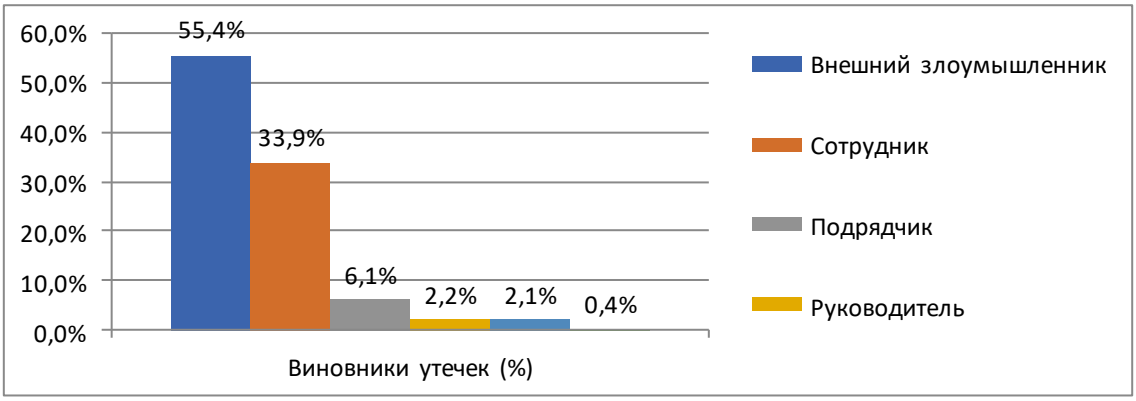

Рис. 3. Виновники утечки информации [5]

3. Также данная компания провела статистику по утечке информации по отраслям. Больше всего утечек произошло в сфере медицины, меньше в сфере промышленности и транспорта. Огромное

число скомпрометированных данных принадлежит сегменту торговых онлайн-площадок – 73,6% (рис.4):

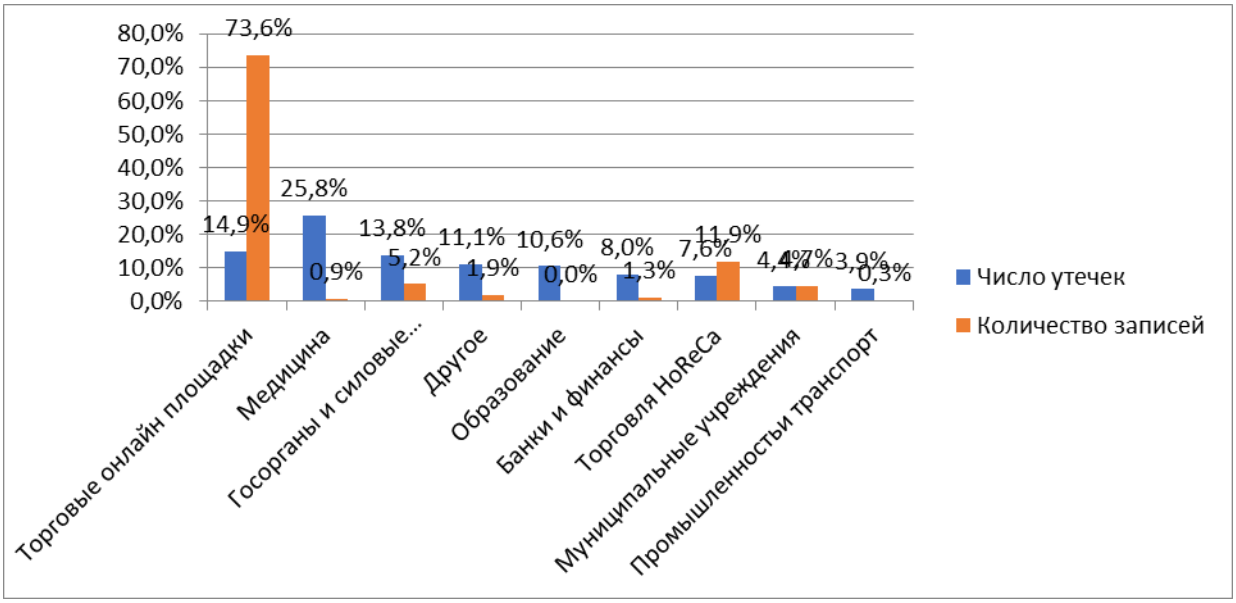

Рис. 4. Утечка информации по отраслям [5]

4. Было выявлено, что объем скомпрометированных данных увеличился в три раза. Это говорит о ценности информации, которая находится в цифровом виде.

В [2] были выделены десять наиболее распространенных и опасных уязвимостей (табл. 1):

Таблица 1. Наиболее распространенные и опасные уязвимости [2]

№	Наименование уязвимости	Описание уязвимости
1	Отсутствие проверки параметров в http-запросах	Злоумышленник может получать доступ к ресурсам сервера через web-приложение, при использовании особых параметров
2	Нарушение политик управления доступом к ресурсам	Злоумышленник использует закрытые ресурсы или получает доступ к учетным записям других пользователей
3	Нарушение правил управления учетными записями и пользовательскими сессиями	Отсутствие надежной защиты пользовательских данных (логина, пароля) и идентификаторов сессий (файлы cookie). Злоумышленник перехватывает данные других пользователей и пользуется системой от их имени
4	Ошибки в механизме Cross-Site Scripting (CSS или XSS), который используется для перенаправления пользователя на другие сайты.	Злоумышленник может получить доступ к пользовательским данным или взлому локального компьютера.
5	Ошибки переполнения буфера, которые есть во многих программных продуктах (от скриптов и драйверов до операционных систем и серверного ПО).	Злоумышленник захватывает управление компьютером.
6	Отсутствие необходимого	При вводе злоумышленника своих команд в эти парамет-

	контроля над параметрами, которые передаются компьютерами при доступе к внешним ресурсам.	ры, последствия могут быть плачевными.
7	Неправильная реализация обработки ошибок в ПО.	Злоумышленник может получить данные о системе или доступ к ней.
8	Неудачное использование криптографии.	Инструменты для шифрования информации могут иметь собственные пробелы, поэтому использование сильной криптографии бессмысленно.
9	Отсутствие необходимой защиты подсистем удаленного администрирования.	Злоумышленник может управлять системой с любого подключенного к Сети компьютера.
10	Неправильное конфигурирование серверного ПО.	Большое влияние на безопасность настроек.

1.3 Требования Guide to Secure Web Services (NIST), OWASP по обеспечению безопасности WEB решений

Стандарты в области безопасности очень важны для разработкипроектов, особенно для зарубежных заказчиков. Поэтому для таких целей необходимо брать стандартизированные документы международных компаний.

Обращаясь к [1], рассмотрим описание стандартов и требований по безопасности web-сервисов.

Выполнение требований по защите web-сервисов

Некоторые организации, в том числе *OASIS, W3C, Liberty Alliance* и другие представители промышленного сектора, собрали многочисленные стандарты безопасности и методы для защиты web-сервисов. В большинстве случаев эти стандарты и методы дополняют или расширяют друг друга, но есть и такие, которые противоречат друг другу или конкурируют друг с другом.

Стандарт безопасности web-сервисов

Сообщества открытых стандартов, которые создали *web*-сервисы, разработали ряд стандартов безопасности для *web*-сервисов. На рис.5 представлена условная ссылочная модель для стандартов безопасности *web*-сервисов. Эта модель отображает различные стандарты на различные функциональные уровни типичной реализации *web*-сервисов. Не следует рассматривать данную модель, как иерархическую

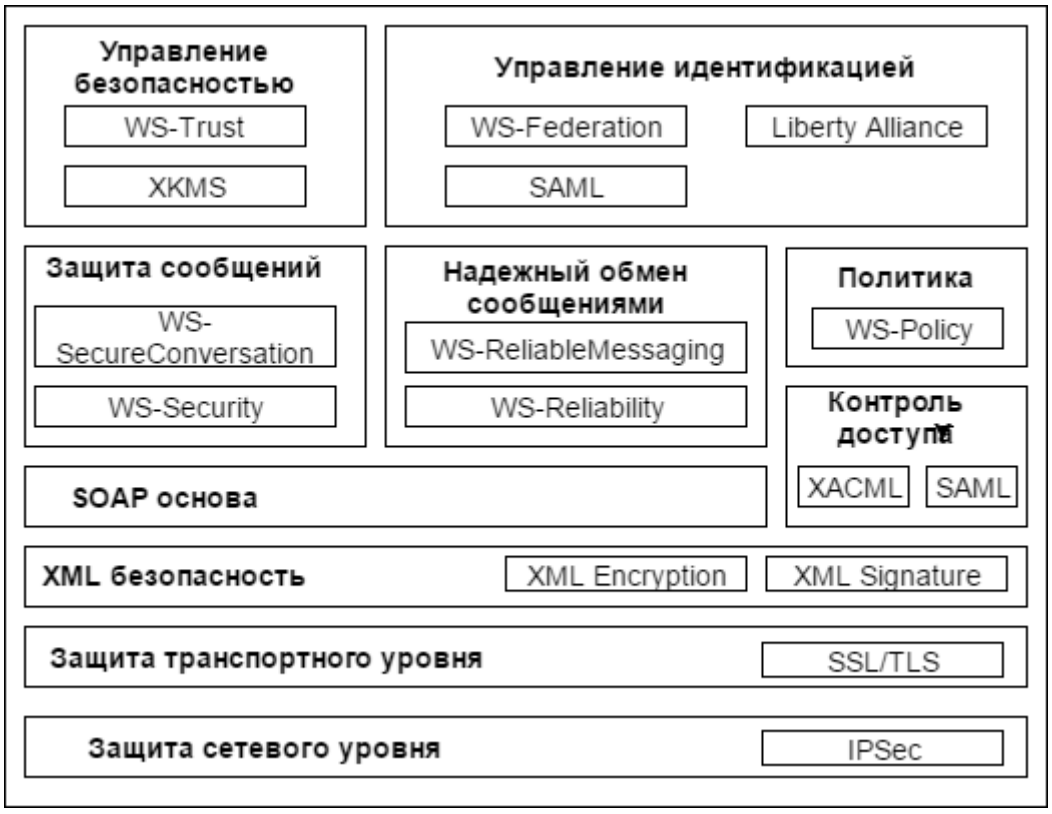

Рис.5. Стандарты безопасности веб-сервисов: условная эталонная модель [1]

Стандарты на уровне защиты сети, транспорта и уровней безопасности *XML* используются для защиты сообщений по мере их передачи по сети. Стандарты безопасности *IPsec*, *SSL / TLS* (*Secure Sockets Layer* / *Transport Layer Security*), *XML Encryption* и *XML Signature* работают с *SOAP*-сообщениями на разных уровнях.

Над уровнем безопасности *XML* существуют два типа стандартов: стандарты, созданные поверх SOAP и автономные стандарты. Стандарты безопасности сообщений *WS-Security* и *WS-SecureConversation* определяют, как использовать подпись *XML*, *XML*-шифрование и учетные данные для защиты *SOAP* на уровне сообщений. Надежные стандарты обмена сообщениями определяют протоколы и конструкции, необходимые для обеспечения того, чтобы получать сообщения. Стандарты контроля доступа не уникальны для *Web*-сервисов. *XACML* может определять политику доступа для любой системы, а *SAML* - для определения утверждений в любой среде. *WS-Policy* уровня политики определяет грамматику для передачи требований политики веб-службы.

Специфики управления безопасностью определяют другие web-сервисы для управления учетными данными, такими как сертификаты *PKI* в *SOA*. Стандарты управления идентификацией используют стандарты контроля доступа, стандарты политики и стандарты *SOAP* для предоставления услуг по распределению и управлению идентификаторами пользователей и учетными данными *в SOA*.

Отношение требований безопасности веб-службы к стандартам

Таблица 2 показывает, какие требования безопасности удовлетворяются различными спецификам и стандартами.

Таблица 2. Стандарты и характеристики, относящиеся к безопасности [1]

Измерение	**Требования**	**Характеристики**
Обмен сообщениями	Конфиденциальность и целостность	*WS-Security* *SSL/TLS*
	Аутентификация	*WS-Security Tokens* *SSL/TLS X.509 Certificates*
Ресурс	Авторизация	*XACML* *XrML* *RBAC, ABAC*
	Конфиденциальность	*EPAL* *XACML*
	Подотчетность	*None*
Переговоры	Реестры	*UDDI* *ebXML*
	Семантика	*SWSA* *OWL-S*
	Бизнес контракты	*ebXML*
Доверие	Создание	*WS-Trust* *XKMS* *X.509*
	Доверенность	*SAML* *WS-Trust*
	Федерация	*WS-Federation* *Liberty IDFF* *Shibboleth*
Свойства безопасности	Политика	*WS-Policy*
	Политика безопасности	*WS-SecurityPolicy*
	Доступность	*WS-ReliableMessaging* *WS-Reliability*

Каждое измерение безопасности *SOA* имеет одно или несколько требований безопасности. Каждое требование может иметь любое количество стандартов, которые его поддерживают. Например, как *SSL* / *TLS*, так и *WS-Security* обеспечивают поддержку конфиденциальности, целостности и аутентификации для измерения сообщений, в то время как требование ответственности в отношении защиты ресурсов не имеет каких-либо стандартов поддержки.

1.4 Требования ГОСТ р ИСО/МЭК 27001 и 27002 по обеспечению безопасности СЭК

Существует множество угроз СЭК, поэтому необходимо обеспечивать их информационную безопасность. Согласно [4], информация – это актив, который, подобно другим активам организации, имеет ценность.

Информационная безопасность, защищает информацию от угроз, обеспечивает непрерывность бизнеса, минимизацию риска бизнеса, получение максимальной отдачи от инвестиций, а также реализацию потенциальных возможностей бизнеса. Информационную безопасность необходимо поддерживать и улучшать, так как она помогает поддерживать конкурентоспособность, денежный оборот и коммерческий имидж.

Информационная безопасность (ИБ) – сохранность и защищенность информационных ресурсов, законных прав личности и общества в информационной среде.

Для обеспечения информационной безопасности необходимо разработать политику безопасности. По [3], цель политики безопасности – обеспечение управления и поддержки высшим руковод-

ством информационной безопасности, согласно требованиям бизнеса и соответствующим законам и нормам.

Политика безопасности – совокупность методов, средств, деятельности и субъектов в области безопасности, которые обеспечивает защиту объекта информационной безопасности от угроз.

Для обеспечения политики безопасности необходимо:

1. Иметь в организации контактное лицо, которое будет заниматься внутренними вопросами ИБ.

2. Необходимо формировать хорошие отношения с внешними специалистами, которые занимаются ИБ. В состав специалистов должны входить соответствующие органы, которые находятся в курсе тенденций, осуществляют мониторинг стандартов и методов оценки.

Прежде чем говорить о требованиях по обеспечению информационной безопасности СЭК, необходимо рассмотреть источники требований безопасности. По [4] выделяют три основных источника:

- первый источник – оценка рисков бизнес-организации, учитывая ее стратегию и цели. Идентификация угроз, оценка уязвимостей и вероятностей возникновения угроз, оценка возможных последствий происходит при помощи оценки рисков;
- второй источник – требования правового, законодательного b нормативного характера. Бизнес-организация, ее партнеры, поставщики, подрядчики, социокультурная среда должны удовлетворять этим требованиям;
- третий источник – принципы, цели и требования бизнеса по обработке информации, разработанные бизнес-организацией для поддержания своей деятельности.

Обеспечение надежной ИБ требует проведение аудита ИБ.

Программа аудита должна включать данные, которые нужны для организации, результативного и эффективного проведения аудита в заданные сроки. Аудит может включать в себя следующее [2]:

- цели для программы аудита и отдельных аудитов;
- объем/количество/типы/места проведения и график проведения аудитов;
- процедуры программы аудита;
- критерии аудита;
- методы аудита;
- формирование группы (групп) по аудиту;
- необходимые ресурсы, включая расходы на командировки и размещение аудиторов;
- процессы, связанные с соблюдением конфиденциальности, обеспечением защиты информации.

Существуют основные принципы проведения аудита ИБ:

1. Независимость аудита ИБ – беспристрастность аудитора при проведении аудита ИБ и объективность в формировании результатов.

2. Полнота аудита ИБ – охват аудитом ИБ всех областей, которые соответствуют аудиторскому заданию. Полнота заключается и в достаточности требуемых и предоставленных документов, материалов, а также уровнем их соответствия поставленным задачам.

3. Оценка на основе свидетельств аудита ИБ – получение повторяемого заключения по результатам аудита ИБ, для повышения доверия к такому заключению.

4. Достоверность свидетельств аудита ИБ – уверенность аудитора в достоверности свидетельств аудита ИБ. Повышения доверия может быть:

- к документальным свидетельствам аудита ИБ – при подтверждении их достоверности третьей стороной или руководством организации БС РФ;
- к фактам, которые получены при опросе персонала проверяемой организации – при подтверждении данных фактов из различных источников;

- к фактам, которые получены при наблюдении за деятельностью проверяемой организации в области ИБ – при получении непосредственно в процессе функционировании проверяемых процедур или процессов.

5. Компетентность – основывается на знаниях навыках аудитора и способности их применять.

6. Этичность поведения – ответственность, беспристрастность, умение хранить тайну, неподкупность.

1.5 Требования приказа ФСТЭК №17 по обеспечению безопасности информационных систем

В данном документе определяются требования по обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация). Защищают ее от:

- утечки по техническим каналам;
- несанкционированного доступа;
- специальных воздействий на такую информацию (носители информации).

Цель защиты - добывание, уничтожение, искажение или блокирование доступа к информации (далее – защита информации) в процессе обработки указанной информации в государственных информационных системах (ИС).

В документе не идет рассмотрение требований о защите информации, связанных с использованием криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

Эти требования обязательны для обработки информации в:

- государственных ИС, которые функционируют на территории Российской Федерации;
- муниципальных ИС, если иное не установлено законодательством Российской Федерации (РФ) о местном самоуправлении.

Требования к организации защиты информации, содержащейся в ИС

Объекты защиты ИС – информация, которая содержится в ИС, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации [6].

Чтобы обеспечить защиту информации, которая содержится в ИС, оператор назначает должностное лицо или структурное подразделение, которое будет ответственно за защиту информации.

Составная часть работ по созданию и эксплуатации ИС – защита информации, которая содержится в ИС. Она обеспечивается на всех этапах ее создания, эксплуатации и вывода из эксплуатации. Это происходит следующим образом - принимаются организационные и технические меры защиты информации, которые направлены на блокирование угроз безопасности информации в ИС

Эти организационные и технические меры защиты информации, с целью создания ИС и задач, которые решаются этой ИС, должны исключать:

- неправомерный доступ, копирование, предоставление или распространение информации (обеспечение конфиденциальности информации);
- неправомерное уничтожение или модифицирование информации (обеспечение целостности информации);
- неправомерное блокирование информации (обеспечение доступности информации).

Проводятся следующие мероприятия, чтобы обеспечить защиту информации, которая содержится в ИС:

1. Формируются требования к защите информации, которая содержится в ИС.
2. Разрабатывается система защиты информации ИС.
3. Внедряется система защиты информации ИС.
4. Проводится аттестация ИС относительно требований защиты информации и вводится в эксплуатацию.
5. Обеспечивается защита информации в процессе эксплуатации ИС, которая была аттестована.
6. Обеспечивается защита информации при выводе из действия аттестованной ИС или после того, как было принято решение закончить обработку информации.

1.6 Требования по безопасности платежных систем

Платёжная система – комплекс правил, процедур и технической инфраструктуры, которые обеспечивают перевод денежных средств от одного субъекта экономики другому.

Прежде чем говорить о требованиях по безопасности платежных систем, необходимо обратиться к законам и нормативным документам.

Существует Федеральный закон № 161 от 27.06.2011 «О национальной платежной системе». Он устанавливает правовые и организационные основы национальной платежной системы (НПС), а также требования к ее организации и функционированию.

Также в 2012 году был опубликован ряд нормативных документов:

Постановление Правительства РФ от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе». В нем устанавливаются требования к защите информации, которая подлежит обязательной защите (в том числе персональных данных). Также описываются организационные и технические меры, которые направлены на защиту конфиденциальности, целостности и доступности защищаемой информации.

Положение Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля над соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». В нем список требований по ИБ, которые предъявляются к участникам национальной платежной системы (НПС).

Указание ЦБ от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств».

Важную роль играют участники НПС. Так как требования по обеспечению безопасности платежных систем, предъявляются не только технической составляющей, но и сотрудникам, которые участвуют в данном процессе. По ФЗ-161 выделяют следующих участников НПС:

- оператор платежной системы;
- оператор по переводу денежных средств;
- оператор электронных денежных средств;
- банковский платежный агент (субагент).

В данном законе акцент ставится на необходимость защиты информации и обеспечение бесперебойности функционирования платежной системы. Поэтому, рассматривая закон с точки зрения ИБ, наиболее интересными являются следующие статьи (таблица 3).

Таблица 3. Статьи ФЗ-161 [7]

Статья ФЗ-161	Что устанавливает
Статья 26. Обеспечение банковской тайны в платежной системе	Декларирование необходимости защиты банковской тайны участниками НПС.
Статья 27. Обеспечение защиты информации в платежной системе	Определение органов государственной власти, которые будут устанавливать требования к защищаемой информации и осуществлять контроль и надзор за выполнением требований
Статья 28. Система управления рисками в платежной системе	Системе защиты информации необходимо применять риск-ориентированный подход. Определение основных направлений при построении системы управления рисками, позволяющей снизить вероятность возникновения неблагоприятных последствий для бесперебойности функционирования платежной системы.
Статья 32. Осуществление надзора в национальной платежной системе	Закрепление за Банком России право проведения инспекционных проверок, а также определения форм и сроков предоставления отчетности, касающихся, в том числе, информационной безопасности.
Статья 34. Действия и меры принуждения, применяемые Банком России в случае нарушения поднадзорной организацией требований настоящего Федерального закона или принятых в соответствии с ним нормативных актов Банка России	Определение полномочий Банка России в отношении поднадзорных организаций, нарушающих требования ФЗ или нормативных документов Банка России.

Данный закон определяет, что должны быть реализованы технические, организационные и правовые меры, и направлены они должны быть на:

- на защиту информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении информации;
- соблюдение конфиденциальности информации;
- реализацию права на доступ к информации в соответствии с законодательством РФ.

Выводы

В СЭК применяется концепция *B2C* – построение коммерческих взаимоотношений между СЭК (*Business*) и потребителем (*Consumer*).

Отношения между объектами СЭК очень важны, так как они дают представление не только о последовательности и информации, которая передается между ними, но и понимание о потенциальных угрозах.

По статистике инцидентов СЭК были определены десять распространенных угроз для безопасности. А также анализ показал, что количество атак на СЭК возрастает, что говорит о повышении

ценности электронной информации. Поэтому необходимо очень серьезно относится к вопросу о защите информации на всех участках ее функционирования.

Существует множество стандартов в области безопасности. Некоторые дополняют друг друга, а некоторые противоречат. Поэтому, для выполнения заказов, особенно иностранных, необходимо использовать стандартизированные документы международных компаний.

Для обеспечение информационной безопасности, организации необходимо сформировать политику безопасности. Политика безопасности – методы, средства, а также деятельность самих субъектов, которые направлены на обеспечении информационной безопасности. Политика безопасности подразумевает проведение аудита ИБ. Были выделены следующие принципы проведение аудита: независимость, полнота, достоверность, компетентность и этичность.

В СЭК очень важную роль играют ПС, так как в них вся оплата, перевод денежных средств происходит безналичным расчетом. Поэтому рассмотрев закон ФЗ-161 было определено, что необходимо соблюдать конфиденциальность информации, как со стороны сотрудников, так и со стороны потребителей (например: никому не сообщать свой пароль), защита информации в ПС должна быть надежно защищена от неправомерных действий различного рода, а также, что права на доступ к информации должна соответствовать законодательству РФ.

Список литературы

1. A.Singhal, T. Winograd, K. Scarfone. Guide to Secure Web Services Recommendations of the National Institute of Standards and Technology. — [Электронный ресурс]. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf. — (дата обращения: 15.05.2017).
2. E-commerce Blog. Стандарты безопасности при разработке интернет-сайтов и веб приложений, OWASP. — [Электронный ресурс]. URL: http://www.siteprojects.ru/blog/. — (дата обращения: 15.05.2017).
3. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования.
4. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
5. Официальный сайт компании InfoWatch. — [Электронный ресурс]. URL: https://www.infowatch.ru//. — (дата обращения: 25.05.2017).
6. Федеральная служба по техническому и экспортному контролю. Приказ об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. — [Электронный ресурс]. URL: http://fstec.ru/. — (дата обращения: 16.05.2017).
7. Федеральный закон № 161 от 27.06.2011 «О национальной платежной системе».