МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный университет»

Институт цифровых технологий, электроники и физики

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ПРОЕКТУ

«Разработка методики оценки защищенности информационной системы по стандарту ГОСТ 57580. 1 - 2018, ГОСТ Р. 57580. 2 - 2018»

Исполнители:
Зубков П.А., 2 курс, 598 группа
Пикуль А.С., 2 курс, 598 группа

_____ (_____)

«12» _июня_ 2021 г.

Барнаул, 2021

Краткая аннотация проекта

Деятельности финансовой организации свойственен операционный риск, связанный с нарушением безопасности информации, что является объективной реальностью, и понизить этот риск можно лишь до определенного остаточного уровня. Для управления операционным риском, связанным с безопасностью информации, финансовой организации необходимо обеспечить:

1. Идентификацию и учет объектов информатизации, в том числе АС, включаемых в область применения настоящего стандарта в соответствии с требованиями нормативных актов Банка России, устанавливающих обязательность применения его положений;
2. Применение на различных уровнях информационной инфраструктуры выбранных финансовой организацией мер защиты информации, направленных на непосредственное обеспечение защиты информации и входящих в систему защиты информации;
3. Применение выбранных финансовой организацией мер защиты информации, обеспечивающих приемлемые для финансовой организации полноту и качество защиты информации, входящих в систему организации и управления защитой информации.

В случаях наступления инцидентов защиты информации их негативные последствия в работе отдельных финансовых организаций могут привести к быстрому развитию системного кризиса банковской системы, финансового рынка Российской Федерации и национальной платежной системы, нанести существенный ущерб интересам собственников и клиентов финансовых организаций. Поэтому для финансовых организаций угрозы безопасности информации представляют существенную опасность, а обеспечение защиты информации является для финансовых организаций одним из основополагающих аспектов их деятельности.

Для противостояния угрозам безопасности информации и их влиянию на операционный риск финансовым организациям следует обеспечить необходимый и достаточный уровень защиты информации, а также сохранять этот уровень при изменении условий как внутри, так и вне организаций.

Программа *«CoolProgram – расчет оценки защищенности информационной системы»* иллюстрирует работу модели. Она разработана с целью демонстрации преимуществ системного подхода к созданию и оценке эффективности систем защиты информации. С помощью указанной программы осуществляется расчет условных показателей эффективности СЗИ.

Программа *«CoolProgram – расчет оценки защищенности информационной системы»* реализована на языке программирования Python и предназначена для оценки эффективности мероприятий, проводимых при создании и функционировании систем защиты информации.

Предложенная модель СЗИ позволяет не только жестко отслеживать взаимные связи между элементами защиты, но может выступать в роли руководства по созданию СЗИ.

Если вы, приступая к созданию системы защиты, не знаете с чего начать, попробуйте ответить на предложенные вопросы, начиная с любого из них. И когда вы пройдетесь по всем вопросам, то поймете, что уже сделано, а чего не хватает для достижения поставленной цели.

Цели проекта

1. Объективная и независимая оценка выбора и реализации требований ГОСТ 57580. 1 – 2018 и ГОСТ Р. 57580. 2 - 2018;
2. Организационные и технические меры для: приведения в соответствие требованиям ГОСТ 57580. 1 – 2018 и ГОСТ Р. 57580. 2 – 2018 и Положениям Банка России, повышения уровня защищенности информации;
3. Определение уровней защиты информации и соответствующих им требований к содержанию базового состава организационных и технических мер защиты информации, применяемых финансовыми организациями;
4. Достижение адекватности состава и содержания мер защиты информации, применяемых финансовыми организациями, актуальным угрозам безопасности информации и уровню принятого финансовой организацией операционного риска;
5. Обеспечение эффективности и возможности стандартизированного контроля мероприятий по защите информации, проводимых финансовыми организациями.

Задачи проекта

1. Разработать модель угроз и нарушителя, определить контуры безопасности;
2. Сформировать «положение о применимости»;
3. Провести инвентаризацию объектов информатизации и АС, входящих в область оценки;
4. Разработать программу для расчета оценки защищенности информационной системы по стандарту ГОСТ 57580. 1 – 2018 и ГОСТ Р. 57580. 2 – 2018;
5. «Донастроить» встроенные средства защиты;
6. Подготовить сотрудников к возможному интервьюированию.

Мероприятия проекта

План:

1. Выбор проверяющей организации;
2. Область проверки;
3. Возможные результаты аудита;
4. Сроки прохождения аудита;
5. Рекомендации.

Кого нельзя привлекать к аудиту?

1. Организации, являющиеся зависимыми от проверяемой организации;
2. Организации, осуществлявшие или осуществляющие оказание услуг проверяемой организации в области реализации информатизации и защиты, и организации от них зависимые.

Чем можно руководствоваться?

1. Рекомендации Банка России;
2. Рекомендации в информационных письмах Банка России;
3. Методики ФСТЭК России;
4. Стандарты ГОСТ 57580. 1 – 2018 и ГОСТ Р. 57580. 2 – 2018.

Деятельность	Количество дней																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Составление плана проекта и его сроков																				
Изучение примеров методик оценивания защищенности ИС и ГОСТа																				
Создание оболочки программы																				
Привязывание созданной оболочки программы расчета к конкретным функциям расчета на языке Python																				
Создание примера для методики оценки защищенности ИС																				
Создание инструкции к написанной программе расчета																				
Создание отчета к проекту																				
Создание наглядной презентации																				

Рис. 1. Диаграмма Ганта для визуализации сроков разработки.

Инновационность

1) *Уникальность проекта, наличие конкурентов и похожих проектов.*

Аналогов данной программы в открытом доступе найдено не было. Даже если есть какие-то единичные программы, то они не касаются именно банковских систем и не подразумевают работу со стандартом. Соответствие стандарту, как правило, приносит много хлопот для банков.

2) *Наличие очевидной пользы для потребителя, заложенной в инновационном продукте.*

Для упрощения получения данной программы, она должна находиться в открытом доступе. Таким образом, если вернуться к первому пункту и учесть, что аналогов в открытом доступе почти не существует, то можно сказать, что для потребителя это дает дополнительные возможности для оценки. Так как достаточно лишь скачать программу, ознакомиться с минимальной инструкцией и получить приближенную оценку системы защиты.

Это выгодно, если начальник банка понимает, что скоро банк ожидает проверка, которая как раз и затрагивает стандарт.

Программа же упрощает этот процесс. В целом в стандарте около 100 страниц, которые нелегко воспринимается необученным в данной сфере человеком. Поэтому гораздо легче воспользоваться чем-то упрощенным, но не искажающим сути.

3) *Наличие потребности в продукте, портрет потребителя, объём рынка.*

В стране много банков – Государственных и негосударственных. Люди хранят деньги, но их хранение должно подразумевать безопасность.

Как известно, банки часто подвергаются различным атакам со стороны злоумышленников. Сюда входит кража денег, персональных данных. Если это случиться, то имидж банка пострадает. Это должны понимать руководители и задумываться о безопасности. В этом им может помочь разработанная нами программа.

4) *Юридическая защищенность проекта — соответствие законодательству.*

Очевидно, что программа соответствует законодательству, так как содержание программы целиком построено на стандарте. Сам стандарт утвержден Приказом Федерального агентства по техническому регулированию и метрологии, а разработан Центральным банком Российской Федерации.

Результаты, которые планируется достигнуть в рамках проекта

1. Отчет об аудите;
2. Числовые оценки соответствия с их обоснованием;
3. Заполненные листы сбора свидетельств;
4. Перечень выявленных нарушений;
5. Рекомендации по совершенствованию информационной системы;
6. Копии документов на бумажных носителях, машинные носители информации с информацией, предоставляемой в качестве свидетельств, проверяемой организацией.

Как будет реализовываться проект.
Работа с программой оценки

Оценку выбора финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации, осуществляют отдельно для следующих процессов ЗИ:

1. *Процесс 1* «Обеспечение защиты информации при управлении доступом»;
   1.1. *Подпроцесс 1* «Управление учетными записями и правами субъектов логического доступа»;
   1.2. *Подпроцесс 2* «Идентификация, аутентификация, авторизация при осуществлении логического доступа»;

1.3. *Подпроцесс 3* «Защита информации при осуществлении физического доступа»;
1.4. *Подпроцесс 4* «Идентификация и учет ресурсов и объектов доступа».

2. *Процесс 2* «Обеспечение защиты вычислительных сетей»;
   2.1. *Подпроцесс 1* «Сегментация и межсетевое экранирование вычислительных сетей»;
   2.2. *Подпроцесс 2* «Выявление вторжений и сетевых атак»;
   2.3. *Подпроцесс 3* «Защита информации, передаваемой по вычислительным сетям»;
   2.4. Подпроцесс 4 «Защита беспроводных сетей».
3. *Процесс 3* «Контроль целостности и защищенности информационной инфраструктуры»;
4. *Процесс 4* «Защита от вредоносного кода»;
5. *Процесс 5* «Предотвращение утечек информации»;
6. *Процесс 6* «Управление инцидентами защиты информации»;
   6.1. *Подпроцесс 1* «Мониторинг и анализ событий защиты информации»;
   6.2. *Подпроцесс 2* «Обнаружение инцидентов защиты информации и реагирование на них».
7. *Процесс 7* «Защита среды виртуализации»;
8. *Процесс 8* «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств».

Кроме того, для оценки защищенности ИС также учитываются оценки по следующим направлениям ЗИ системы организации и управления ЗИ:

1. *Направление 1* «Планирование процесса системы защиты информации»;
2. *Направление 2* «Реализация процесса системы защиты информации»;
3. *Направление 3* «Контроль процесса системы защиты информации»;
4. *Направление 4* «Совершенствование процесса системы защиты информации».

Для того чтобы получить общую оценку защищенности ИС для своей информационной системы, пользователю необходимо отметить пункты, которые соблюдены в его организации. Далее в полях ввода пользователю необходимо ввести оценки*, которые были рассчитаны в предыдущих подпроцессах, процессах или направлениях (какие именно оценки и где нужно записать, в программе будет указано). В результате пользователь получает общую оценку защищенности ИС в своей организации.

Для оценки полноты реализации процессов системы ЗИ используют следующую качественную модель оценивания:

1. Нулевой уровень соответствия *(оценка 0)*;
2. Первый уровень соответствия *(оценка от 0 до 0.5 включительно)*;
3. Второй уровень соответствия *(оценка от 0.5 до 0.7 включительно)*;
4. Третий уровень соответствия *(оценка от 0.7 до 0.85 включительно)*;
5. Четвертый уровень соответствия *(оценка от 0.85 до 0.9 включительно)*;
6. Пятый уровень соответствия *(оценка от 0.9 до 1 включительно).*

** Примечание: дробные числа необходимо вводить через точку (пример: 0.75).*

Общая оценка защищенности ИС в программе *«CoolProgram – расчет оценки защищенности информационной системы»* производится по формулам, описанным в стандартах ГОСТ 57580. 1 – 2018 и ГОСТ Р. 57580. 2 – 2018.

При создании программы *«CoolProgram – расчет оценки защищенности информационной системы»* нами было принято решение сократить количество пунктов, по которым оценивается защищенность ИС. Это было сделано в силу того, чтобы сократить время пользования программой, облегчить освоение программы, но качество оценки защищенности ИС при этом не пострадало, т.к. мы выделили и оставили наиболее важные пункты оценивания, а второстепенные и менее нужные – отбросили.

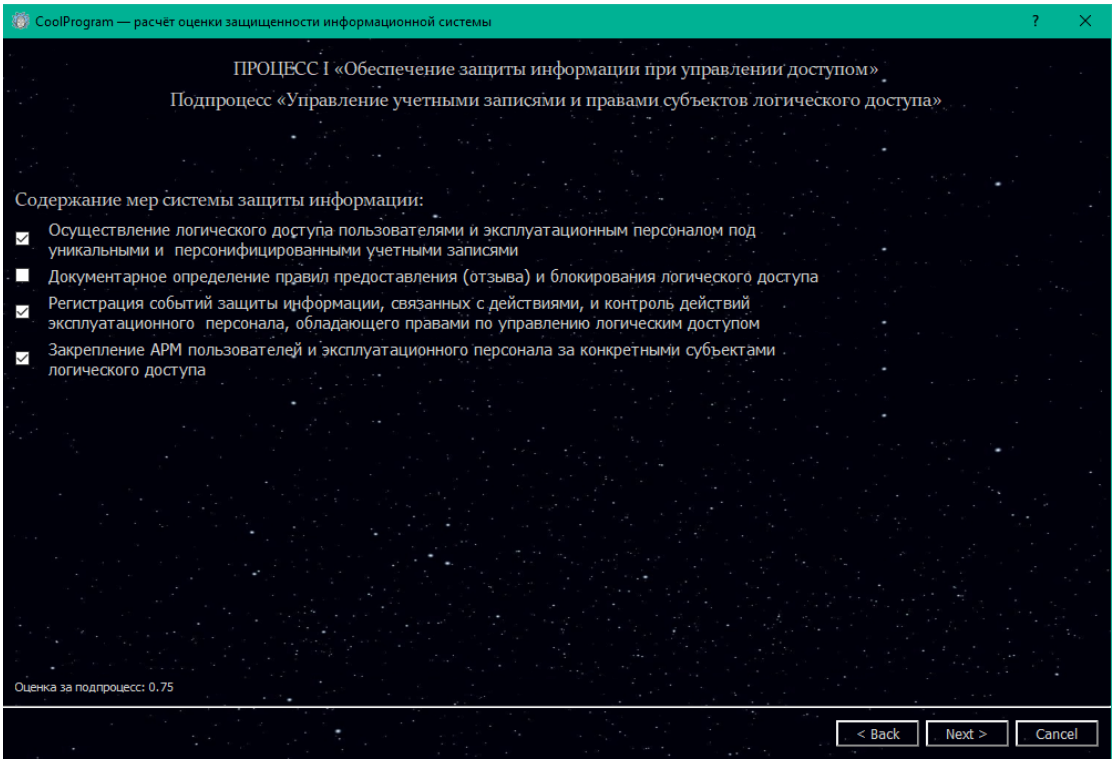
Оценку, характеризующую выбор финансовой организацией каждой из мер ЗИ, направленных на обеспечение ЗИ, определяют путем использования следующих числовых значений:

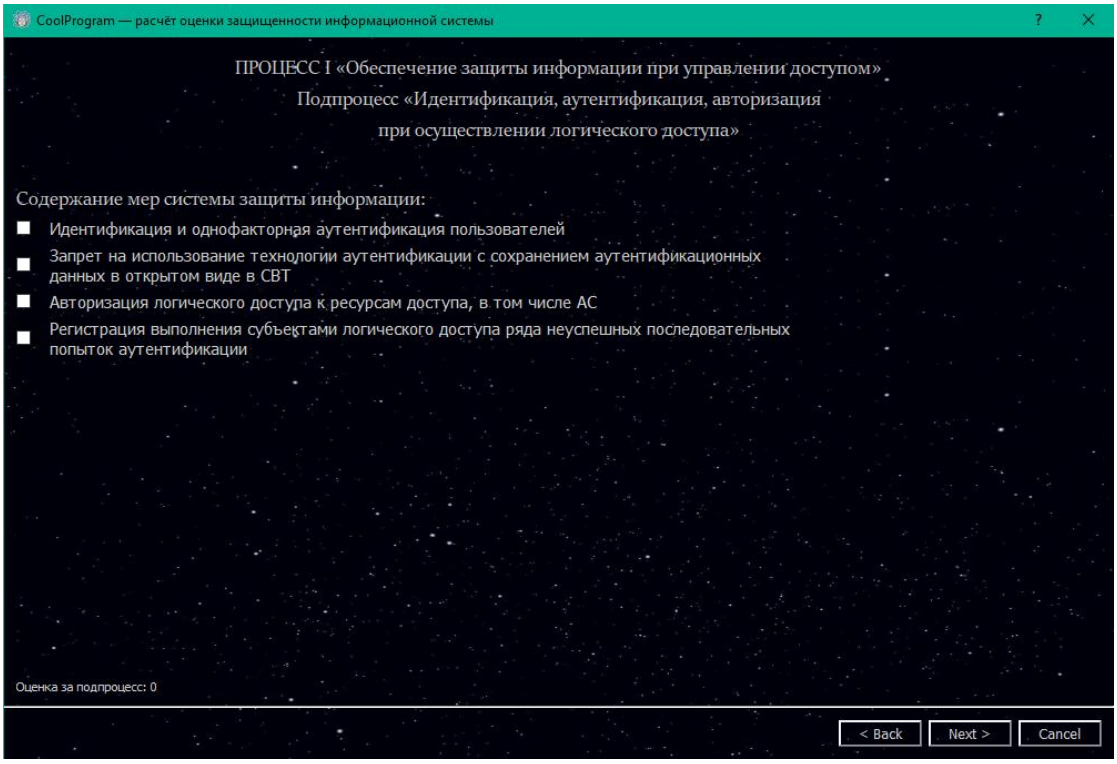
0 — не выбрана (при отсутствии у проверяемой организации свидетельств выбора);

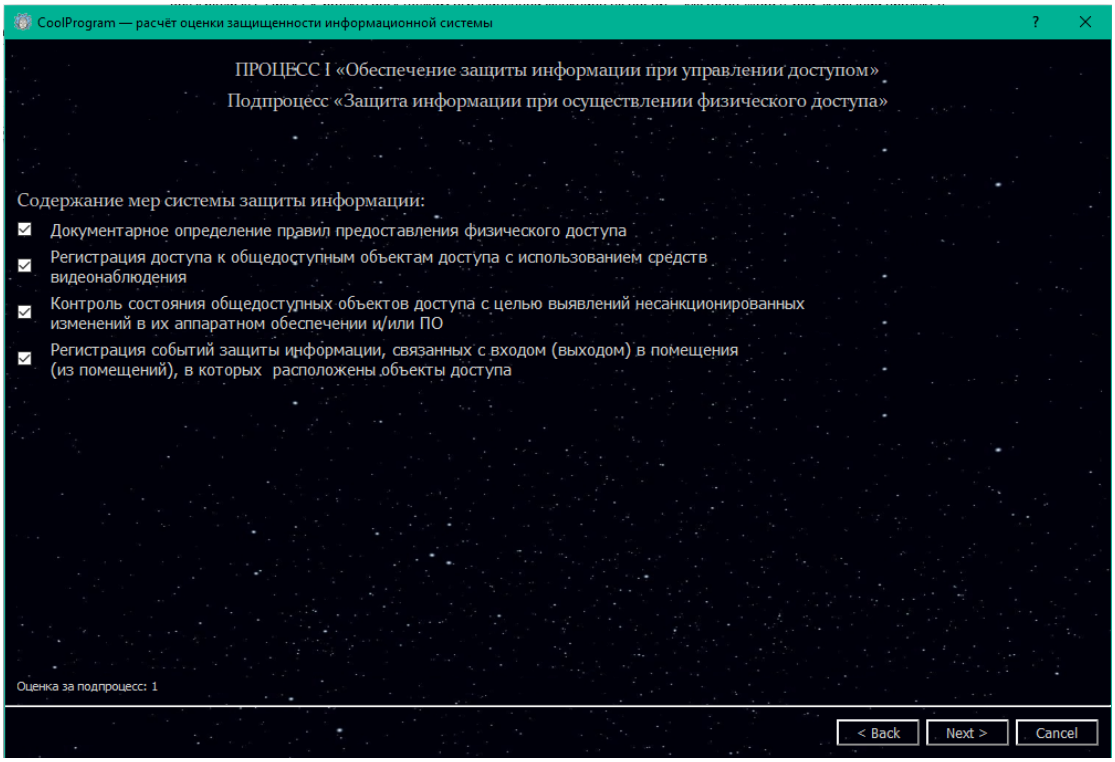
1 — выбрана (при предъявлении проверяемой организацией свидетельств выбора).

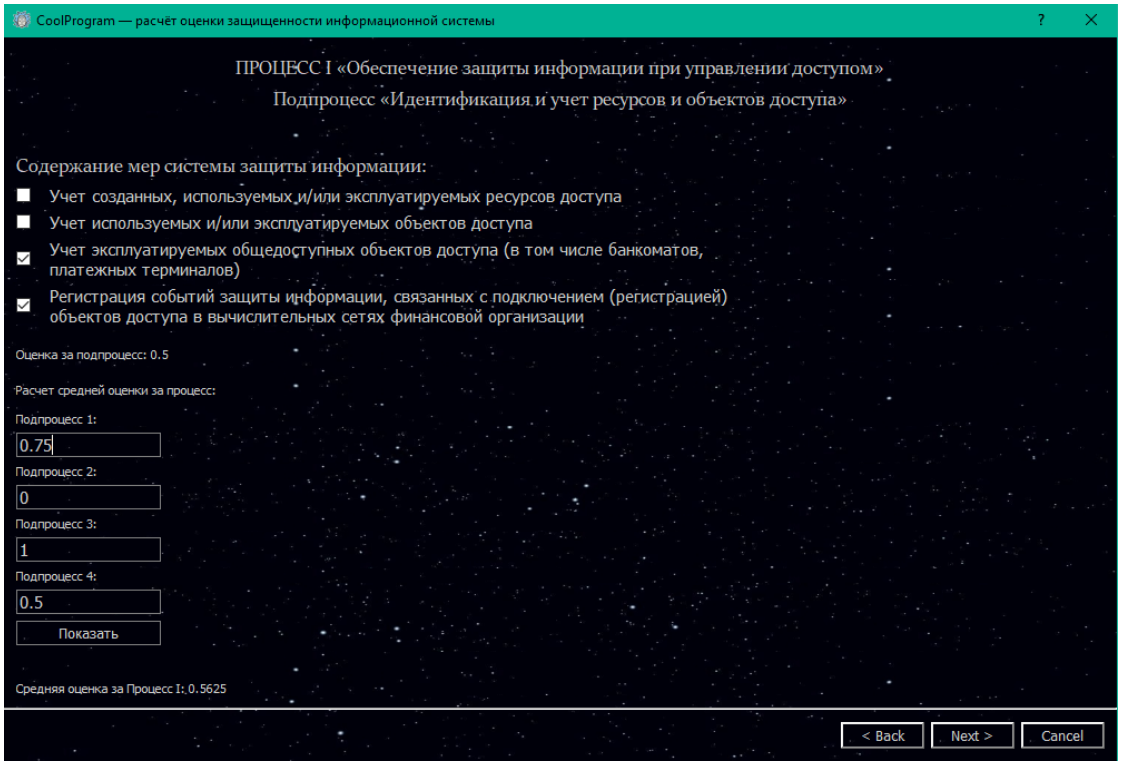
Значения оценок автоматически записываются в необходимые формулы для каждого из процессов, подпроцессов и направлений системы ЗИ. Это происходит при отметке соблюденных пунктов.

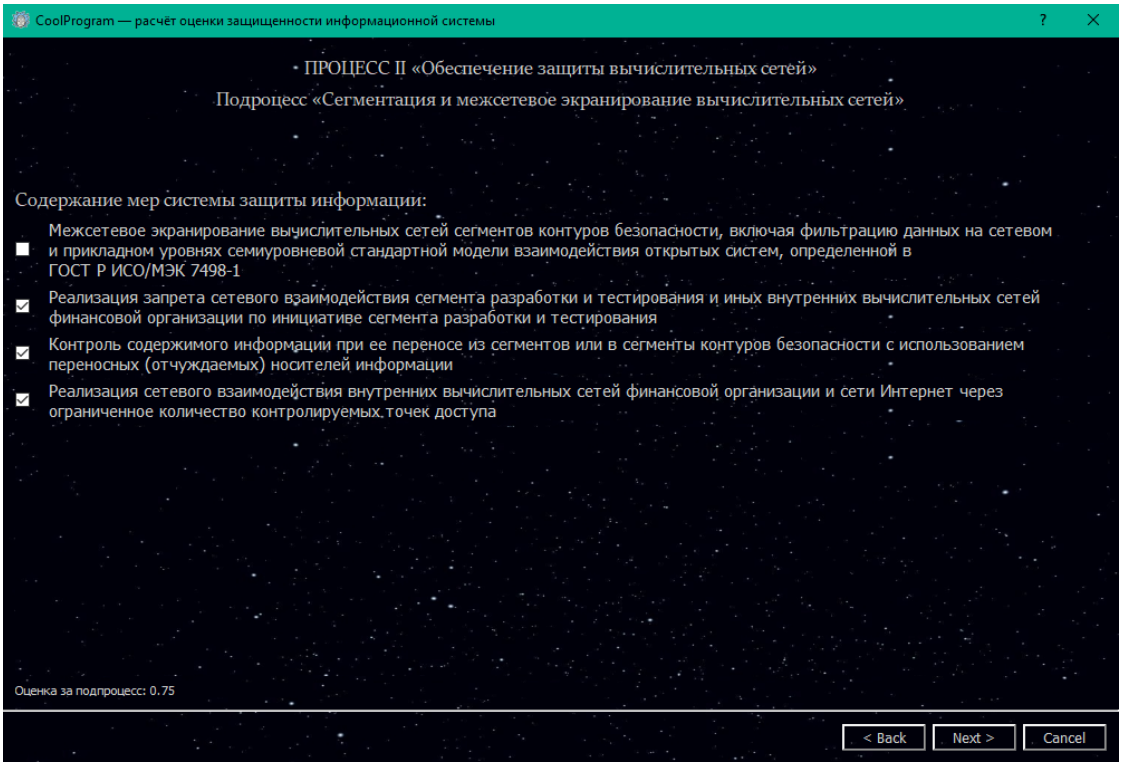
Пример работы программы

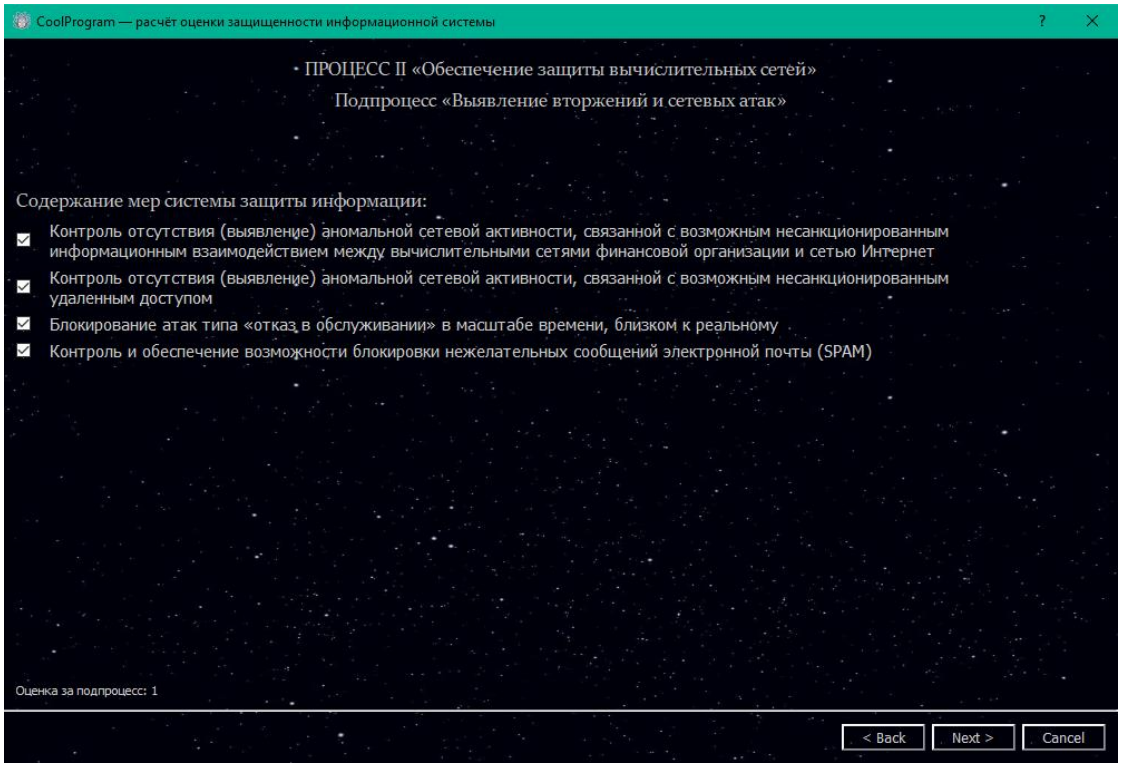


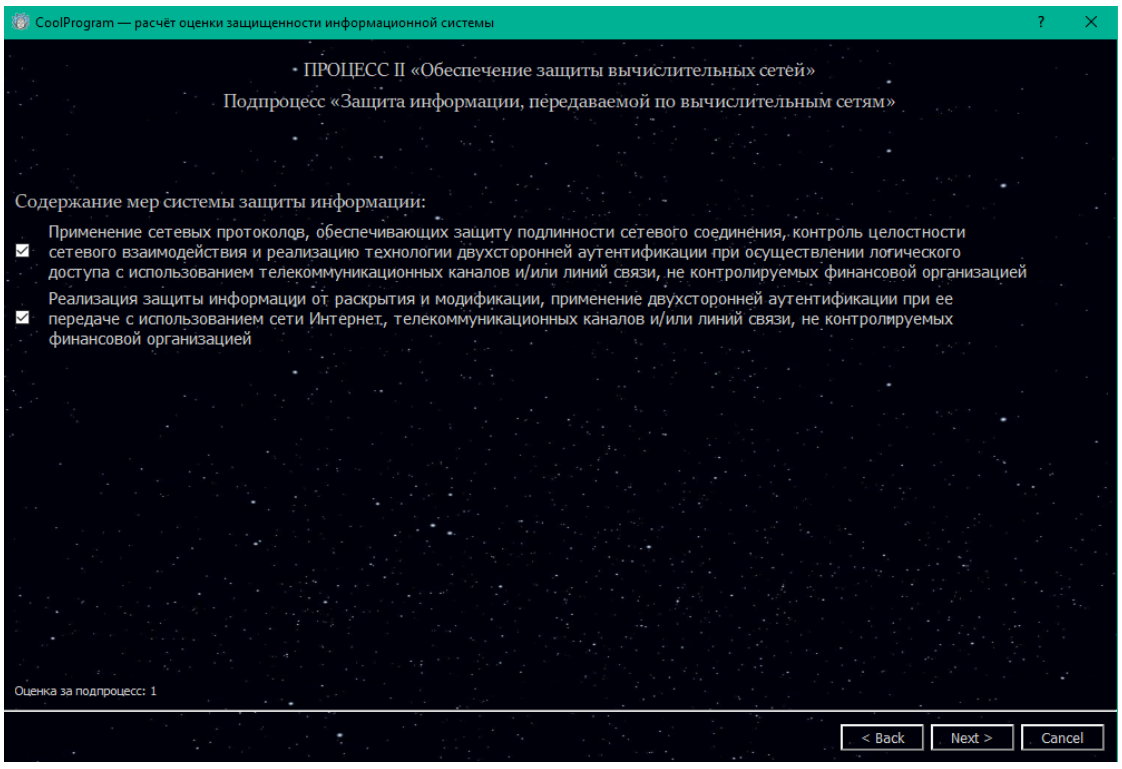

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС I «Обеспечение защиты информации при управлении доступом»
Подпроцесс «Идентификация, аутентификация, авторизация
при осуществлении логического доступа»
Содержание мер системы защиты информации:
Идентификация и однофакторная аутентификация пользователей
Запрет на использование технологии аутентификации с сохранением аутентификационных данных в открытом виде в СВТ
Авторизация логического доступа к ресурсам доступа, в том числе АС
Регистрация выполнения субъектами логического доступа ряда неуспешных последовательных попыток аутентификации
Оценка за подпроцесс: 0
< Back
Next >
Cancel

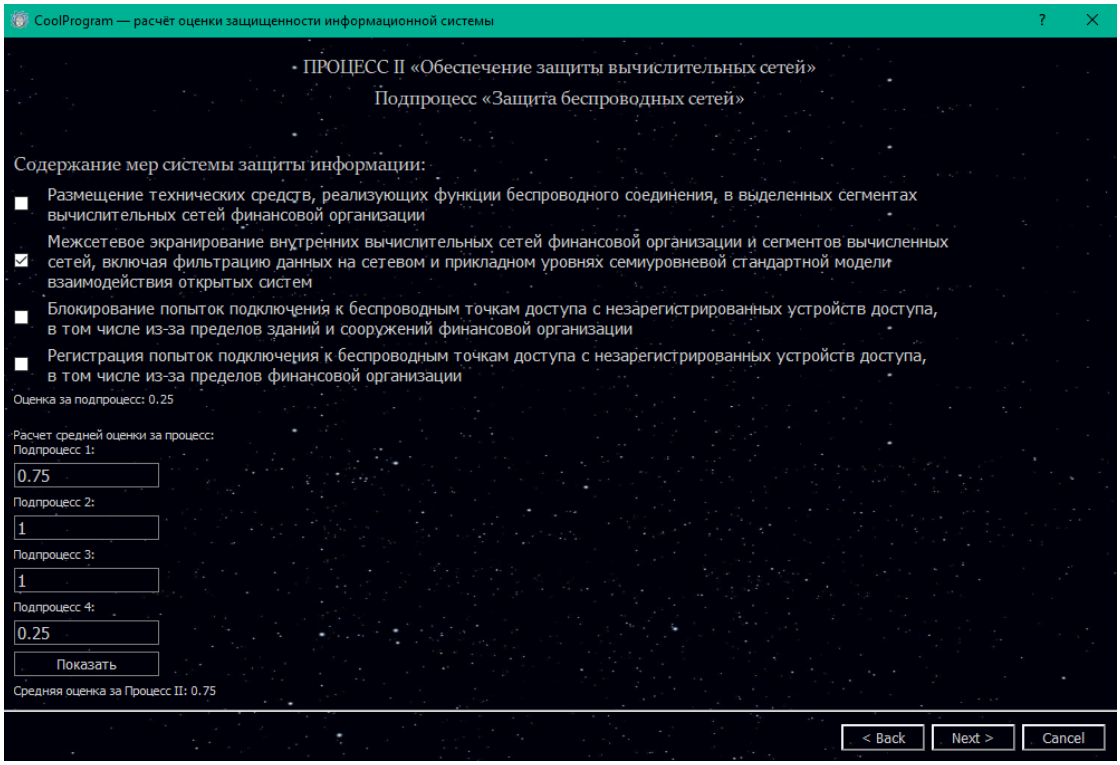

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС I «Обеспечение защиты информации при управлении доступом»
Подпроцесс «Защита информации при осуществлении физического доступа»
Содержание мер системы защиты информации:
Документарное определение правил предоставления физического доступа
Регистрация доступа к общедоступным объектам доступа с использованием средств видеонаблюдения
Контроль состояния общедоступных объектов доступа с целью выявлений несанкционированных изменений в их аппаратном обеспечении и/или ПО
Регистрация событий защиты информации, связанных с входом (выходом) в помещения (из помещений), в которых расположены объекты доступа
Оценка за подпроцесс: 1
< Back
Next >
Cancel

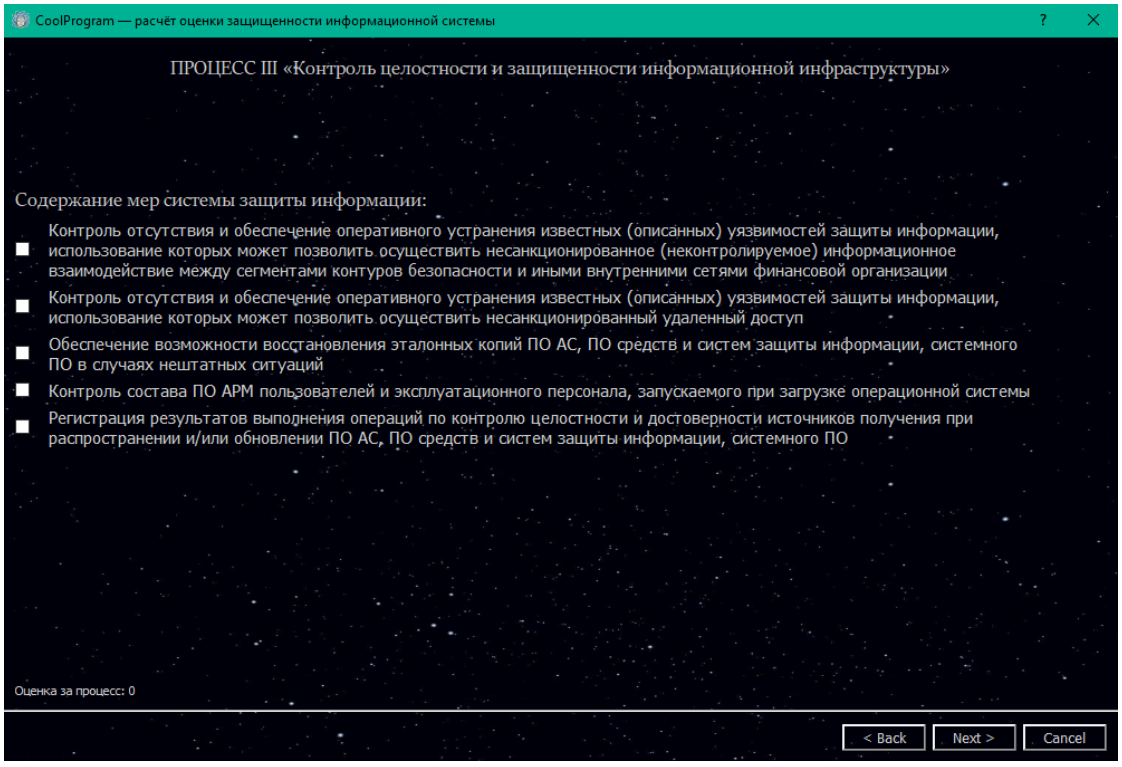

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС I «Обеспечение защиты информации при управлении доступом»
Подпроцесс «Идентификация и учет ресурсов и объектов доступа»
Содержание мер системы защиты информации:
Учет созданных, используемых и/или эксплуатируемых ресурсов доступа
Учет используемых и/или эксплуатируемых объектов доступа
Учет эксплуатируемых общедоступных объектов доступа (в том числе банкоматов, платежных терминалов)
Регистрация событий защиты информации, связанных с подключением (регистрацией) объектов доступа в вычислительных сетях финансовой организации
Оценка за подпроцесс: 0.5
Расчет средней оценки за процесс:
Подпроцесс 1:
0.75
Подпроцесс 2:
0
Подпроцесс 3:
1
Подпроцесс 4:
0.5
Показать
Средняя оценка за Процесс I: 0.5625
< Back
Next >
Cancel


CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС II «Обеспечение защиты вычислительных сетей»
Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей»
Содержание мер системы защиты информации:
Межсетевое экранирование вычислительных сетей сегментов контуров безопасности, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1
Реализация запрета сетевого взаимодействия сегмента разработки и тестирования и иных внутренних вычислительных сетей финансовой организации по инициативе сегмента разработки и тестирования
Контроль содержимого информации при ее переносе из сегментов или в сегменты контуров безопасности с использованием переносных (отчуждаемых) носителей информации
Реализация сетевого взаимодействия внутренних вычислительных сетей финансовой организации и сети Интернет через ограниченное количество контролируемых точек доступа
Оценка за подпроцесс: 0.75
< Back
Next >
Cancel

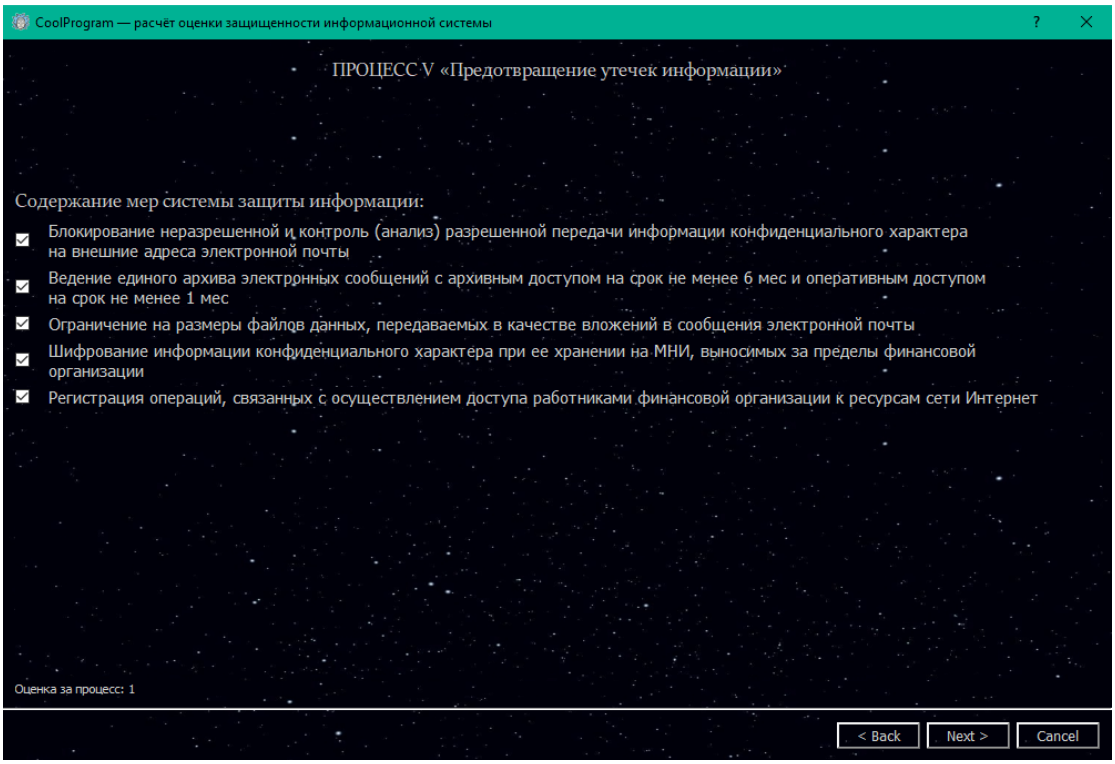

CoolProgram — расчёт оценки защищенности информационной системы
- ПРОЦЕСС II «Обеспечение защиты вычислительных сетей»
Подпроцесс «Выявление вторжений и сетевых атак»
Содержание мер системы защиты информации:
Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между вычислительными сетями финансовой организации и сетью Интернет
Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным удаленным доступом
Блокирование атак типа «отказ в обслуживании» в масштабе времени, близком к реальному
Контроль и обеспечение возможности блокировки нежелательных сообщений электронной почты (SPAM)
Оценка за подпроцесс: 1
< Back
Next >
Cancel

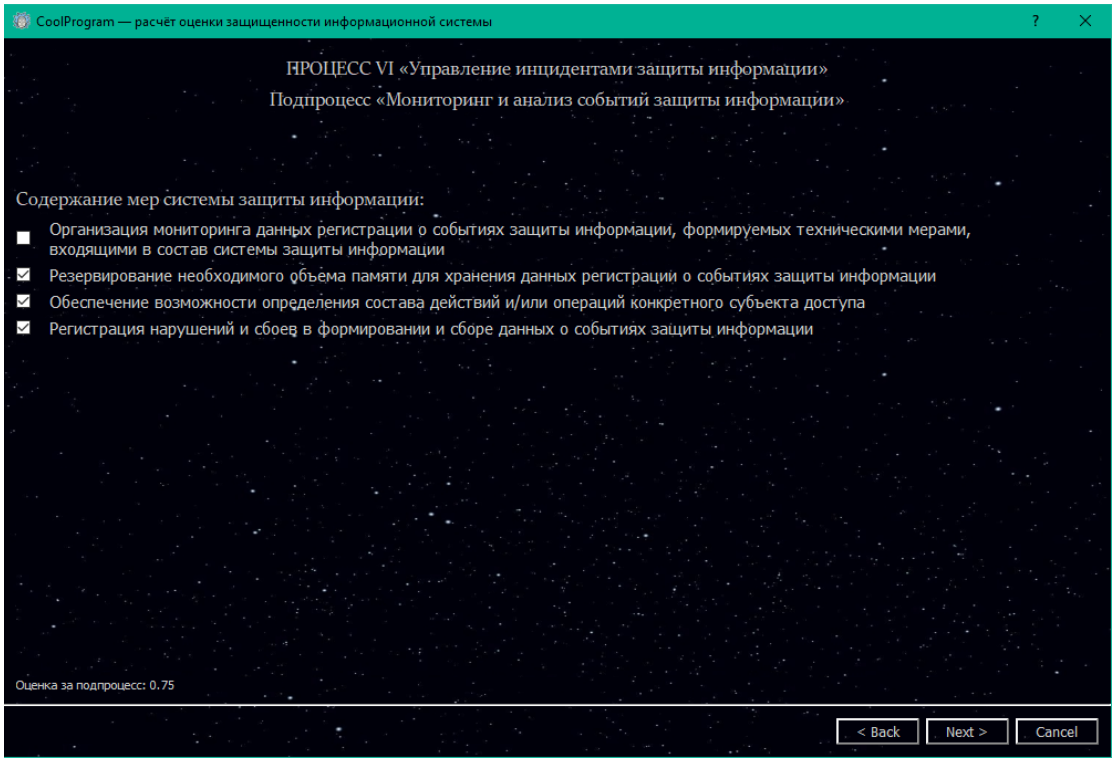

CoolProgram — расчёт оценки защищенности информационной системы
- ПРОЦЕСС II «Обеспечение защиты вычислительных сетей»
Подпроцесс «Защита информации, передаваемой по вычислительным сетям»
Содержание мер системы защиты информации:
Применение сетевых протоколов, обеспечивающих защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии двухсторонней аутентификации при осуществлении логического доступа с использованием телекоммуникационных каналов и/или линий связи, не контролируемых финансовой организацией
Реализация защиты информации от раскрытия и модификации, применение двухсторонней аутентификации при ее передаче с использованием сети Интернет, телекоммуникационных каналов и/или линий связи, не контролируемых финансовой организацией
Оценка за подпроцесс: 1
< Back
Next >
Cancel

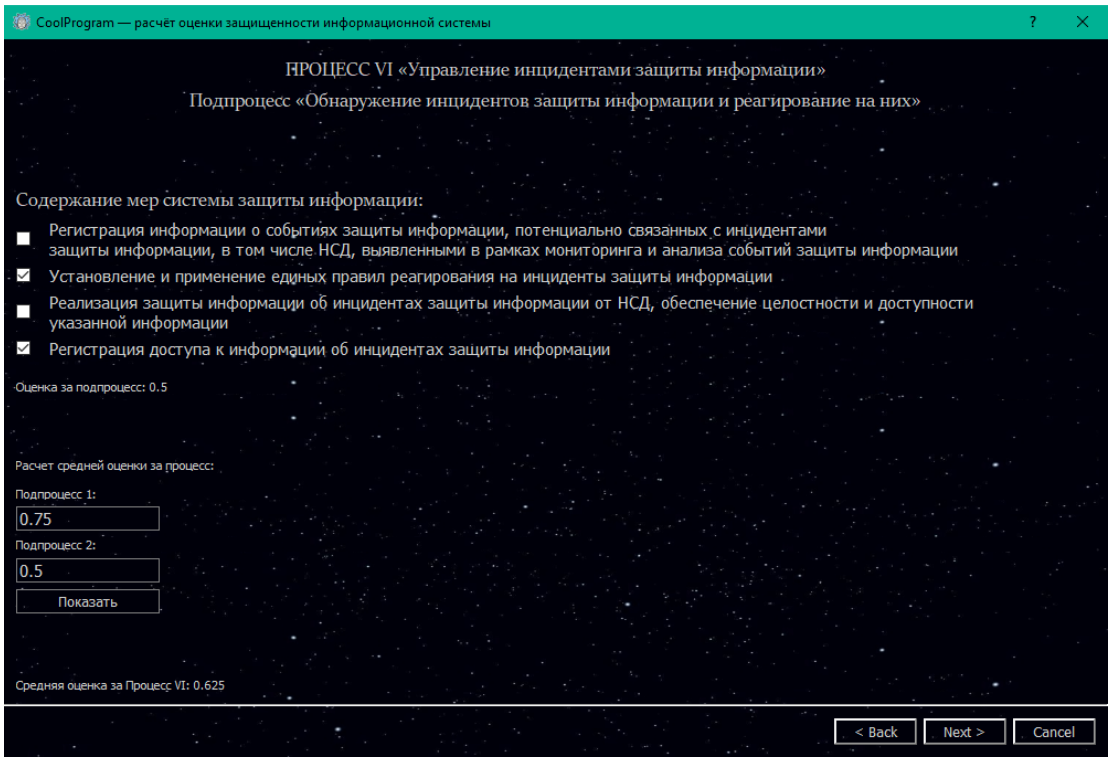

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС II «Обеспечение защиты вычислительных сетей»
Подпроцесс «Защита беспроводных сетей»
Содержание мер системы защиты информации:
Размещение технических средств, реализующих функции беспроводного соединения, в выделенных сегментах вычислительных сетей финансовой организации
Межсетевое экранирование внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем
Блокирование попыток подключения к беспроводным точкам доступа с незарегистрированных устройств доступа, в том числе из-за пределов зданий и сооружений финансовой организации
Регистрация попыток подключения к беспроводным точкам доступа с незарегистрированных устройств доступа, в том числе из-за пределов финансовой организации
Оценка за подпроцесс: 0.25
Расчет средней оценки за процесс:
Подпроцесс 1:
0.75
Подпроцесс 2:
1
Подпроцесс 3:
1
Подпроцесс 4:
0.25
Показать
Средняя оценка за Процесс II: 0.75
< Back
Next >
Cancel

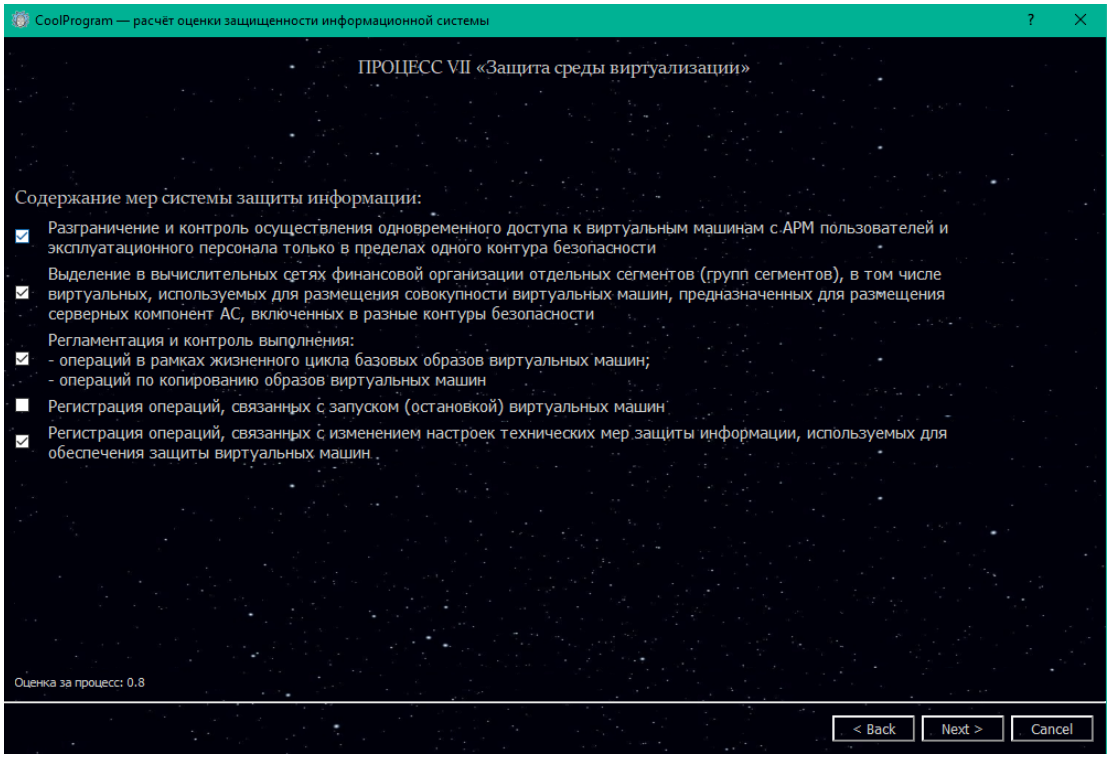

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС III «Контроль целостности и защищенности информационной инфраструктуры»
Содержание мер системы защиты информации:
Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами контуров безопасности и иными внутренними сетями финансовой организации
Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный удаленный доступ
Обеспечение возможности восстановления эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО в случаях нештатных ситуаций
Контроль состава ПО АРМ пользователей и эксплуатационного персонала, запускаемого при загрузке операционной системы
Регистрация результатов выполнения операций по контролю целостности и достоверности источников получения при распространении и/или обновлении ПО АС, ПО средств и систем защиты информации, системного ПО
Оценка за процесс: 0
< Back
Next >
Cancel

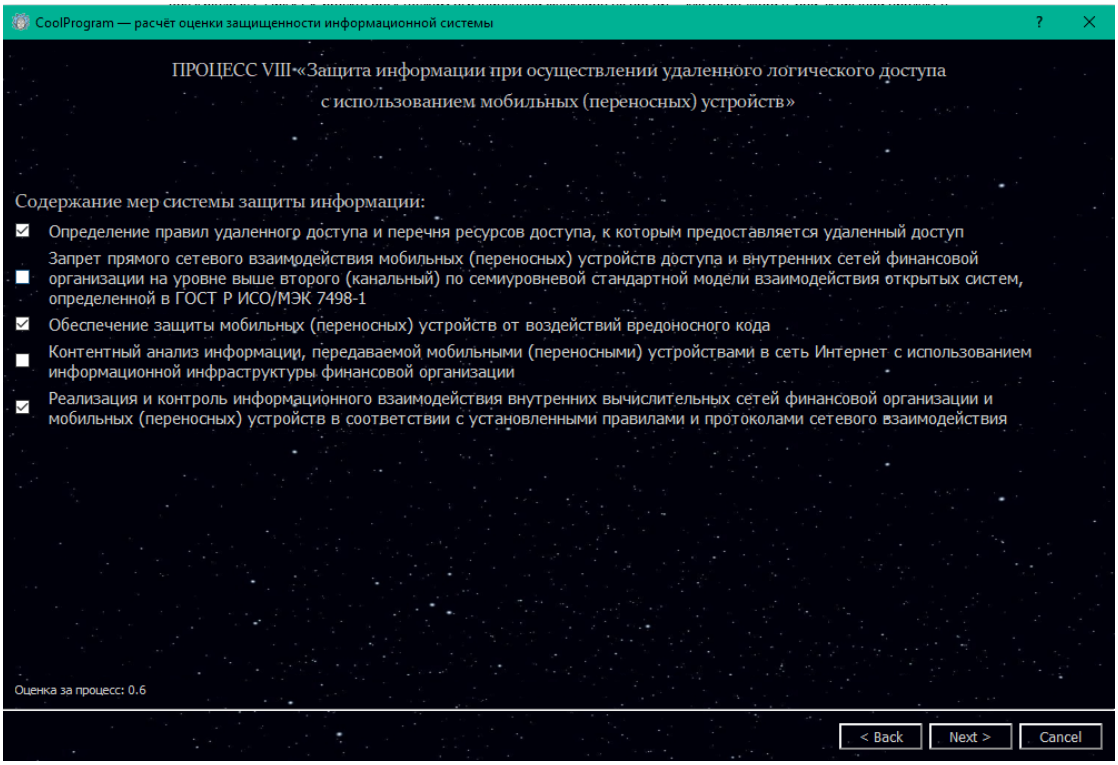

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС IV «Защита от вредоносного кода»
Содержание мер системы защиты информации:
Реализация защиты от вредоносного кода на уровне виртуальной информационной инфраструктуры
Реализация защиты от вредоносного кода на уровне контроля почтового трафика
Контроль отключения и своевременного обновления средств защиты от вредоносного кода
Регистрация операций по проведению проверок на отсутствие вредоносного кода
Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода
Оценка за процесс: 0.8
< Back
Next >
Cancel

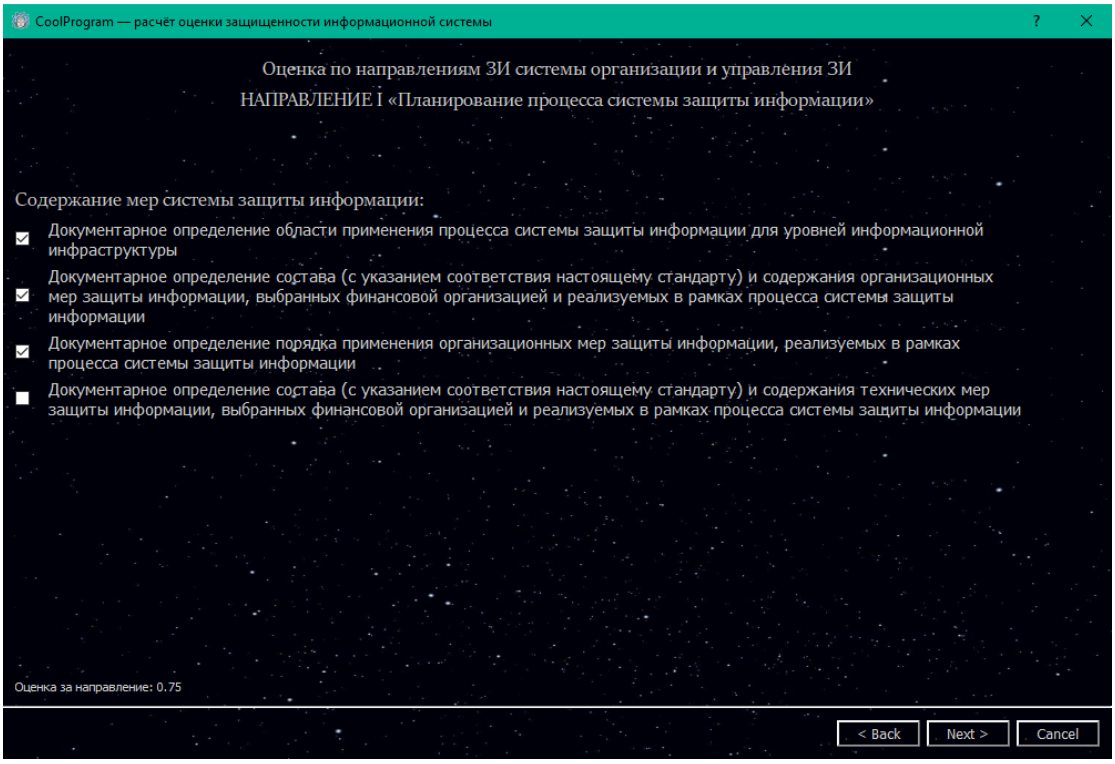

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС V «Предотвращение утечек информации»
Содержание мер системы защиты информации:
Блокирование неразрешенной и контроль (анализ) разрешенной передачи информации конфиденциального характера на внешние адреса электронной почты
Ведение единого архива электронных сообщений с архивным доступом на срок не менее 6 мес и оперативным доступом на срок не менее 1 мес
Ограничение на размеры файлов данных, передаваемых в качестве вложений в сообщения электронной почты
Шифрование информации конфиденциального характера при ее хранении на МНИ, выносимых за пределы финансовой организации
Регистрация операций, связанных с осуществлением доступа работниками финансовой организации к ресурсам сети Интернет
Оценка за процесс: 1
< Back
Next >
Cancel

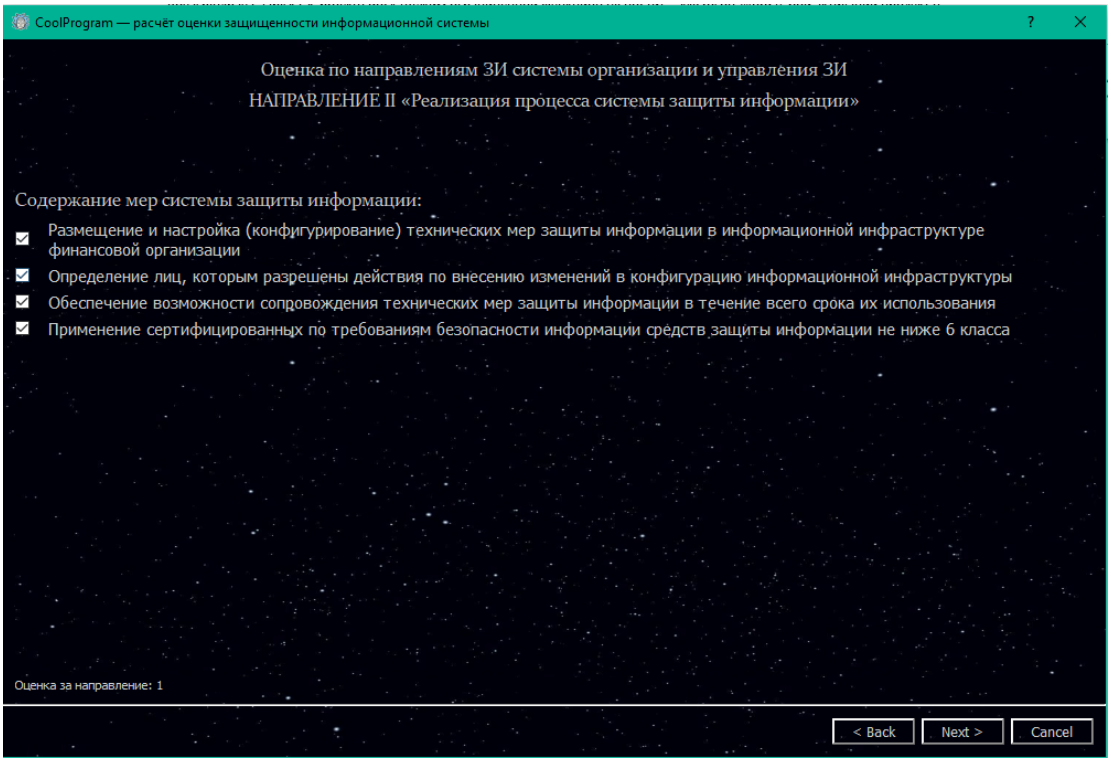

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС VI «Управление инцидентами защиты информации»
Подпроцесс «Мониторинг и анализ событий защиты информации»
Содержание мер системы защиты информации:
Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации
Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации
Обеспечение возможности определения состава действий и/или операций конкретного субъекта доступа
Регистрация нарушений и сбоев в формировании и сборе данных о событиях защиты информации
Оценка за подпроцесс: 0.75
< Back
Next >
Cancel

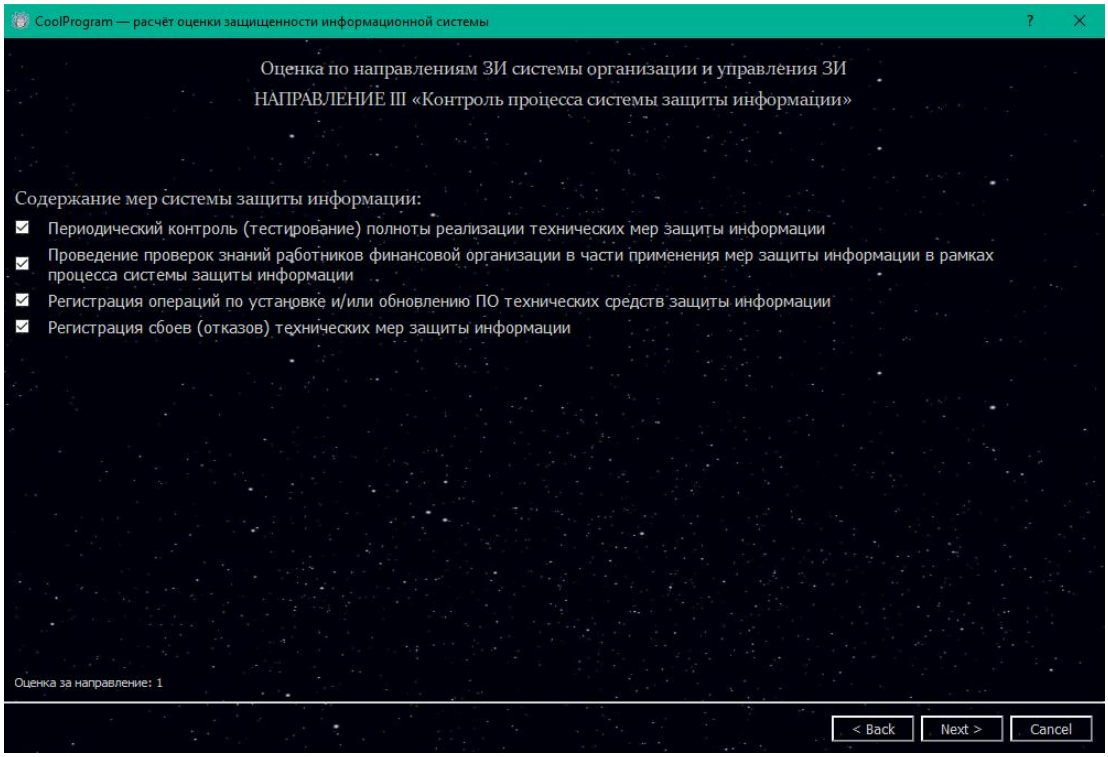

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС VI «Управление инцидентами защиты информации»
Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них»
Содержание мер системы защиты информации:
Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации
Установление и применение единых правил реагирования на инциденты защиты информации
Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации
Регистрация доступа к информации об инцидентах защиты информации
Оценка за подпроцесс: 0.5
Расчет средней оценки за процесс:
Подпроцесс 1:
0.75
Подпроцесс 2:
0.5
Показать
Средняя оценка за Процесс VI: 0.625
< Back
Next >
Cancel

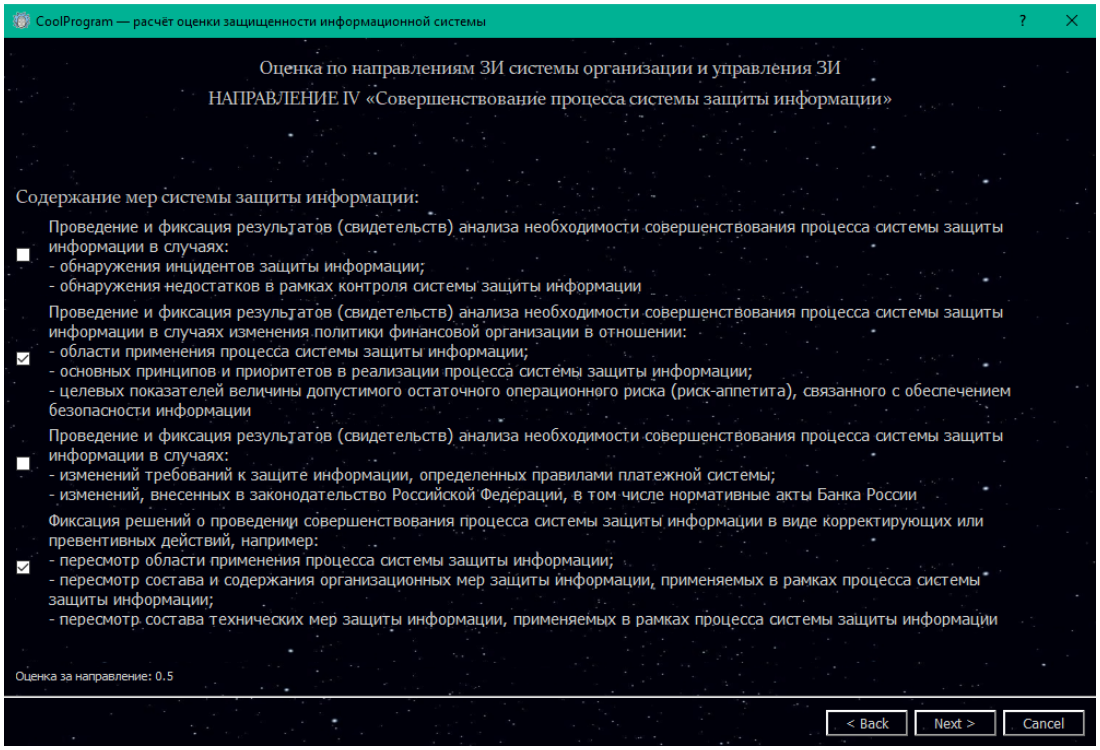

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС VII «Защита среды виртуализации»
Содержание мер системы защиты информации:
Разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала только в пределах одного контура безопасности
Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения серверных компонент АС, включенных в разные контуры безопасности
Регламентация и контроль выполнения:
- операций в рамках жизненного цикла базовых образов виртуальных машин;
- операций по копированию образов виртуальных машин
Регистрация операций, связанных с запуском (остановкой) виртуальных машин
Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин
Оценка за процесс: 0.8
< Back
Next >
Cancel

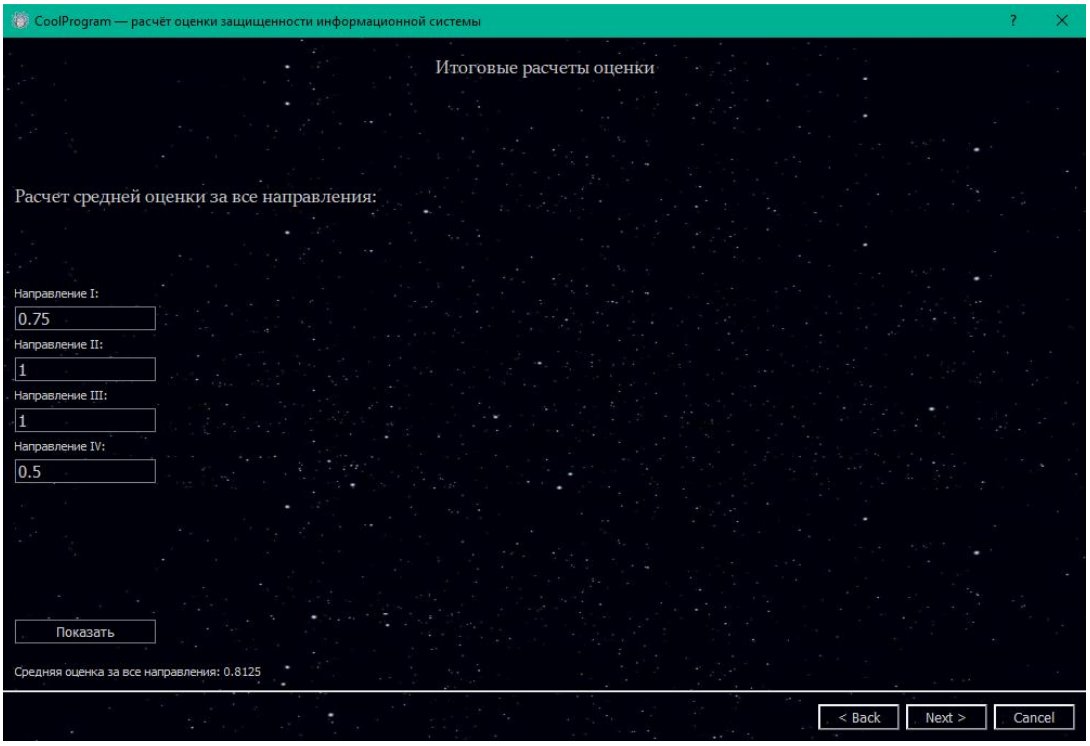

CoolProgram — расчёт оценки защищенности информационной системы
ПРОЦЕСС VIII-«Защита информации при осуществлении удаленного логического доступа
с использованием мобильных (переносных) устройств»
Содержание мер системы защиты информации:
Определение правил удаленного доступа и перечня ресурсов доступа, к которым предоставляется удаленный доступ
Запрет прямого сетевого взаимодействия мобильных (переносных) устройств доступа и внутренних сетей финансовой организации на уровне выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1
Обеспечение защиты мобильных (переносных) устройств от воздействий вредоносного кода
Контентный анализ информации, передаваемой мобильными (переносными) устройствами в сеть Интернет с использованием информационной инфраструктуры финансовой организации
Реализация и контроль информационного взаимодействия внутренних вычислительных сетей финансовой организации и мобильных (переносных) устройств в соответствии с установленными правилами и протоколами сетевого взаимодействия
Оценка за процесс: 0.6
< Back
Next >
Cancel

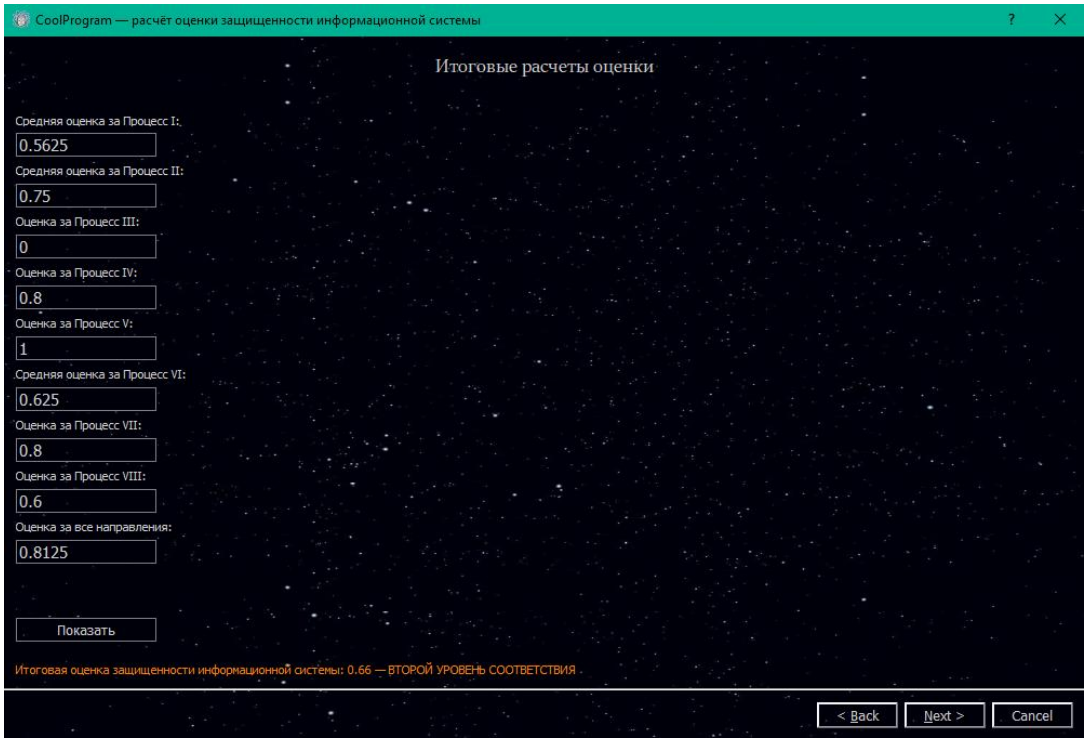

CoolProgram — расчёт оценки защищенности информационной системы
Оценка по направлениям ЗИ системы организации и управления ЗИ
НАПРАВЛЕНИЕ I «Планирование процесса системы защиты информации»
Содержание мер системы защиты информации:
Документарное определение области применения процесса системы защиты информации для уровней информационной инфраструктуры
Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания организационных мер защиты информации, выбранных финансовой организацией и реализуемых в рамках процесса системы защиты информации
Документарное определение порядка применения организационных мер защиты информации, реализуемых в рамках процесса системы защиты информации
Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания технических мер защиты информации, выбранных финансовой организацией и реализуемых в рамках процесса системы защиты информации
Оценка за направление: 0.75
< Back
Next >
Cancel


CoolProgram — расчёт оценки защищенности информационной системы
Оценка по направлениям ЗИ системы организации и управления ЗИ
НАПРАВЛЕНИЕ II «Реализация процесса системы защиты информации»
Содержание мер системы защиты информации:
Размещение и настройка (конфигурирование) технических мер защиты информации в информационной инфраструктуре финансовой организации
Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры
Обеспечение возможности сопровождения технических мер защиты информации в течение всего срока их использования
Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса
Оценка за направление: 1
< Back
Next >
Cancel


CoolProgram — расчёт оценки защищенности информационной системы
Оценка по направлениям ЗИ системы организации и управления ЗИ
НАПРАВЛЕНИЕ III «Контроль процесса системы защиты информации»
Содержание мер системы защиты информации:
Периодический контроль (тестирование) полноты реализации технических мер защиты информации
Проведение проверок знаний работников финансовой организации в части применения мер защиты информации в рамках процесса системы защиты информации
Регистрация операций по установке и/или обновлению ПО технических средств защиты информации
Регистрация сбоев (отказов) технических мер защиты информации
Оценка за направление: 1
< Back
Next >
Cancel


CoolProgram — расчёт оценки защищенности информационной системы
Оценка по направлениям ЗИ системы организации и управления ЗИ
НАПРАВЛЕНИЕ IV «Совершенствование процесса системы защиты информации»
Содержание мер системы защиты информации:
Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:
- обнаружения инцидентов защиты информации;
- обнаружения недостатков в рамках контроля системы защиты информации
Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях изменения политики финансовой организации в отношении:
- области применения процесса системы защиты информации;
- основных принципов и приоритетов в реализации процесса системы защиты информации;
- целевых показателей величины допустимого остаточного операционного риска (риск-аппетита), связанного с обеспечением безопасности информации
Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:
- изменений требований к защите информации, определенных правилами платежной системы;
- изменений, внесенных в законодательство Российской Федерации, в том числе нормативные акты Банка России
Фиксация решений о проведении совершенствования процесса системы защиты информации в виде корректирующих или превентивных действий, например:
- пересмотр области применения процесса системы защиты информации;
- пересмотр состава и содержания организационных мер защиты информации, применяемых в рамках процесса системы защиты информации;
- пересмотр состава технических мер защиты информации, применяемых в рамках процесса системы защиты информации
Оценка за направление: 0.5
< Back
Next >
Cancel





В данной ситуации программа вывела результат – *второй уровень соответствия* при итоговой оценке защищенности ИС *0.66*.

Фрагменты кода программы

```
        return Wizard.classLastPage2

# итоговые расчеты
class ClassesLastPage2(QtWidgets.QWizardPage):
    def __init__(self, *args, **kwargs):
        super(ClassesLastPage2, self).__init__(*args, **kwargs)

        font = QtGui.QFont()
        font.setFamily("Sitka")
        font.setPointSize(14)
        self.setFont(font)

        self.label_74 = QtWidgets.QLabel('Итоговые расчеты оценки', self)
        self.label_74.setAlignment(Qt.AlignCenter)

        self.label_80 = QtWidgets.QLabel('\n\nСредняя оценка за Процесс I: ')
        self.text_1 = QtWidgets.QLineEdit(self)
        self.text_1.setFixedWidth(130)
        self.text_1.setMaxLength(6)
        self.text_1.setStyleSheet("font: Sitka; font-size: 15")
        self.label_81 = QtWidgets.QLabel('Средняя оценка за Процесс II: ')
        self.text_2 = QtWidgets.QLineEdit(self)
        self.text_2.setFixedWidth(130)
        self.text_2.setMaxLength(6)
        self.text_2.setStyleSheet("font: Sitka; font-size: 15")
        self.label_82 = QtWidgets.QLabel('Оценка за Процесс III: ')
```

```
        self.button.clicked.connect(self.on_click)

    def on_click(self):
        value_1 = self.text_1.text()
        value_2 = self.text_2.text()
        value_3 = self.text_3.text()
        value_4 = self.text_4.text()
        value_5 = self.text_5.text()
        value_6 = self.text_6.text()
        value_7 = self.text_7.text()
        value_8 = self.text_8.text()
        value_9 = self.text_9.text()

        if float(value_1) > 1 or float(value_1) < 0:
            self.label_res.setText('\nОшибка ввода!')
        elif float(value_2) > 1 or float(value_2) < 0:
            self.label_res.setText('\nОшибка ввода!')
        elif float(value_3) > 1 or float(value_3) < 0:
            self.label_res.setText('\nОшибка ввода!')
        elif float(value_4) > 1 or float(value_4) < 0:
            self.label_res.setText('\nОшибка ввода!')
        elif float(value_5) > 1 or float(value_5) < 0:
            self.label_res.setText('\nОшибка ввода!')
        elif float(value_6) > 1 or float(value_6) < 0:
            self.label_res.setText('\nОшибка ввода!')
```

Вывод

В ходе реализации проекта мы изучили необходимые документы, примеры и стандарты ГОСТ и разработали программу *«CoolProgram – расчет оценки защищенности информационной системы»* предназначенную для оценки защищенности ИС.

CoolProgram.exe