



SmartCard-Service

Акционерное общество «СмартКард-Сервис»

127106, г. Москва, Алтуфьевское шоссе, д. 1

Телефон: +7 (495) 981-12-10, 8 (800) 100-31-64, факс: +7 (495) 981-12-11

E-mail: reception@scserv.ru, site: www.scserv.ru

У Т В Е Р Ж Д Е Н О

Генеральный директор

АО «СмартКард-Сервис»

\_\_\_\_\_ В.А. Васильев

№ \_\_\_\_\_ «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г.

## Программное обеспечение «АТ-NFC»

# ПОЛИТИКА ОБУЧЕНИЯ И ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ВОПРОСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Файл: политика обучения и повышения осведомленности.docx

СОГЛАСОВАНО

Технический директор

\_\_\_\_\_ В.В. Петров

«\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г.

СОГЛАСОВАНО

Заместитель

Генерального директора

\_\_\_\_\_ О.В. Андряков

«\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г.

Москва  
2023

## СОДЕРЖАНИЕ

1. Сведения о документе.....	3
2. Список терминов и сокращений .....	3
3. Назначение и область применения .....	4
4. методы и средства повышения осведомленности сотрудников в области ИБ .....	4
5. Требования к процессу повышения осведомленности сотрудников в области ИБ.....	5
Приложение 1. Программа внутреннего обучения сотрудников АО «СмартКард-Сервис» принципам безопасного программирования .....	8
Приложение 2. Отчет по внутреннему обучению сотрудников АО «СмартКард-Сервис» принципам разработки безопасного ПО .....	<b>Ошибка! Закладка не определена.</b>
6. История изменений документа .....	13

## 1. СВЕДЕНИЯ О ДОКУМЕНТЕ

Номер версии:	01.01
Дата выпуска:	28.12.2023 г.
Дата утверждения:	
Частота пересмотра:	<p>— 1 раз в год;</p> <p>— в случае существенных изменений в информационной инфраструктуре или организационной структуре Компании;</p> <p>— в случае выявления инцидентов информационной безопасности, свидетельствующих о неполноте или несовершенстве настоящей Политики</p>

## 2. СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Расшифровка сокращения
PCI SSF	Семейство стандартов, направленных на обеспечение безопасности программного обеспечения (PCI Software Security Framework), на данный момент состоит из двух связанных между собой стандартов — Secure Software Standard (SSS) и Secure Software Lifecycle (Secure SLC) Standard.
PCI SSS	Стандарт безопасности данных программного обеспечения индустрии платежных карт (Payment Card Industry Security Software Standard)
PCI SLC	Стандарт, который определяет безопасные методы управления жизненным циклом платёжного ПО, позволяющие гарантировать вендору такого ПО, что оно спроектировано и разработано для защиты платежных транзакций и данных, минимизации уязвимостей и защиты от атак.
ПО	Программное обеспечение
ПО «АТ-NFC»	Программное обеспечение «АТ-NFC»
УС	Устройство самообслуживания
ИБ	Информационная безопасность
Компания	АО «СмартКард-Сервис»

### 3. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Компания АО «СмартКард-Сервис» прилагает необходимые усилия для обеспечения защиты конфиденциальности, целостности и доступности исходных кодов посредством разработки, внедрения и периодической переоценки программы осведомленности и обучения работников Компании, включая руководителей структурных подразделений в части обеспечения ИБ Компании.

Внедрение программы повышения осведомленности персонала в вопросах ИБ осуществляется в целях сокращения числа нарушений ИБ в Компании и снижения возможных рисков и угроз, связанных с нарушением требований ИБ работниками Компании.

Мероприятия, направленные на повышение осведомленности работников в сфере ИБ, должны охватывать весь персонал Компании.

### 4. МЕТОДЫ И СРЕДСТВА ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ В ОБЛАСТИ ИБ

К методам повышения осведомленности персонала могут относиться:

- реализация программ дистанционного обучения внутри Компании;
- организация информационных разделов по вопросам ИБ (раздел по безопасности в базе нормативных актов, страница ИБ на внутреннем портале и т. д.);
- проведение вводных инструктажей по ИБ для новых работников Компании;
- проведение периодических инструктажей, обучений и тренингов;
- распространение плакатов, специализированных компьютерных заставок и других средств наглядной агитации;
- проведение тематических рассылок и уведомлений по электронной почте для работников Компании;
- ознакомление под подпись персонала с новыми нормативными актами Компании, регламентирующими процессы обеспечения ИБ;
- проведение периодического письменного или электронного тестирования работников на предмет знания установленных требований ИБ;
- обучающие видеоролики;
- прочие методы.

С целью лучшего доведения материала до работников Компании, подготавливаемые для обучения материалы должны включать:

- основные методы действия злоумышленников;
- способы противодействия нарушителям ИБ;
- описание типичных ошибок пользователей информационных систем;
- обсуждение конкретных примеров ошибочных действий персонала и их последствий;
- обоснование причин введения конкретных правил и ограничений в нормативных актах Компании в области ИБ и необходимости их сознательного соблюдения.

Основные требования к программе повышения осведомленности персонала:

- предоставление возможности регулярного повышения осведомленности работников вне зависимости от их территориального местонахождения и без отрыва от рабочего процесса;
- преподнесение материала пользователям в простой и понятной форме;
- использование методов, делающих процесс повышения осведомленности увлекательным и интересным.

## 5. ТРЕБОВАНИЯ К ПРОЦЕССУ ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ В ОБЛАСТИ ИБ

Процесс повышения осведомленности работников Компании в области ИБ включает в себя:

- вводные инструктажи работников при приеме на работу;
- периодическое (не реже 1 раза в год) плановое, а также внеплановое обучение работников действующим требованиям ИБ;
- периодическое плановое обучение работников, участвующих в разработке ПО;
- периодическое плановое обучение работников Компании, ответственных за обеспечение ИБ.

Нормативные документы, регламентирующие процессы обеспечения ИБ в Компании, должны быть доступны для ознакомления для всех работников, на которых возлагается ответственность за исполнение и поддержание соответствующих процессов.

После проведения обучения необходимо (в зависимости от метода обучения) обеспечить регистрацию записей, подтверждающих проведение обучения.

По окончании обучения может быть проведена проверка полученных знаний путем проведения тестирования.

Каждый работник Компании, получающий доступ к активам Компании, должен проходить вводный инструктаж по ИБ и получать вспомогательные материалы, позволяющие ему выполнять свои функции, соблюдая правила и политики ИБ, установленные в Компании. Вводные инструктажи проводятся ответственным работником по обучению путем показа обучающего видеоролика.

Обучение работников Компании новым требованиям ИБ проводится работниками отдела ИБ, и может быть вызвано:

- изменением и пересмотром политик и процедур ИБ;
- внедрением новых механизмов и средств ИБ;
- значимыми изменениями используемых механизмов и средств ИБ;
- изменением требований законодательства, международных платежных систем и контрактных обязательств Компании в отношении ИБ;
- возникновением новых (изменения старых) угроз и уязвимостей ИБ в отношении активов Компании.

Детальное разъяснение требований ИБ проводится в рамках планового и внепланового обучения работников Компании действующим требованиям ИБ.

Программа обучения работников в области ИБ на предстоящий год составляется специалистом отдела ИБ, согласуется с руководителями вовлеченных подразделений и утверждается менеджером по управлению отделом ИБ.

Программа должна определять:

- план обучения (дата/время, основные темы, источники информации);
- ответственного за организацию обучения;
- ожидаемые результаты;
- отчетные материалы по результатам обучения.

План обучения должен быть направлен на поддержку и развитие навыков и компетенций работников, соответствующих их должностным обязанностям и/или выполняемой роли.

Все работники должны проходить обучение, соответствующее их должностным обязанностям и/или выполняемой роли.

Менеджер по управлению отделом ИБ определяет необходимую периодичность проведения обучения ИБ исходя из результатов мониторинга инцидентов ИБ, внутренних и внешних аудиторских проверок состояния системы ИБ Компании.

Обучение для всех работников должно включать осведомленность и знание политик, правил и процедур обеспечения ИБ, установленных в Компании.

Все работники, участвующие в разработке ПО, должны проходить обучение приемам и практикам безопасного программирования. А так же, на ежегодной основе, дополнительное ознакомление с новыми видами уязвимостей и практиками защиты от них.

Обучение для работников, участвующие в разработке ПО должно включать следующие темы:

- требования стандарта PCI SSS, краткий обзор PCI SSF;
- обеспечение безопасности при проектировании ПО;
- методы и практики безопасного программирования;
- обработка критичных данных ПО;
- анализ безопасности исходного кода;
- тестирование безопасности ПО;
- оценка рисков и моделирование угроз ПО;

Материалы для организации внутреннего обучения:

- [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);
- <http://projects.webappsec.org/w/page/13246978/Threat-Classification>;
- <http://www.cert.org/secure-coding/>;
- <http://cwe.mitre.org/data/graphs/699.html>.

Может быть организовано внешнее обучение работников, направленное на повышение осведомленности в области ИБ. Программа обучения должна включать в себя основные понятия ИБ, определение места и роли конечных пользователей в системе обеспечения ИБ Компании, рассмотрение типичных ошибок — нарушений правил ИБ и путей их предотвращения.

По результатам обучения может быть проведено тестирование уровня усвоения материала.

С целью обеспечения поддержания квалификации на должном уровне, работники отдела ИБ (в том числе работники, ответственные за реагирование на инциденты ИБ), обязаны

проходить регулярное внешнее обучение. Темы обучения определяются Менеджером по управлению отделом ИБ и зависят от текущей квалификации работника и возложенных на него обязанностей.

ПРИЛОЖЕНИЕ 1

**Программа внутреннего обучения сотрудников АО «СмартКард-Сервис»  
принципам безопасного программирования**

Тема	План	Время
Стандарты PCI SSF и PCI SSS	<ol style="list-style-type: none"> <li>1. Основные положения стандартов PCI SSF и PCI SSS.</li> <li>2. Связь между стандартами PCI SSF и PCI SSS.</li> <li>3. Рамки действия стандарта PCI SSS.</li> <li>4. Требования стандарта PCI SSS.</li> <li>5. Подробнее рассмотреть требования стандарта, касаемые разработки ПО</li> </ol>	1,5 ч.
Наиболее опасные ошибки при разработке ПО (CWE/SANS TOP 25 Most Dangerous Software Errors)	<p>The Top 25 Software Errors in three categories:</p> <ol style="list-style-type: none"> <li>1. Insecure Interaction Between Components (6 errors);</li> <li>2. Risky Resource Management (8 errors);</li> <li>3. Porous Defenses (11 errors)</li> </ol>	2 ч.
Статический анализ кода (Static Code Analysis)	<ol style="list-style-type: none"> <li>1. Что такое САК? Последовательная цепочка «Анализ ПО» – «Анализ с запуском» (динамический) – «Анализ без запуска» (статический). Статический анализ в свою очередь делится на ручной (ревью (понимание) кода) и автоматизированный (САК).</li> <li>2. В чем польза? Основная мысль – чем раньше обнаруживаем ошибку, тем дешевле её исправить.</li> <li>3. Какие проблемы и дефекты кода помогает обнаружить? Несколько примеров, как САК помогает найти использование неинициализированных переменных, угрозы инъекции и пр.</li> <li>4. Как он это делает? Три этапа статического анализа: лексический, синтаксический и статистический</li> <li>5. Какие алгоритмы бывают? Собственно, не вдаваясь в глубокие подробности.</li> <li>6. Какие средства можно использовать? Обзор статических анализаторов: под разные языки/платформы, с разным уровнем анализа и т.д. Что умеют делать конкретные статические анализаторы, как запускаются, какой результат работы анализатора.</li> <li>7. Возможные проблемы Обзор неудачных сценариев перехода и/или использования САК.</li> <li>8. Заключение Подведение итогов</li> </ol>	1,5 ч.



Тема	План	Время
Инспекции кода (OWASP Code Review Guide)	<ol style="list-style-type: none"> <li>1. Methodology <ul style="list-style-type: none"> <li>• Security Code Review in the SDLC;</li> <li>• Security Code Review Coverage;</li> <li>• Application Threat Modeling.</li> </ul> </li> <li>2. Crawling Code <ul style="list-style-type: none"> <li>• Crawling Code;</li> <li>• Searching for Code in J2EE/Java;</li> <li>• JavaScript/Web 2.0 Keywords and Pointers.</li> </ul> </li> <li>3. Code Reviews and PCI SSF</li> <li>4. Examples by Technical Control</li> <li>5. Examples by Vulnerability</li> <li>6. Language Specific Best Practice: <ul style="list-style-type: none"> <li>• Java Gotchas;</li> <li>• Leading Java Security Practice;</li> <li>• Rich Internet Applications.</li> </ul> </li> <li>7. Automating Code Reviews</li> </ol>	1,5 ч.

ПРИЛОЖЕНИЕ 2

**Отчет**  
**по внутреннему обучению сотрудников АО «СмартКард-Сервис»**  
**принципам разработки безопасного ПО**

Обучение проводилось с 04 декабря 2023 г. по 18 декабря 2023 г. в офисе АО «СмартКард-Сервис» в форме тренингов и семинаров силами сотрудников Отдела разработки и Отдела сопровождения программного обеспечения.

Контроль результатов по отдельным темам осуществлялся ответственным за обучение путем тестирования или устной проверки знаний Программы обучения.

**Тема № 1: «Семейство стандартов PCI SSF»**  
04.12.2023 г., 1,5 часа

**План**

1. Основные положения семейства стандартов PCI SSF.
2. Требования стандарта PCI SSS.
3. Требования стандарта PCI Secure SLC.

**Ответственный:** Сорокин В.С.

**Участники:** Петров В.В., Ефимов О.В., Якушкин К.Л., Прокопенко А.Ю., Лапушкин С.М., Цвентарный А.Г., Сажнев А.В., Кирао А.В., Чубуков А.Б., Евтеев А.И., Ючкин Е.Б., Богданов Д.Д., Чиракадзе А.Г., Андрияков О.В., Браславский В.Н., Попов С.Ю., Гунин С.Ю., Юрцев С.В., Карускевич А.В., Быкова А.В., Колодкин К.Д., Морозов И.В.

**Контроль результатов:** тестирование

**Тема № 2: «Наиболее опасные ошибки при разработке ПО**  
**(CWE/SANSTOP 25 MostDangerousSoftwareErrors)»**  
07.12.2023г., 2 часа

**План**

The Top 25 Software Errors in three categories:

1. Insecure Interaction Between Components (6 errors);
2. Risky Resource Management (8 errors);
3. PorousDefenses (11 errors)

**Ответственный:** Сорокин В.С.

**Участники:** Петров В.В., Ефимов О.В., Якушкин К.Л., Прокопенко А.Ю., Лапушкин С.М.

**Контроль результатов:** тестирование



### Тема № 3: «Статический анализ кода (StaticCodeAnalysis)»

11.12.2023 г., 1,5 часа

#### План

1. Что такое статический анализ кода (САК)?
2. В чем польза САК?
3. Какие проблемы и дефекты кода помогает обнаружить САК?
4. Как САК это делает?
5. Какие алгоритмы бывают?
6. Какие средства можно использовать?
7. Возможные проблемы.
8. Заключение.

**Ответственный:** Сорокин В.С.

**Участники:** Петров В.В., Ефимов О.В., Якушкин К.Л., Прокопенко А.Ю., Лапушкин С.М., Ючкин Е.Б., Богданов Д.Д., Чиракадзе А.Г.

**Контроль результатов:** тестирование

### Тема № 4: «Инспекции кода (CodeReviews)»

14.12.2023г., 1,5 часа

#### План

1. Methodology.
2. Crawling Code.
3. Code Reviews and PCI SSF.
4. Examples by Technical Control.
5. Examples by Vulnerability.
6. Language Specific Best Practice.
7. Automating Code Reviews.

**Ответственный:** Сорокин В.С.

**Участники:** Петров В.В., Ефимов О.В., Якушкин К.Л., Прокопенко А.Ю., Лапушкин С.М., Ючкин Е.Б., Богданов Д.Д., Чиракадзе А.Г.

**Контроль результатов:** индивидуальные задания для проведения взаимных инспекций кода в ClearCaseTools (утилита - ClearCase DiffMerge tool).

## 6. ИСТОРИЯ ИЗМЕНЕНИЙ ДОКУМЕНТА

Дата изменений	Версия док-та	Описание изменений
18.08.2021	01.00	Исходная редакция документа, разработанная с учетом требований PCI DSS (версия 3.2.1) и PA-DSS (версия 3.2)
28.12.2023	01.01	Внесены корректировки, учитывающие требования PCI DSS (версия 4.0), PCI SLC v.1.1 и PCI SSS v.1.2.1 Обновлено Приложение 2.