

## **Требования к оформлению проектов по предмету «Информатика» профиль «Информационная безопасность»**

Проект представляет собой самостоятельную исследовательскую и опытно-конструкторскую работу участника.

На региональный этап допускается предоставление проекта со степенью готовности порядка 75% при условии прозрачного и аргументированного описания всех недоработанных частей в пояснительной записке.

Участник должен выбрать одно из двух направлений для своего проекта: Red Team или Blue Team. Выбор направления определяет цели, методы и конечный продукт проекта.

### **Направление «Red Team»**

Red Team – это подход к оценке безопасности, при котором участник моделирует тактики, техники и процедуры (TTP) реального злоумышленника с целью проверки устойчивости систем, процессов и персонала к целенаправленной атаке. В контексте проекта данное направление нацелено на проактивный поиск, исследование, доказательство и демонстрацию уязвимостей и слабых мест в информационных системах, программном обеспечении или организационных процессах.

#### **Примеры:**

- инструмент для автоматизации сканирования уязвимостей или эксплуатации известных слабостей;
- исследование и описание нового вектора атаки на определенную информационную систему или технологию;
- методика проведения пентеста для конкретного класса систем (веб-приложений, сетевой инфраструктуры и т.д.).

### **Направление «Blue Team»**

Blue Team – это подход, нацеленный на создание, внедрение и поддержание эффективных контрмер для защиты информационных активов от киберугроз. В рамках проекта участник выступает в роли защитника, чья задача – разработать решение, которое повышает общий уровень безопасности системы, упрощает работу аналитиков или автоматизирует рутинные операции по обеспечению информационной безопасности.

#### **Примеры:**

- прототип системы обнаружения вторжений (IDS) или предотвращения вторжений (IPS);
- инструмент для мониторинга и анализа логов безопасности;
- средство для контроля настроек безопасности операционных систем или

приложений.

В рамках выбранного направления участнику предлагается самостоятельно на основе открытых источников выявить и конкретизировать произвольную, но существующую и подтверждённую определённым кругом источников проблему информационной безопасности. Это может быть, например:

- слабость популярных средств обеспечения информационной безопасности;
- типичная проблема использования информационных систем, ведущая к нарушению конфиденциальности, целостности или доступности данных;
- отсутствие инструмента защиты от известной угрозы;
- новый класс уязвимостей или атак.

### Критерии оценивания проектного тура

#### Направление «Red Team»

Критерии оценки проекта		Баллы
<b>Пояснительная записка 10 баллов</b>	<b>1</b>	<b>Содержание и оформление документации проекта</b>
	<b>1.1</b>	<b>Общее оформление: (ориентация на ГОСТ 7.32-2001 Международный стандарт оформления проектной документации)</b>
	1.1.1	Соответствие ГОСТ 7.32-2017 (полное – 1, частичное – 0.5, нет – 0)
	1.1.2	Полнота и структурированность описания этапов выполнения проекта (полное – 2, частичное – 1, нет – 0)
	1.1.3	Глубина анализа предметной области и аналогов (глубокий – 1, поверхностный – 0.5, нет – 0)
	1.1.4	Качество и оформление списка литературы и источников (соответствует стандарту – 1, не соответствует стандарту – 0)
	<b>1.2</b>	<b>Качество теоретического и практического исследования</b>
	1.2.1	Актуальность и обоснование выбранной уязвимости/вектора атаки (да – 1, нет – 0)
	1.2.2	Четкость формулировки цели, задач и гипотезы (полное – 1, частичное – 0.5, нет – 0)
	1.2.3	Новизна предложенного метода атаки или инструмента (высокая – 1, средняя – 0.5, нет – 0)
	1.2.4	Описание методологии разработки и тестирования средства (детальное – 1, поверхностное – 0.5, нет – 0)
	1.2.5	Глубина анализа результатов тестирования и эффективности защиты (глубокий – 1, поверхностный – 0.5, нет – 0)
	<b>2</b>	<b>Оценка продукта</b>
	<b>2.1</b>	<b>Функциональность и технологичность</b>

Критерии оценки проекта			Баллы
<b>Оценка разработанного продукта 10 баллов</b>	2.1.1	Глубина проработки атаки: Продукт демонстрирует эксплуатацию уязвимости на уровне кода/логики/протокола, а не поверхностное сканирование (глубокая – 2, средняя – 1, низкая – 0.5)	2
	2.1.2	Масштаб охвата угроз: Разработка направлена на выявление и демонстрацию не единичной уязвимости, а класса уязвимостей или тактики атаки (класс уязвимостей – 2, тактика – 1, единичная уязвимость – 0.5)	2
	2.1.3	Степень автоматизации и воспроизводимости: Инструмент автоматизирует процесс атаки от разведки до получения результата, обеспечивая стабильное воспроизведение (полная – 2, частичная – 1, отсутствует – 0)	2
	<b>2.2</b>	<b>Качество исполнения и новизна</b>	<b>4</b>
	2.2.1	Архитектура и дизайн (читаемость, модульность) (высокие – 1, средние – 0.5, низкие – 0)	1
	2.2.2	<b>Новизна вектора атаки или подхода:</b> Предложен ранее не описанный метод эксплуатации или существенно доработан существующий (новый – 1, доработка – 0.5, стандартный – 0)	1
	2.2.3	<b>Практическая ценность для защиты:</b> Результаты работы продукта позволяют сформулировать конкретные рекомендации по усилению защиты для целого класса систем (высокая – 1, средняя – 0.5, низкая – 0)	2
	<b>3</b>	<b>Процедура презентации проекта</b>	<b>10</b>
	<b>3.1</b>	<b>Качество презентации и процедуры защиты</b>	<b>6</b>
	3.1.1	Структура и логика изложения (четкая – 2, частичная – 1, отсутствует – 0)	2
<b>Оценка защиты проекта 10 баллов</b>	3.1.2	Качество подачи материала (ясность, убедительность, использование визуализации) (высокое – 2, среднее – 1, низкое – 0.5)	2
	3.1.3	Соблюдение регламента выступления (да – 1, нет – 0)	1
	3.1.4	Наглядность и успешность демонстрации продукта (полная – 1, частичная – 0.5, нет – 0)	1
	<b>3.2</b>	<b>Глубина понимания и ответы на вопросы</b>	<b>4</b>
	3.2.1	Понимание принципов защиты, моделей угроз (например, MITRE ATT&CK) (глубокое – 2, поверхностное – 1, нет – 0)	2
	3.2.2	Качество аргументации выводов, ограничений и путей развития системы (высокое – 1, среднее – 0.5, низкое – 0)	1
	3.2.3	Уверенность и аргументированность ответов на вопросы (высокие – 1, средние – 0.5, низкие – 0)	1
		<b>Итого</b>	<b>30</b>

## Направление «Blue Team»

Критерии оценки проекта		Баллы
<b>Пояснительная записка 10 баллов</b>	<b>1</b>	<b>Содержание и оформление документации проекта</b>
	1.1	Общее оформление: (ориентация на ГОСТ 7.32-2001 Международный стандарт оформления проектной документации)
	1.1.1	Соответствие ГОСТ 7.32-2017 (полное – 1, частичное – 0.5, нет – 0)
	1.1.2	Полнота и структурированность описания этапов выполнения проекта (полное – 2, частичное – 1, нет – 0)
	1.1.3	Глубина анализа предметной области и аналогов (глубокий – 1, поверхностный – 0.5, нет – 0)
	1.1.4	Качество и оформление списка литературы и источников (соответствует стандарту – 1, не соответствует стандарту – 0)
	<b>1.2</b>	<b>Качество теоретического и практического исследования</b>
	1.2.1	Актуальность и обоснование выбранной угрозы и средства защиты
	1.2.2	Четкость формулировки цели, задач и модели угроз (полные – 1, частичные – 0.5, нет – 0)
	1.2.3	Новизна предложенного метода защиты или анализа (высокая – 1, средняя – 0.5, нет – 0)
	1.2.4	Описание методологии тестирования (детальное – 1, поверхностное – 0.5, нет – 0)
	1.2.5	Глубина анализа полученных результатов и выводов (глубокий – 1, поверхностный – 0.5, нет – 0)
	<b>2</b>	<b>Оценка продукта</b>
	<b>2.1</b>	<b>Функциональность и технологичность</b>
	2.1.1	Уровень повышения защищенности: Внедрение продукта значительно повышает устойчивость системы к целевому классу угроз (значительное – 2, среднее – 1, незначительное – 0.5)
	2.1.2	Широта охвата контрмер: продукт обеспечивает защиту от единичной уязвимости – 0.5, от тактики злоумышленника (по MITRE ATT&CK) – 1, от нескольких тактик или всей цепочки кибератаки – 2
	2.1.3	Эффективность продукта (высокая – 2, средняя – 1, нет – 0)
	<b>2.2</b>	<b>Качество исполнения и новизна</b>
	2.2.1	Проактивность и адаптивность: Решение способно не только детектировать известные угрозы, но и адаптироваться к новым или применять проактивные методы защиты (да – 1, частично – 0.5, нет – 0)

Критерии оценки проекта			Баллы
	2.2.2	Масштабируемость и модульность архитектуры: Архитектура продукта позволяет расширять его функциональность и применять в различных конфигурациях (продумана – 1, базово – 0.5, отсутствует – 0)	2
<b>Оценка защиты проекта 10 баллов</b>	<b>3</b>	<b>Процедура презентации проекта</b>	<b>10</b>
	<b>3.1</b>	<b>Качество презентации и процедуры защиты</b>	<b>6</b>
	3.1.1	Структура и логика изложения (четкая – 2, частичная – 1, отсутствует – 0)	2
	3.1.2	Качество подачи материала (ясность, убедительность, использование визуализации) (высокое – 2, среднее – 1, низкое – 0.5)	2
	3.1.3	Соблюдение регламента выступления (да – 1, нет – 0)	1
	3.1.4	Наглядность и успешность демонстрации продукта (полная – 1, частичная – 0.5, нет – 0)	1
	<b>3.2</b>	<b>Глубина понимания и ответы на вопросы</b>	<b>4</b>
	3.2.1	Понимание тактик, техник и процедур (ТТР) в контексте проекта (глубокое – 2, поверхностное – 1, нет – 0)	2
	3.2.2	Качество аргументации выводов и предложенных контрмер (высокое – 1, среднее – 0.5, низкое – 0)	1
	3.2.3	Уверенность и аргументированность ответов на вопросы (высокие – 1, средние – 0.5, низкие – 0)	1
<b>Итого</b>			<b>30</b>