РАЗДЕЛ V.
МОЛОДЫЕ УЧЕНЫЕ – ПОИСК САМООПРЕДЕЛЕНИЯ

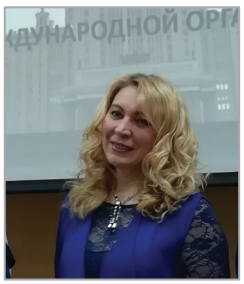
АЛГОРИТМ ПОСТРОЕНИЯ ПРОФИЛЕЙ ЗАЩИТЫ И ЗАДАНИЙ ПО БЕЗОПАСНОСТИ БАНКОВСКОГО ПО

Александрова Алина Викторовна
Студентка 5-го курса, направление «Информационная безопасность автоматизированных систем», Московский политехнический университет

Широков Анатолий Александрович
Студент 5-го курса, направление «Информационная безопасность автоматизированных систем», Московский политехнический университет

Соболь Дмитрий Викторович
Студент 5-го курса, направление «Информационная безопасность автоматизированных систем», Московский политехнический университет

Федоров Николай Владимирович
Кандидат технических наук, заведующий кафедрой «Информационная безопасность», Московский политехнический университет



Бритвина Валентина Валентиновна
Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»

Аннотация: В проекте проведен анализ и разработан алгоритм построения профилей защиты и заданий по безопасности банковского ПО. Отсутствие аналогичных решений, повышение по-

требностей с выходом новых положений 683-П и 684-П, легкость и доступность использования, передачи и поддержания нашего решения позволяет получить спрос при выходе на рынок. Практическая значимость проекта заключается в ускоренном формировании документов, доступности необходимых данных и компонентов, а также в легкости администрирования решения, что позволит поддерживать сайт в актуальном состоянии. Результатом работы является создание программного алгоритма для построения профилей защиты и заданий по безопасности банковского ПО. Для алгоритма были использованы описанные в работе ГОСТы, готовые и утвержденные ФСТЭК профили защиты, а также созданная база данных, которая содержала среду безопасности, цели безопасности, функциональные требования безопасности и требования доверия. Итогом работы является полноценный алгоритм, при использовании которого, происходит создание профилей защиты согласно всем ГОСТам.

Ключевые слова: Профиль защиты, задание по безопасности, база данных, среда безопасности, цели безопасности, функциональные требования, оценочный уровень доверия.

Abstract: The project analyzes and develops an algorithm for constructing protection profiles and tasks for the security of banking software. Lack of similar solutions, increased needs with the release of new provisions 683-P and 684-P, ease and availability of use, transmission and maintenance of our solution allows us to get demand when entering the market. The practical significance of the project lies in the accelerated formation of documents, the availability of the necessary data and components, as well as the ease of administration of the solution, which will keep the site up to date. The result of the work is the creation of a software algorithm for building protection profiles and tasks for the security of banking software. For the algorithm, the GOSTs described in the work, ready-made and approved by FSTEC protection profiles, as well as the created database, which contained the security environment, security objectives, functional security requirements and trust requirements, were used. The result of the work is a full-fledged algorithm, when using which, protection profiles are created in accordance with all GOSTs.

Keywords: Security Profile, Security Target, Database, Security Environment, Security Objectives, Functional Requirements, Assessment Level of Trust.

Цель исследования

Смоделировать программу и базу данных для построения профилей защиты и заданий по безопасности банковского ПО

Задачи

1. Сформировать алгоритм построения профилей защиты на основе существующих ГОСТов.
2. Проанализировать сформированные профилей защиты ФСТЭК.
3. Разработать архитектуру базы данных.

Введение

Все больше программ и приложений для автоматизации бизнес-процессов от различных вендоров набирают популярность на ИТ-рынке. Правильно разработанная программа позволяет сэкономить большое количество денег для руководства и человеко-часов для менеджеров проекта. Также стоит брать во внимания новые положения от исполнительных органов, которые необходимо учитывать различным компаниям и государственным учреждениям для повышения уровня безопасности информации. Однако приведение в соответствие с этими положениями занимает много времени по разным причинам. Такими причинами может являться сложность выполнения новых обязательств, недопонимание требований или невозможность выполнить новое постановление из-за введённых ранее требований [4]. Для исключения таких ситуаций часто основной объем работы отдается специально разработанным программам, по выполнению которых итоговый результат проверяется специалистом.

Формирование алгоритма построения профилей защиты на основе существующих ГОСТов

Для создания алгоритма был взят ГОСТ Р 57628-2017 «Методы и средства обеспечения безопасности» [1]. Руководство по разработке профилей защиты и заданий по безопасности». В нем детально расписываются необходимые действия специалисту ИБ для создания профиля защиты. Также методика определяет несколько функциональных требований безопасности, которые мы классифицируем как «рубрики требований безопасности»:

- Управление доступом;
- Собственная защита ОО;
- Защита каналов связи;
- Аудит безопасности;
- Требования к архитектуре объекта оценки.

На основании ГОСТ Р ИСО/МЭК 15408-2-2013 в базу данных были введены «Рубрики требований безопасности», а также организована связь «один-ко-многим» с функциональных требований безопасности [2]. Благодаря этому происходит классификация по «рубрикам требований безопасности» (рис. 1).

ГОСТ Р 57628-2017 и наш алгоритм устанавливает три меры для целей безопасности [1]:

- Предупреждение;
- Обнаружение;
- Реагирование.

Таблица 2 — Управление доступом

Требование	Применимые компоненты
Определение субъектов, объектов, операций	FDP_ACC.1, FDP_ACC.2, FDP_IFC.1, FDP_IFC.2, FMT_SMF.1
Определение атрибутов безопасности	FDP_DAU.1, FDP_DAU.2, FDP_IFF.1, FDP_IFF.2, FRU_PRS.1, FRU_PRS.2, FRU_RSA.1, FRU_RSA.2

Окончание таблицы 2

Требование	Применимые компоненты
Создание субъектов, объектов	FDP_ITC.1, FDP_ITC.2, FMT_SMF.1
Экспортирование объектов	FDP_ETC.1, FDP_ETC.2
Управление атрибутами безопасности	FDP_ITC.2, FIA_USB.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1, FTA_LSA.1
Определение правил доступа	FDP_ACF.1, FDP_IFF.1, FDP_IFF.2, FDP_ROL.1, FDP_ROL.2, FRU_PRS.1, FRU_PRS.2, FRU_RSA.1, FRU_RSA.2
Управление правилами управления доступом	FMT_MOF.1, FMT_SMF.1

Таблица 3 — Управление пользователями

Требование	Применимые компоненты
Определение типов пользователей	FMT_SMF.1
Определение атрибутов безопасности	FIA_ATD.1
Правила идентификации пользователей	FIA_UID.1, FIA_UID.2
Правила аутентификации пользователей	FIA_AFL.1, FIA_SOS.1, FIA_SOS.2, FIA_UAU.1, FIA_UAU.2, FIA_UAU.3, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7
Управление учетными данными и атрибутами безопасности пользователей	FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1, FMT_SMR.1, FMT_SMR.2, FMT_SMR.3, FTA_LSA.1, FTA_MCS.1, FTA_MCS.2
Управление правилами идентификации и аутентификации	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1
Управление связями пользователь — субъект	FIA_USB.1

Таблица 4 — Собственная защита ОО

Требование	Применимые компоненты
Обнаружение неисправности	FPT_TEE.1, FPT_ITI.2, FPT_ITT.3, FPT_PHP.1, FPT_PHP.2, FPT_PHP.3, FPT_RPL.1, FPT_TST.1, FRU_FLT.1, FRU_FLT.2
Реагирование на неисправность	FPT_ITT.3, FPT_PHP.2, FPT_PHP.3, FPT_RCV.1, FPT_RCV.2, FPT_RCV.3, FPT_RCV.4, FPT_RPL.1, FRU_FLT.1, FRU_FLT.2
Управление правилами обнаружения и реагирования	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1

Таблица 5 — Защита каналов связи

Требование	Применимые компоненты
Установление канала связи	FMT_SMF.1, FTP_ITC.1, FTP_TRP.1
Определение свойств канала связи (атрибутов безопасности)	FCO_NRO.1, FCO_NRO.2, FCO_NRR.1, FCO_NRR.2, FDP_UTC.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FPT_ITC.1, FPT_ITI.1, FPT_ITI.2, FPT_RPL.1, FTP_ITC 1, FTP_TRP.1
Управление свойствами канала связи	FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1
Управление правилами установления связи	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1, FTA_SSL.1, FTA_SSL.2, FTA_SSL.3, FTA_SSL.4, FTA_TAB.1, FTA_TAH.1, FTA_TSE.1

Таблица 6 — Аудит

Требование	Применимые компоненты
Определение событий, подлежащих аудиту	FAU_GEN.1, FAU_GEN.2, FAU_SEL.1
Определение реагирования на события	FAU_ARP.1, FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4
Определение управления событиями	FAU_SAR.1, FAU_SAR.2, FAU_SAR.3
Определение управления журналом аудита	FAU_STG.1
Управление правилами аудита	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3

Таблица 7 — Требования к архитектуре

Требование	Применимые компоненты
Защита журнала аудита	FAU_STG.2, FAU_STG.3, FAU_STG.4
Управление информационными потоками	FDP_IFF.3, FDP_IFF.4, FDP_IFF.5, FDP_IFF.6
Передача данных внутри ОО	FDP_ITT.1, FDP_ITT.2, FDP_ITT.3, FDP_ITT.4
Защита остаточной информации	FDP_RIP.1, FDP_RIP.2
Целостность хранимых данных	FDP_SDI.1, FDP_SDI.2
Управление	FMT_MTD.1
Защита конфиденциальности	FPR_ANO.1, FPR_ANO.2, FPR_PSE.1, FPR_PSE.2, FPR_PSE.3, FPR_UNL.1, FPR_UNO.1, FPR_UNO.2, FPR_UNO.3, FPR_UNO.4
Сбой безопасности	FPT_FLS.1
Доступность	FPT_ITA.1, FPT_ITT.1, FPT_ITT.2
Синхронизация состояния	FPT_SSP.1, FPT_SSP.2
Надежные метки времени	FPT_STM.1
Непротиворечивость данных	FPT_TDC.1, FPT_TRC.1

Рис. 1. Связь функциональных требований безопасности с рубриками

Таблица 5 — Защита каналов связи

Требование	Применимые компоненты
Установление канала связи	FMT_SMF.1, FTP_ITC.1, FTP_TRP.1
Определение свойств канала связи (атрибутов безопасности)	FCO_NRO.1, FCO_NRO.2, FCO_NRR.1, FCO_NRR.2, FDP_UTC.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FPT_ITC.1, FPT_ITI.1, FPT_ITI.2, FPT_RPL.1, FTP_ITC 1, FTP_TRP.1
Управление свойствами канала связи	FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1
Управление правилами установления связи	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1, FTA_SSL.1, FTA_SSL.2, FTA_SSL.3, FTA_SSL.4, FTA_TAB.1, FTA_TAH.1, FTA_TSE.1

Рис. 2. Функциональные требований безопасности из рубрики «Защита каналов связи»

Эти меры необходимы для категорирования целей безопасности по этапам их работоспособности. Благодаря этим этапам проще реализовывается управление требованиям безопасности.

Основываясь на описанной методике нами создается новый, программный алгоритм, который использует в качестве входных данных среду безопасности для создания профилей защиты. Среда безопасности делится на внутреннюю и внешнюю. Во внешнюю среду входят:

- Угрозы безопасности, которым должна противостоять среда функционирования объекта оценки;
- Предположения о среде.

А во внутреннюю среду входят:

- Угрозы безопасности, которым необходимо противостоять средствами объекта оценки
- Политики безопасности организации.

При определении среды безопасности осуществляется формирование целей безопасности объекта оценки, при условии, что среди выбранных параметров есть те, которые были сформированы и связанны нами позже [3].

В зависимости от сформированных целей безопасности для пользователя формируются функциональные требования безопасности, которые необходимо связать с целями по связи «один к многому». В качестве примера ниже приведена вырезка этих требований из рубрики «Защита каналов связи» (рис. 2).

Эти требования формируются благодаря указанной пользователем рубрикой у каждого элемента

среды безопасности. Специалист прикрепляет к каждой цели безопасности функциональное требования, основываясь на описание цели.

Далее определяются компоненты оценочного уровня доверия. При проектировании профиля защиты специалист устанавливает изначальный оценочный уровень доверия. Каждый такой уровень имеет определенный шаблон компонентов, описанных в ГОСТ 15408-3. Данный ГОСТ использовался нами для заполнения базы данных элементами, необходимых для корректной работы алгоритма.

ГОСТ Р ИСО/МЭК 15408 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. делится на три части [2]:

1. Введение и общая модель.
2. Функциональные компоненты безопасности.
3. Компоненты доверия к безопасности.

ИСО/МЭК 15408-1 содержит информацию:

- термины, используемые в стандарте, определены в разделе 3 ИСО/МЭК 15408-1;
- структура ЗБ приведена в приложении А к ИСО/МЭК 15408-1;
- структура ПЗ приведена в приложении В к ИСО/МЭК 15408-1.

Также в данном документе описан возможный способ последовательного формирования требований безопасности и спецификаций при разработке ПЗ и ЗБ (рис. 3).

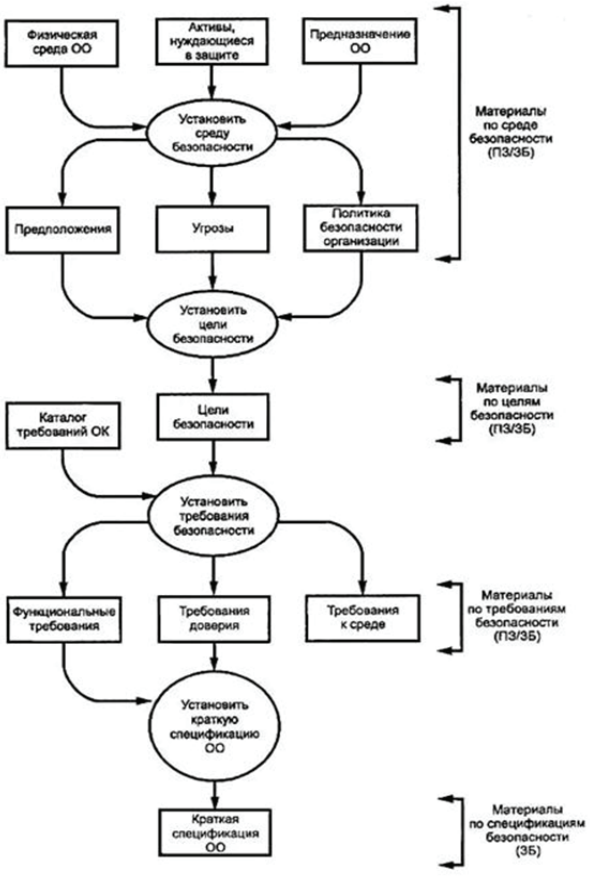


Рис. 3. Последовательное формирование требований и спецификаций

ГОСТ Р 57628-2017 Информационная технология (ИТ). Методы и средства обеспечения безопасности [1]. Руководство по разработке профилей защиты и заданий по безопасности дает общее понятие о процессе разработки профилей защиты и заданий по безопасности и описано это в следующих пунктах:

a) первоначальное определение проблемы безопасности;

b) идентификация целей безопасности, направленных на решение проблемы безопасности;

c) формирование требований безопасности, направленных на удовлетворение целей безопасности для ОО;

d) выбор конкретных функциональных возможностей безопасности, направленных на выполнение требований безопасности.

Также в этом документе говориться, что процесс разработки ПЗ или ЗБ может также включать в себя внесение изменений в документ при появлении новой информации в рамках проблемы безопасности для того чтобы отразить такие изменения как:

a) идентификацию новых угроз;

b) изменение ПБОр;

c) изменения в распределении задач по обеспечению безопасности информации, возлагаемой соответственно на ОО и среду ОО, связанные со стоимостными и временными ограничениями;

d) корректировку проблемы безопасности для ОО вследствие изменения предполагаемого потенциала нападения нарушителя.

Анализ сформированных профилей защиты ФСТЭК

В зависимости от года и типа профиля защиты были сформированы разные виды документов. В каждом наборе документов присутствуют и отсутствуют определённые главы и от этого немного видоизменяется структура. Анализ сформированных профилей защиты ФСТЭК заключает в себя поиск элементов связи между разными компонентами внутри документов для определения неизменяемой структурной связи [5].

Все усложняется тем, что от выбора специалистом компонентов профиля защиты меняется содержимое документов. На рисунке ниже видны основные, зависящие от выбор специалистом, элементы (рис. 4).

Каждый категория — это зависимый элемент, который содержит в себе описательную характеристику документа.

- Наименование ПЗ — это название документа, которое формируется при определении специалистом других параметров;
- Тип ОС или тип МЭ — операционная система или межсетевой экран, предназначенные для конкретного выполнения своих функций (тип зависит от этих функций).
- Класс защиты — чем он выше (1 класс самый высокий) тем больше к нему требований
- Версия ПЗ — версия данного ПЗ
- Обозначение ПЗ — Краткое название ПЗ

2.1. Ссылка на профиль защиты

Наименование ПЗ:	Профиль защиты операционных систем типа «Б» четвертого класса защиты.
Тип ОС:	ОС типа «Б».
Класс защиты:	Четвертый.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.ОС.Б4.ПЗ.
Идентификация ОО:	ОС типа «Б» четвертого класса защиты.
Уровень доверия:	Оценочный уровень доверия 3 (ОУД3), усиленный компонентами ADV_FSP.4 «Полная функциональная спецификация», ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VAN.5 «Усиленный методический анализ», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы», AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы» и AVA_CCA_EXT.1 «Анализ скрытых каналов».

Рис. 4. Элементы Профиля защиты

- Идентификация ОО — тип ОС и класс защиты
- Уровень доверия — показывает какие компоненты доверия включены в данное ПЗ

Выделяются три основных типа ОС:

- операционная система общего назначения (тип «А») — операционная система, предназначенная для функционирования на средствах вычислительной техники общего назначения (автоматизированные рабочие места, серверы, смартфоны, планшеты, телефоны и иные);
- встраиваемая операционная система (тип «Б») — операционная система, встроенная (прошитая) в специализированные технические устройства, предназначенные для решения заранее определенного набора задач;
- операционная система реального времени (тип «В») — операционная система, предназначенная для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности.

Типы МЭ делятся на:

- МЭ типа «А» — это МЭ, применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы.
- МЭ типа «Б» — это МЭ, применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы.
- МЭ типа «В» — это МЭ, применяемый на узле (хосте) информационной системы.
- МЭ типа «Г» — это МЭ, применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера).
- МЭ уровня промышленной сети (тип «Д») — это МЭ, применяемый в автоматизированной системе управления технологическими или производственными процессами.

Однако стоит заметить, что хоть и профили защиты могут отличаться друг от друга, они все равно содержат определенные элементы профиля защиты, описанной в ГОСТ 15408 (рис. 5).

Рис. 5. Структура Профиля защиты

В профиле защиты описание всех новых, сформированных пользователем, требований безопасности размещается в приложениях к профилю защиты. Это сделано для четкого понимания и разделения новых компонентов от старых, утвержденных ГОСТ.

Выявлено, что в пункте «требования безопасности» компоненты доверия берутся из ОУД, а функциональные компоненты в зависимости от нужды в реализации целей безопасности.

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10
FAU_GEN.1							X			
FAU_GEN.2							X			
FAU_SAR.1							X			
FAU_SAR.2							X			
FAU_SAR.3							X			
FMT_MOF.1	X				X					
FMT_MTD.1	X				X					
FMT_MTD.2	X				X					
FMT_SMR.1						X				
FPT_TST.1	X							X		
FID_COL_EXT.2		X								
FID_ANL_EXT.2			X							
FID_MTH_EXT.1			X							
FID_MTH_EXT.2			X							
FID_RCT_EXT.1				X						
FID_PCL_EXT.1		X								
FID_CON_EXT.1					X					
FID_UPD_EXT.1										X
FID_INF_EXT.1									X	

Рис. 6. Пример связи функциональных компонентов с целями безопасности

Разработка архитектуры базы данных

После полной разработки алгоритма построения профиля защиты необходимо осуществить разработку и заполнение архитектуры базы данных (далее – БД). При разработке архитектуры БД необходимо обеспечить максимально корректную и быструю связь между объектами разных отношений-(таблиц) и избежать переполнения таблиц данными.

Для оптимальной работы базы данных были созданы следующие таблицы (рис. 7).

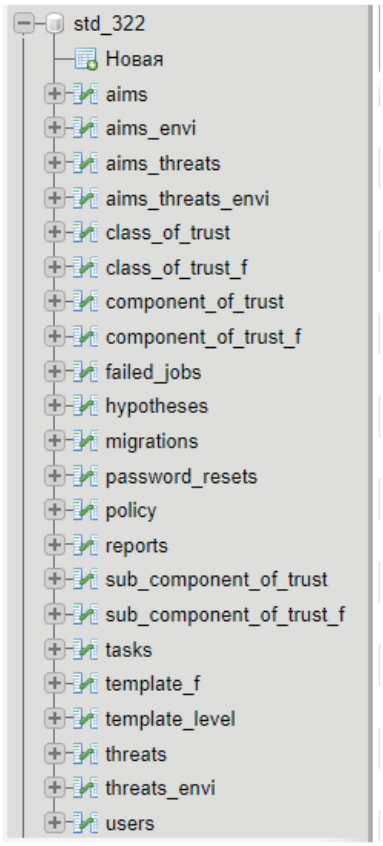


Рис. 7. Таблицы базы данных

На данных отношениях основан весь алгоритм построения ПЗ и ЗБ. Таблицы имеют связи между друг другом, что позволяет организовать взаимосвязь между такими объектами как «Угроза безопасности», «Политика безопасности» и «Цель безопасности».

На рис. 8–9 представлены примеры двух этих типов отношений.

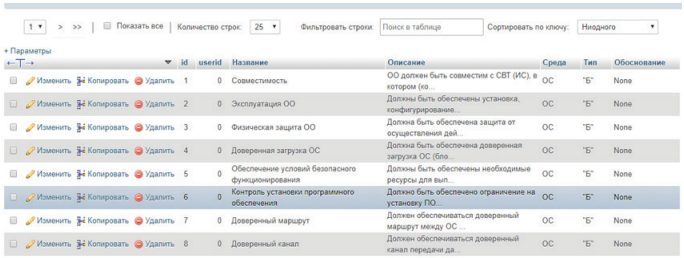


Рис. 8. Таблица для описания данных

В данной работе присутствует два вида отношений:

1) Для описания данных;
2) Для связи этих данных.

В первом случае в отношении прописываются данные, которые понадобятся при самом формировании ПЗ (таблицы наполняются информацией).

Второй тип таблиц служит только для обеспечения взаимосвязи между отношениями первого типа.

+ Параметры

	id	id_цели	id_угроз	id_политик
Изменить Копировать Удалить	1	1	1	1
Изменить Копировать Удалить	2	1	3	2
Изменить Копировать Удалить	3	1	4	0
Изменить Копировать Удалить	4	2	1	3
Изменить Копировать Удалить	5	2	2	4
Изменить Копировать Удалить	6	2	4	9
Изменить Копировать Удалить	7	2	5	0
Изменить Копировать Удалить	8	3	0	5
Изменить Копировать Удалить	9	4	0	6
Изменить Копировать Удалить	10	5	5	7
Изменить Копировать Удалить	11	5	0	10
Изменить Копировать Удалить	12	6	0	8
Изменить Копировать Удалить	13	7	6	11
Изменить Копировать Удалить	14	7	11	0
Изменить Копировать Удалить	15	7	12	0
Изменить Копировать Удалить	16	8	6	13

Рис. 9. Таблица для связи данных

Заключение

Цель и задачи, которые были поставлены в начале работы выполнены. Проанализированы профили защиты ФСТЭК, сформирован алгоритм построения профилей защиты на основе существующих ГОСТов, разработана архитектура базы данных. Данная работа была выполнена для экономии денежных ресурсов и человеко-часов для менеджеров проекта. Также разработанный алгоритм позволяет сэкономить большое количество времени если на предприятии вносятся какие-либо изменения, которые затрагивают средства профилей защиты.

Список литературы

1. ГОСТ Р 57628-2017 «Методы и средства обеспечения безопасности».
2. ГОСТ Р ИСО/МЭК 15408-2-2013.
3. **Наби Ф.** Процесс унификации свойств обеспечения безопасности для логики приложений / Ф. Наби, М. Наби // Международный журнал электроники и информационной инженерии. – 2017. – №6, С. 40–48.
4. **Kriaa, S., Pietre-Cambacedes, L., Bouissou, M.** и **Halgand, Y.** (2015) Обзор подходов, сочетающих безопасность и защищенность для промышленных систем управления. Надежность и безопасность систем, 139, 156-178.
5. Методический документ ФСТЭК России «Профиль защиты средств контроля подключения съемных машинных носителей информации пятого класса защиты» (ИТ.СКН.П5.ПЗ). – 2014.