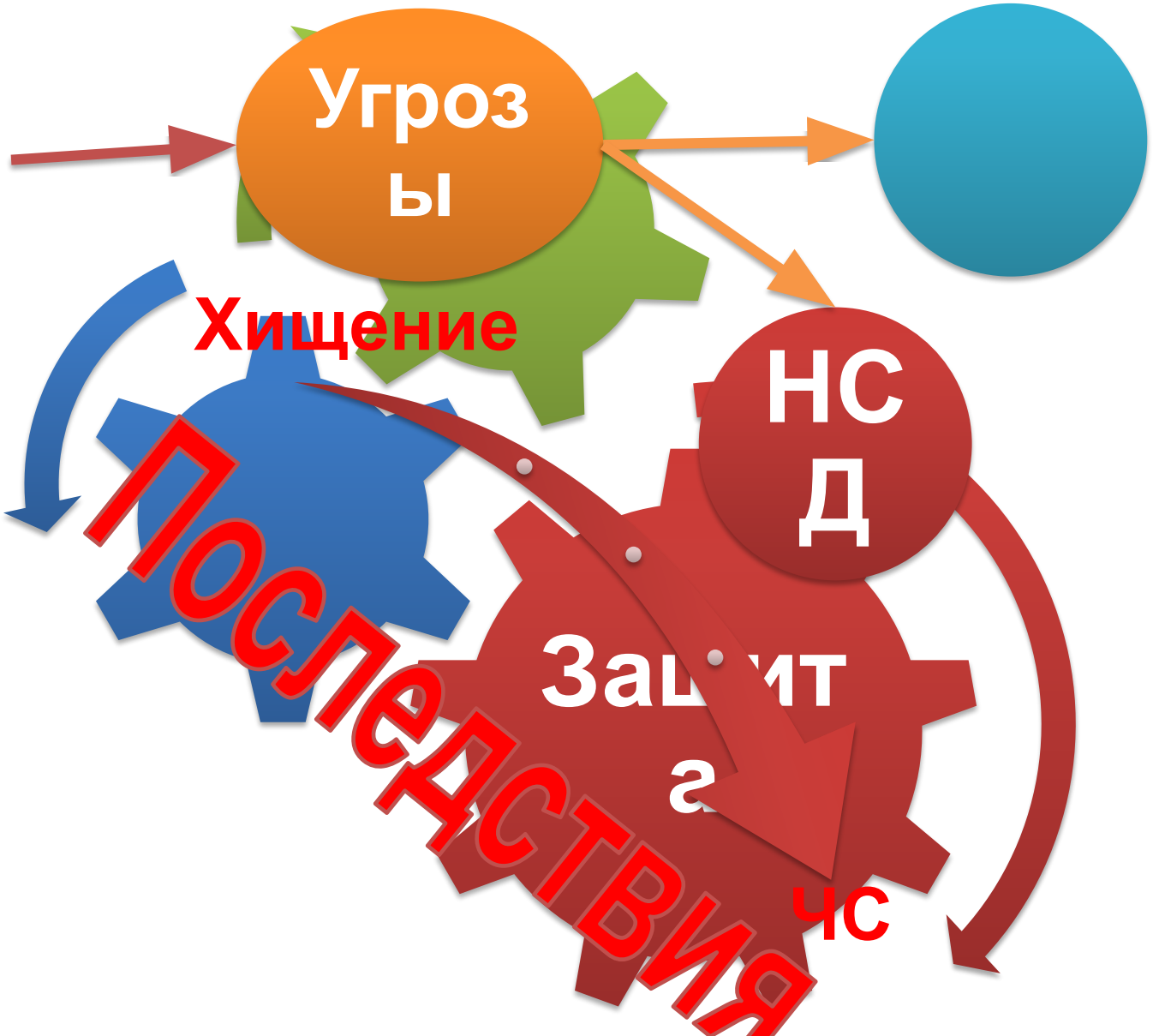
УДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

«Участник молодежного научно-инновационного конкурса»
«У.М.Н.И.К.»

Разработка программно-аппаратного комплекса оценки несанкционированных действий злоумышленников в системе физической защиты информационных объектов

Цвырко Снежана Олеговна,
студентка III курса МГОТУ

Защита информационных объектов



Цель проекта

Снижение ожидаемого **ущерба** (**рисков**) от действий злоумышленника за счет моделирования оптимальных действий служб безопасности

Научная новизна проекта

- Создание интегрированный поведенческой функции на базе дифференцированных поведенческий функций объекта
- Динамическое прогнозирование поведенческой функции нарушителя методами хромоматематики
- Использование инновационного зонно-рубежного отображения прогнозируемых перемещений
- Предлагается построение поведенческих функций с использованием ИИ на базе пролог-машины

Актуальность идеи

Повышение требовании **эффективности** физической защиты информационных объектов в условиях современных агрессивных воздействий

Многофакторность условий и высокая **оперативность** выходных решений в области противодействия несанкционированному доступу злоумышленника к защищаемым информационным объектам требуют **автоматизации** процессов моделирования

Использование программы

Моделирование проникновения

Режимы

- Реальное
- Прогнозируемое
- Статистическое

Исходные данные для оценки НСД

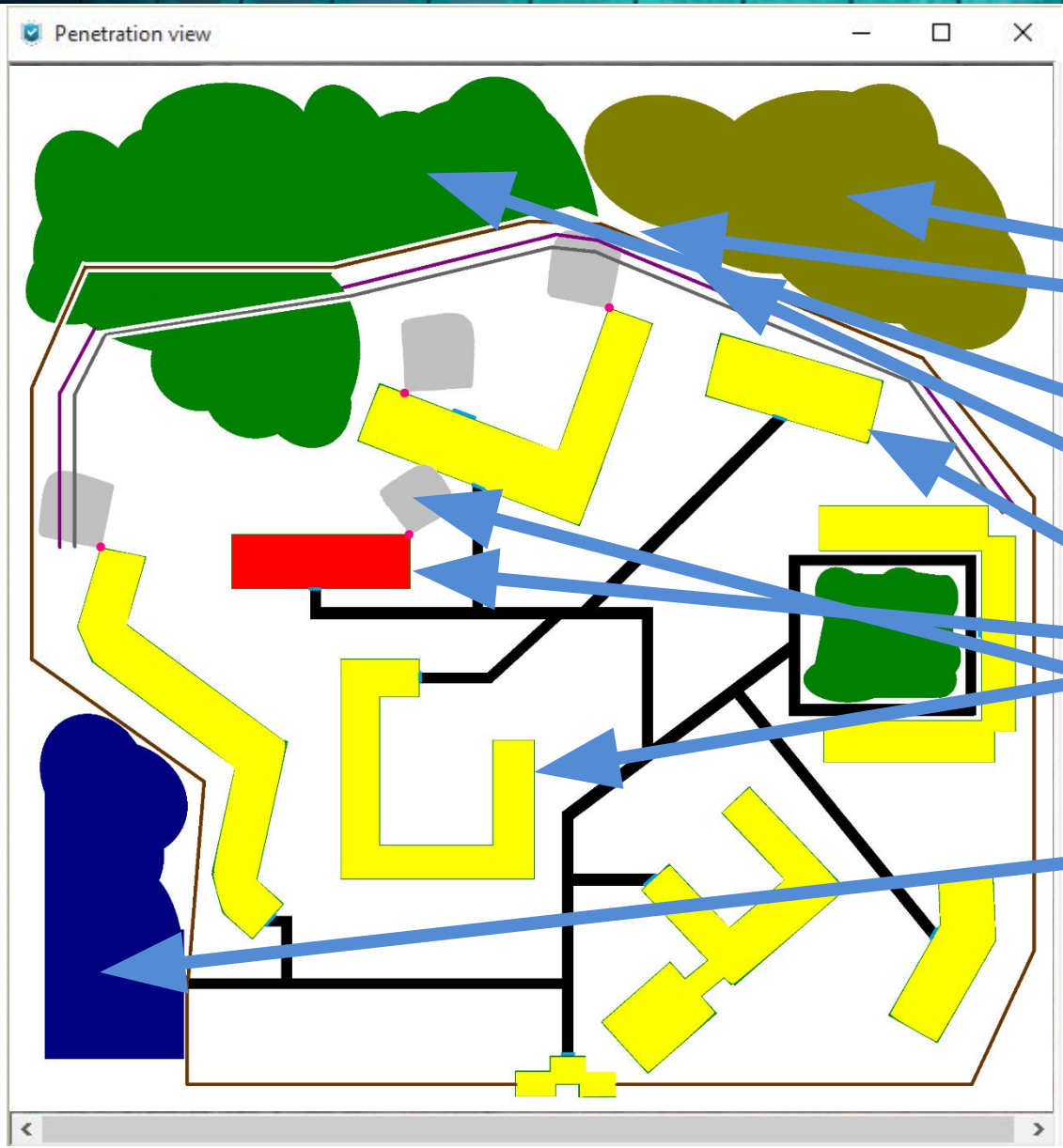
Болото

Лес

Здания

Озеро

Исходные данные для оценки НСД



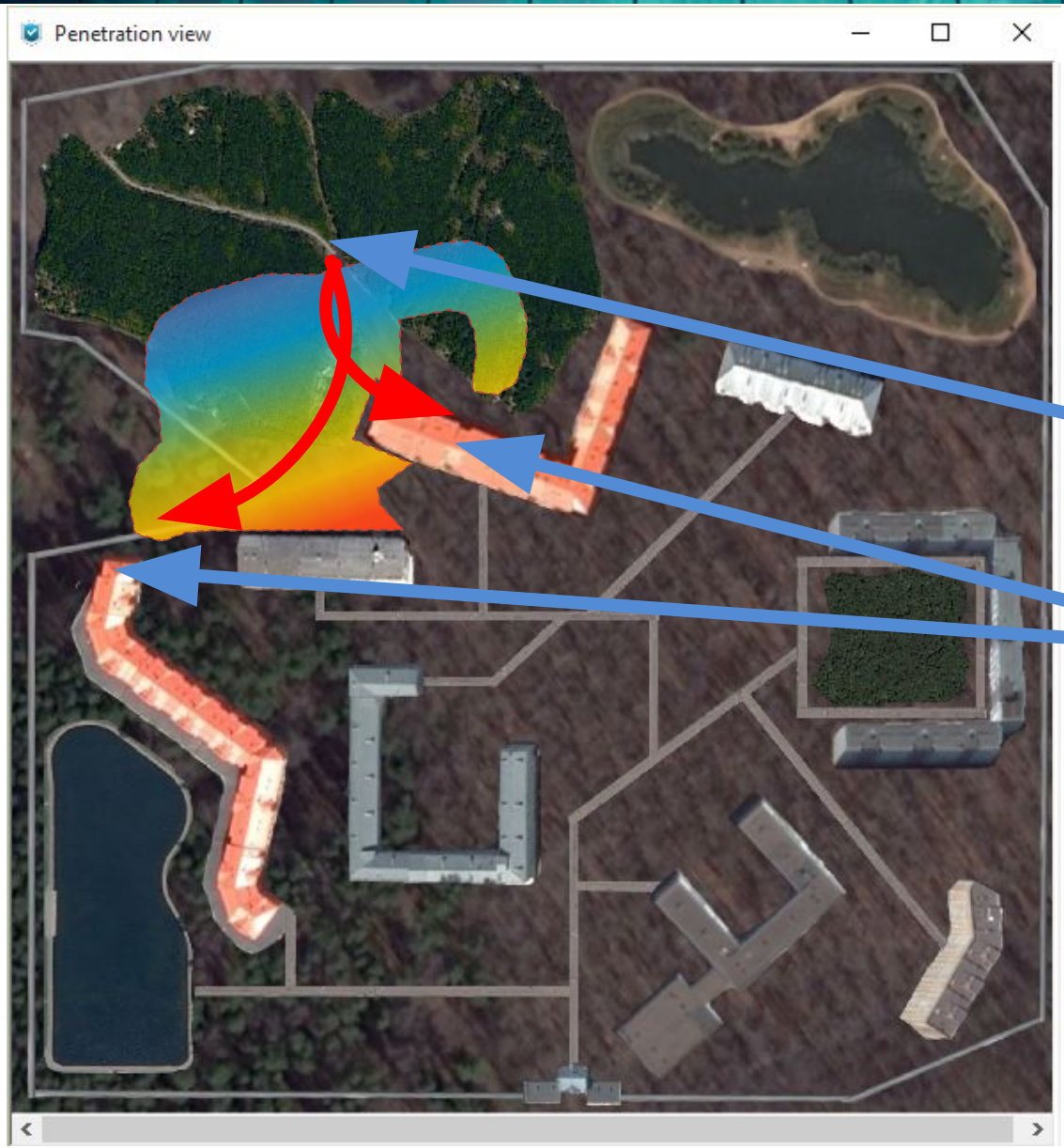
Ограждения

Барьеры

Камеры

Озеро

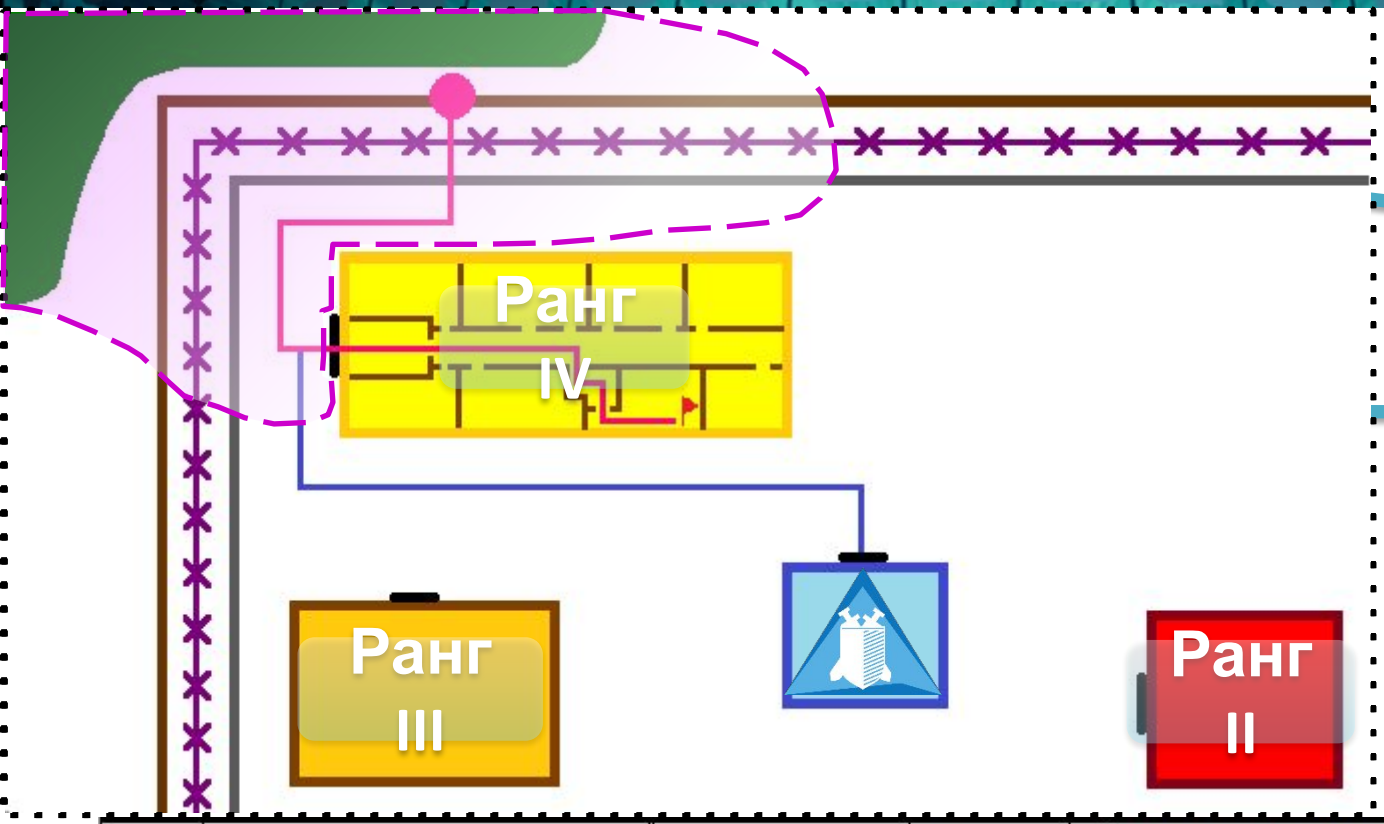
Исходные данные для оценки НСД



Старт

Цели

Техническая значимость



Здание

Прогноз на
5 минут

Охрана

Колючая проволока

Забор 1

Лес

Дверь

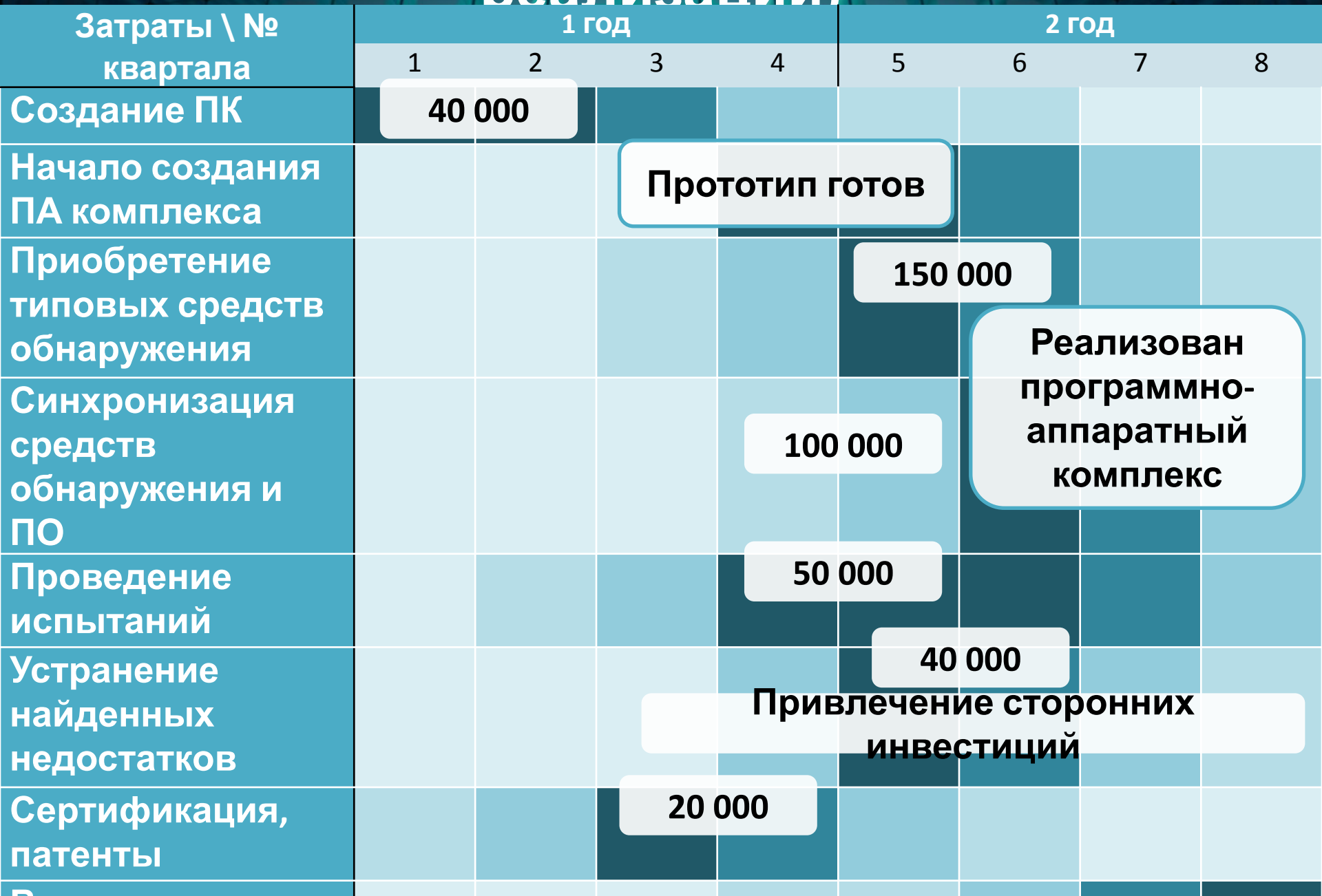
Забор 2

					9
2	Преодолеть колючую проволоку	0	B	180	54
					12
					36
					12
					90
					108

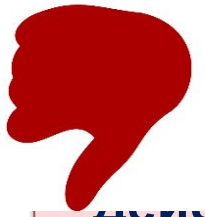
План реализации

Сейчас	1 год	2 год	Будущее
Определение направлений исследований	Программа У.М. Н.И.К.	Проведение испытаний. Демонстрация продукта	Получение сертификатов и лицензий
Сравнительная оценка вариантов решений	Создание прототипа	Поиск и привлечение инвесторов	Использование проекта на практике
Расчетно-теоретическое подтверждение	Методические работы, разработка технологий	Оформление авторских прав	Расширение круга потребителей и рынка
Анализ мирового опыта	Апробация на предприятии	Выход на рынок	Дальнейшее развитие проекта

Использование средств (план реализации)



Анализ рынка



- ожена жесткая тактика действий сил реагирования
- ✔Отсутствует база данных по реальным тактико-техническим характеристикам ТСФЗ и ФБ, относящихся к чувствительной информации
- ✔Погрешности в расчетах
- ✔Произведено за рубежом
- ✔Государственные (*не продаются*)

«Вега-2»

- АО «ФЦНИВТ «СНПО «Элерон»

«Контрфорс»

- ГЦ АСУ ВВ МВД России

«Спрут» и «Спрут-ИМ»

- Центр анализа уязвимостей НПП «Иста»

«ASSESS»

- Лаборатория «Сандия» США

«EASI»

- Министерство энергетики США

Совокупная стоимость владения

ROSI

Программно-аппаратный комплекс окупит себя через 1 год и 4 месяца

Перспективы коммерциализации

Потенциальный заказчик

Государственная корпорация по космической деятельности «Роскосмос»
Федеральное государственное унитарное предприятие
"ГОСУДАРСТВЕННЫЙ КОСМИЧЕСКИЙ НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР имени М.В. ХРУНИЧЕВА"
"НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ КОСМИЧЕСКИХ СИСТЕМ имени А.А. МАКСИМОВА" -
филиал ФГУП "ГКНПЦ им. М.В. Хруничева"

ул. М.К. Тихонравова, д. 27, микрорайон Юбилейный, г. Королёв, Московская область
Тел.: 8-498-300-29-19

Рецензия

на научно-исследовательскую работу

«Программно-аппаратный комплекс оценки несанкционированных действий злоумышленников в системе физической защиты информационных объектов»

Отдел комплексной безопасности «НИИ КС имени А.А. Максимова» рассмотрел содержание научно-исследовательского проекта Бессонова А.В. и Цвырко С.О. на тему: «Программно-аппаратный комплекс оценки несанкционированных действий злоумышленников в системе физической защиты информационных объектов» и подтверждает, что работа построена на основе материалов, предоставленных предприятием. Имеет практическую значимость, актуальность и рекомендуема к использованию профильными специалистами предприятия при проведении мероприятий по обеспечению информационной безопасности критических объектов.

В целом, разработанный Бессоновым А.В. и Цвырко С.О. программно-аппаратный комплекс имеет практическое значение не только для критически важных предприятий космической промышленности в части анализа управления прогнозируемыми и реальными инцидентами в области информационной безопасности. В то же время, разработанную в работе методологию оценки эффективности противодействия несанкционированным действиям злоумышленников целесообразно использовать в научно-исследовательской деятельности в сфере информационной безопасности.

На данный момент проект Бессонова А.В. и Цвырко С.О. находится на стадии дальнейшего развития. Отдельные результаты проекта использовались при комплексном анализе уязвимостей на базе НИИ КС.

Служба безопасности НИИ КС заинтересована в дальнейшем развитии проекта и поддерживает участие Бессонова А.В. и Цвырко С.О. в открытом конкурсе на лучшую работу студентов ВУЗов в области информационной безопасности.

Заместитель директора НИИ КС
по безопасности и режиму – начальник отдела
комплексной безопасности объекта

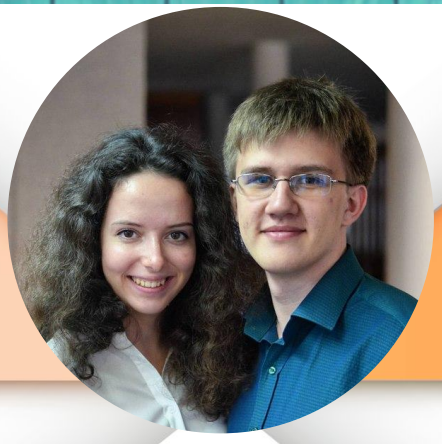
Ткаченко Григорий Иванович

«12» окт 2016 г.

??

Команда проекта

Цвырко
Снежана Олеговна
tsnwork@mail.ru



Бессонов
Александр
Владимирович
alexanderbessonov@mail.ru

Цвырко
Олег Леонидович
http://ameta.ucoz.org/

Соляной
Владимир Николаевич
solyanoy@ut-mo.ru

УДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

«Участник молодежного научно-инновационного конкурса»
«У.М.Н.И.К.»

Разработка программно-аппаратного комплекса оценки несанкционированных действий злоумышленников в системе физической защиты информационных объектов

Цвырко Снежана Олеговна,
tsnwork@mail.ru
+7 985 855 97 89

Благодарю за

Структура модулей программного комплекса

Выводы

1. Создан **авторский алгоритм** моделирования области предполагаемого нахождения и прогнозирования перемещения злоумышленника на защищаемой территории

2. Разработан **прототип** программного комплекса, позволяющий на первом этапе прогнозировать во времени действия злоумышленника с графическим отображением.

Выводы (продолжение)

3. Основой предложенного проекта по усовершенствованию подсистемы физической защиты информационных объектов предприятия является **использование мероприятий** на основе внедрения разработанного программного комплекса.

Выводы (продолжение)

4. Функциональная оценка эффективности подсистемы физической защиты с учетом предложенных мер повысилась и достигла требуемого уровня (вероятность защиты информации) 0,89.

При этом вероятность защиты информации всей ИБ предприятия достигла требуемого уровня и составила 0,87.

Экономическая оценка проекта составила 12 300 000 руб. (экономически

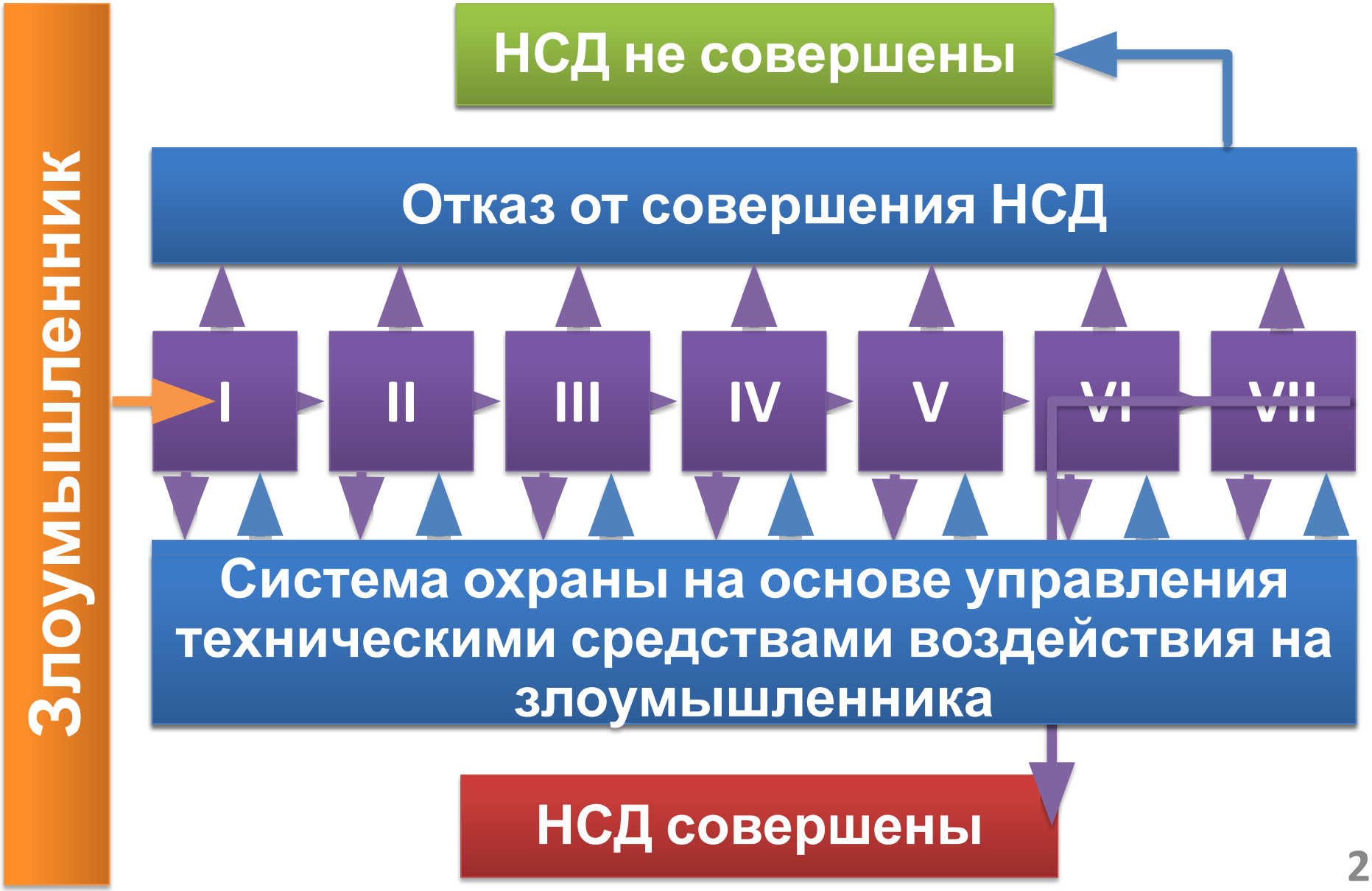
Выводы (продолжение)

5. Была уточнена **Политика безопасности** НИИ КС путем дополнения и добавления пунктов в части:

- правовой базы;
- задач;
- мер обеспечения безопасности.

6. Цели проекта **достигнуты**.

Действия злоумышленника



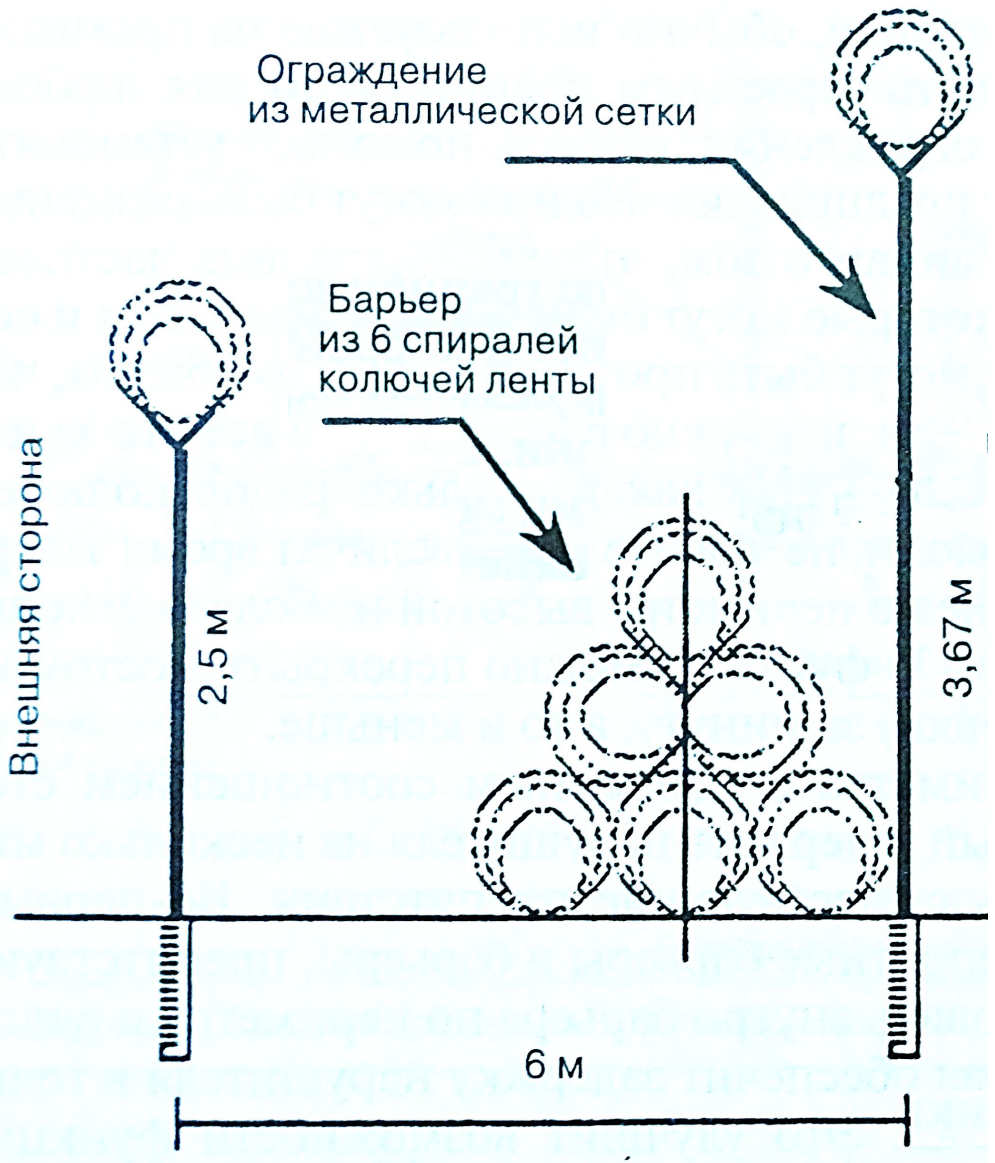
Принцип многослойности графического представления

- Карта
  - Здания
  - Особые УФО
- Схема
  - Здания
  - Особые УФО
- Приоритеты
  - Объекты
- Пути достижения
  - Наикротчайшие
- Время прохождения
  - Каждой клетки

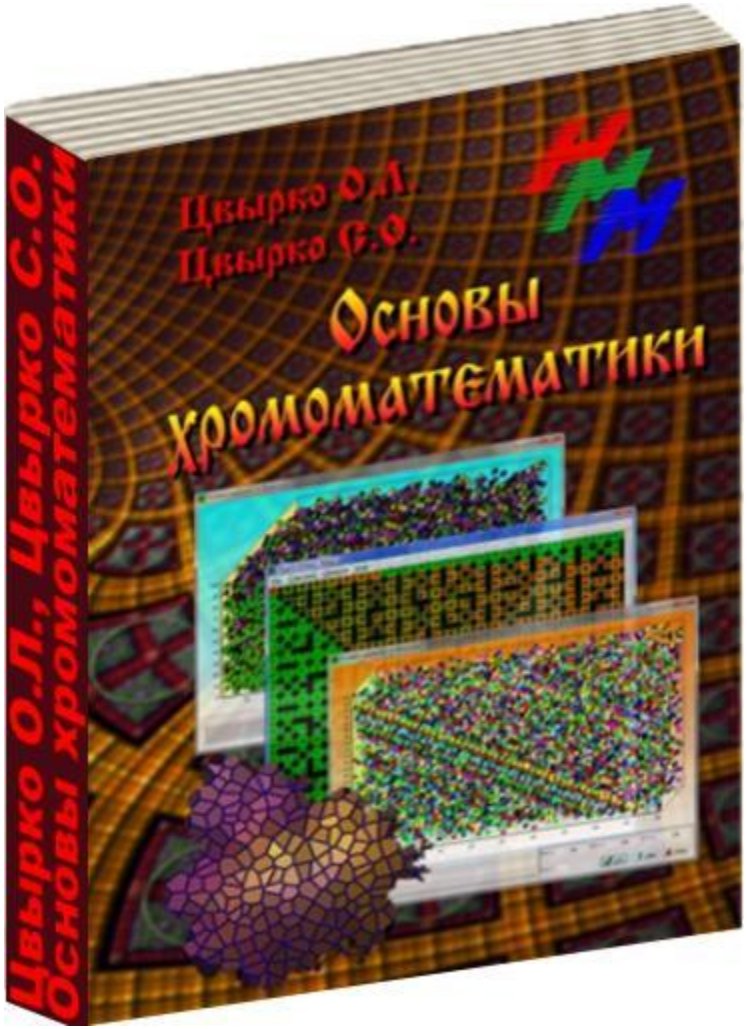
Система с ограждением и барьером

М.Гарсиа «Проектирование и оценка систем физический защиты», Мир: Москва, 2003

Время задержки ≈ 6 минут



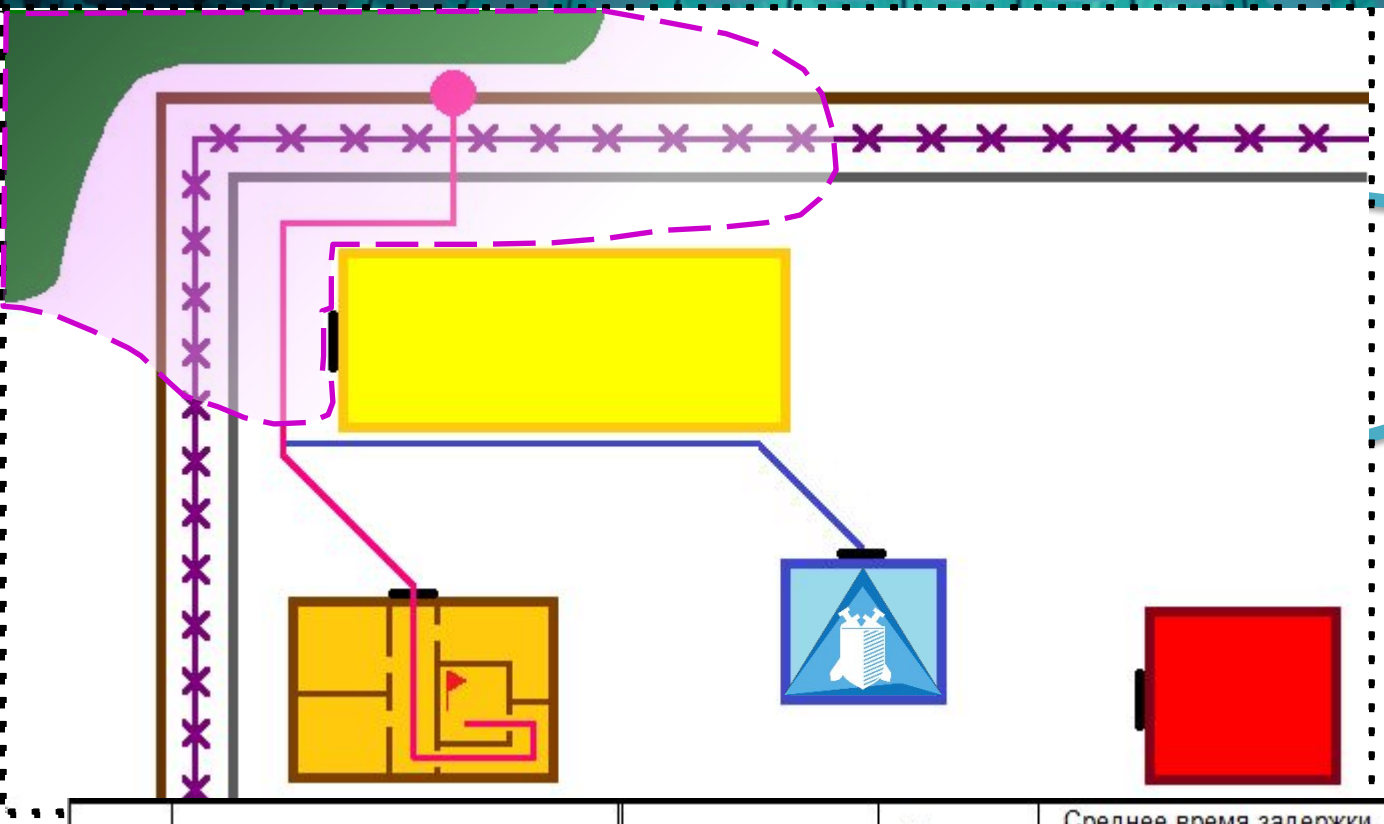
Публикации по проекту



Цвырко О.Л., Цвырко С.О. Основы хромоматематики

- **Монография**
  - Цвырко О.Л., Цвырко С.О. Основы хромоматематики. Монография. – Ишим: Изд-во ИГПИ им. П.П. Ершова, 2013. – 122 с.
- **Статьи**
  - Бессонов А.В., Цвырко С.О. Создание прикладного программного комплекса прогнозирования перемещения нарушителя. /сб. тезисов работ XV научной конференции студентов ФТА «Ресурсам области – эффективное использование», 2015.
  - Бессонов А.В., Цвырко С.О. Создание прикладного программного комплекса прогнозирования перемещения нарушителя. /сб. тезисов работ участников всероссийских конкурсов

Принцип моделирования НСД (2 путь)

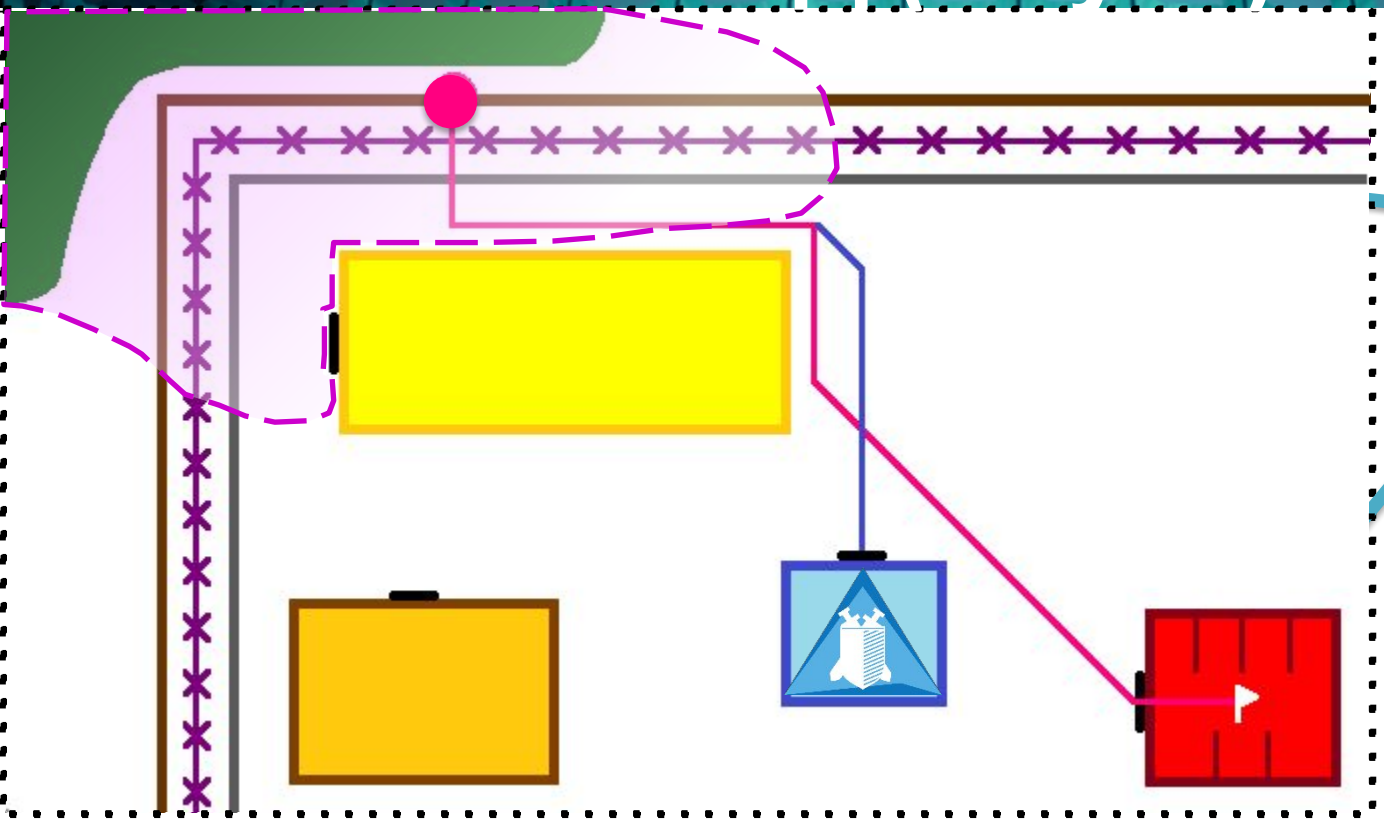


Старт

Вероятность перехвата 0,95

Задача	Описание	Вероятность обнаружения (Po)	Местопо-ложение ("B","M","E")	Среднее время задержки (Tsz),сек (или средн. время для прохождения участков пути нарушителем)	Стандартн. отклонение времени задержки (Sz),сек (приблизит. 30% от ср. знач)
1	Преодолеть первый забор	0,9	B	30	9
2	Преодолеть колючую проволоку	0	B	180	54
3	Преодолеть второй забор	0,8	B	30	12
4	Добежать до здания 2	0	B	60	18
5	Взлом внешней двери	0,7	B	120	36
6	Проникновение в кабинет	0	B	30	12
7	Кража информации	0,8	B	300	90
8	Уход с объекта	0	B	360	108

Принцип моделирования НСД (3 путь)

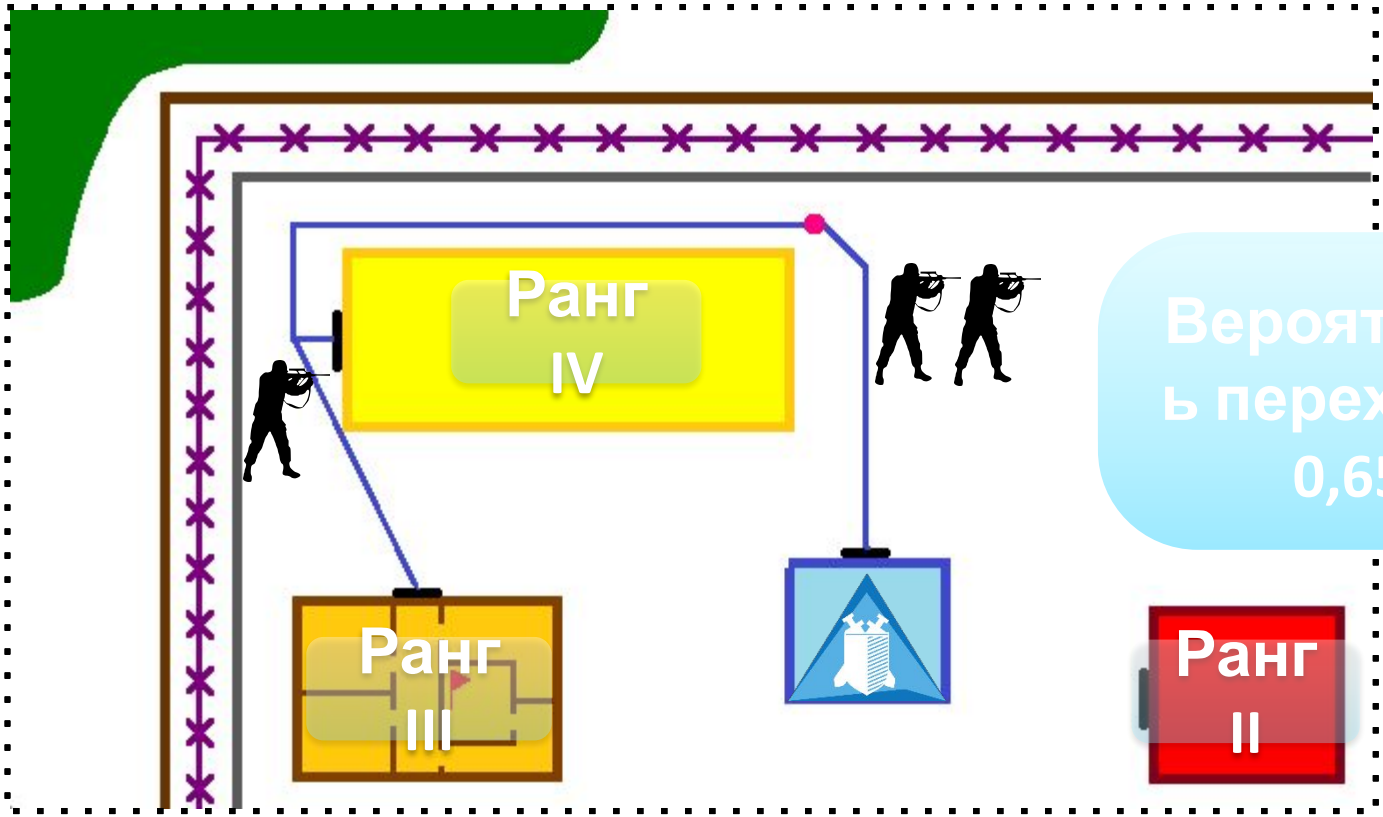


Старт

Вероятность перехвата 0,92

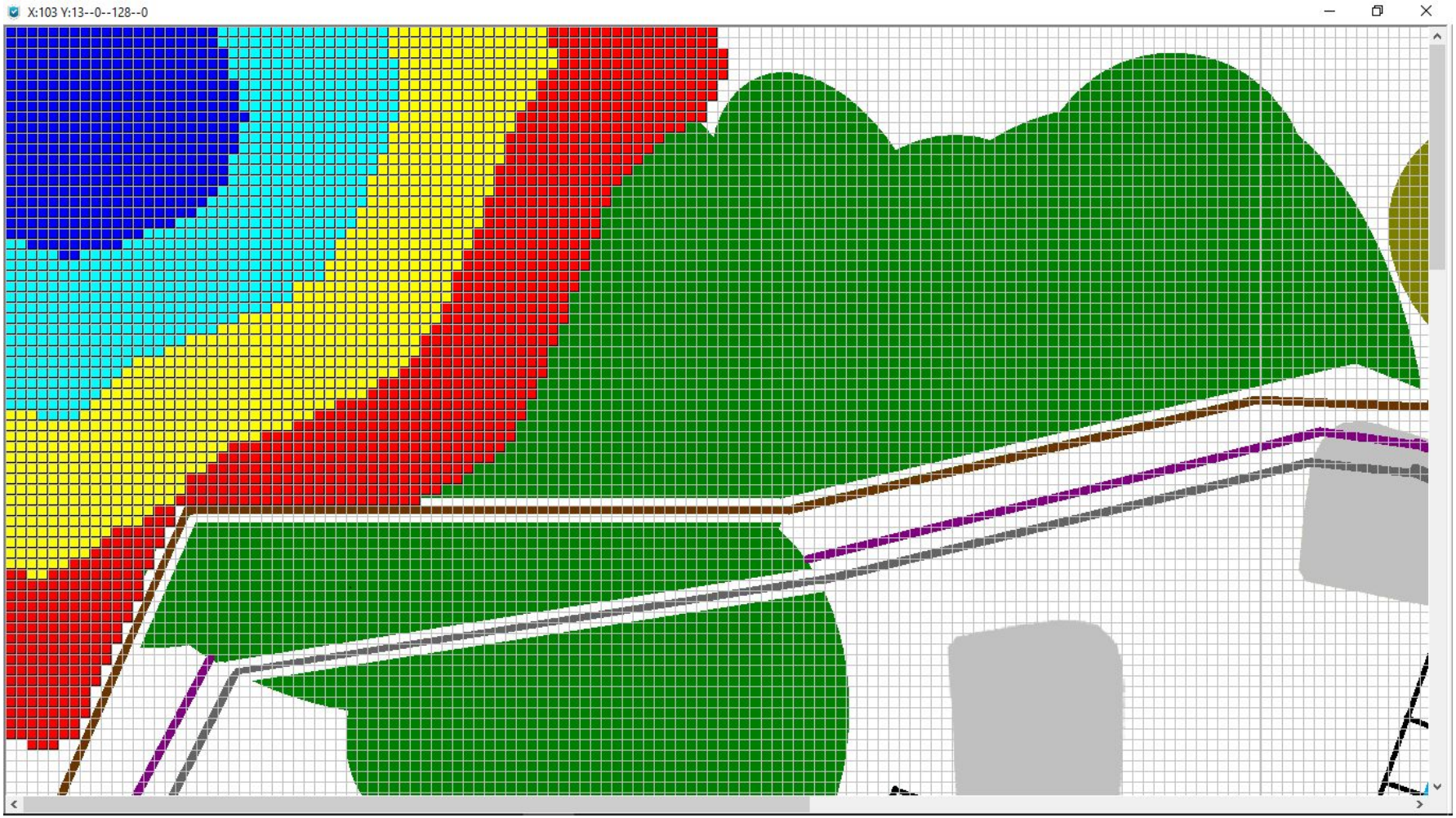
	Задача	Описание	Вероятность обнаружения (Po)	Местопо-ложение ("B","M","E")	Среднее время задержки (Tsz),сек (или средн. время для прохождения участков пути нарушителем)	Стандартн. отклонение времени задержки (Sz),сек (приблизит. 30% от ср. знач)
1.	1	Преодолеть первый забор	0,9	B	30	9
2.	2	Преодолеть колючую проволоку	0	B	180	54
3.	3	Преодолеть второй забор	0,8	B	30	12
	4	Добежать до здания 3	0	B	90	27
	5	Взлом внешней двери	0,7	B	120	36
	6	Диверсия	0	B	30	9

Возможные автоматизированные

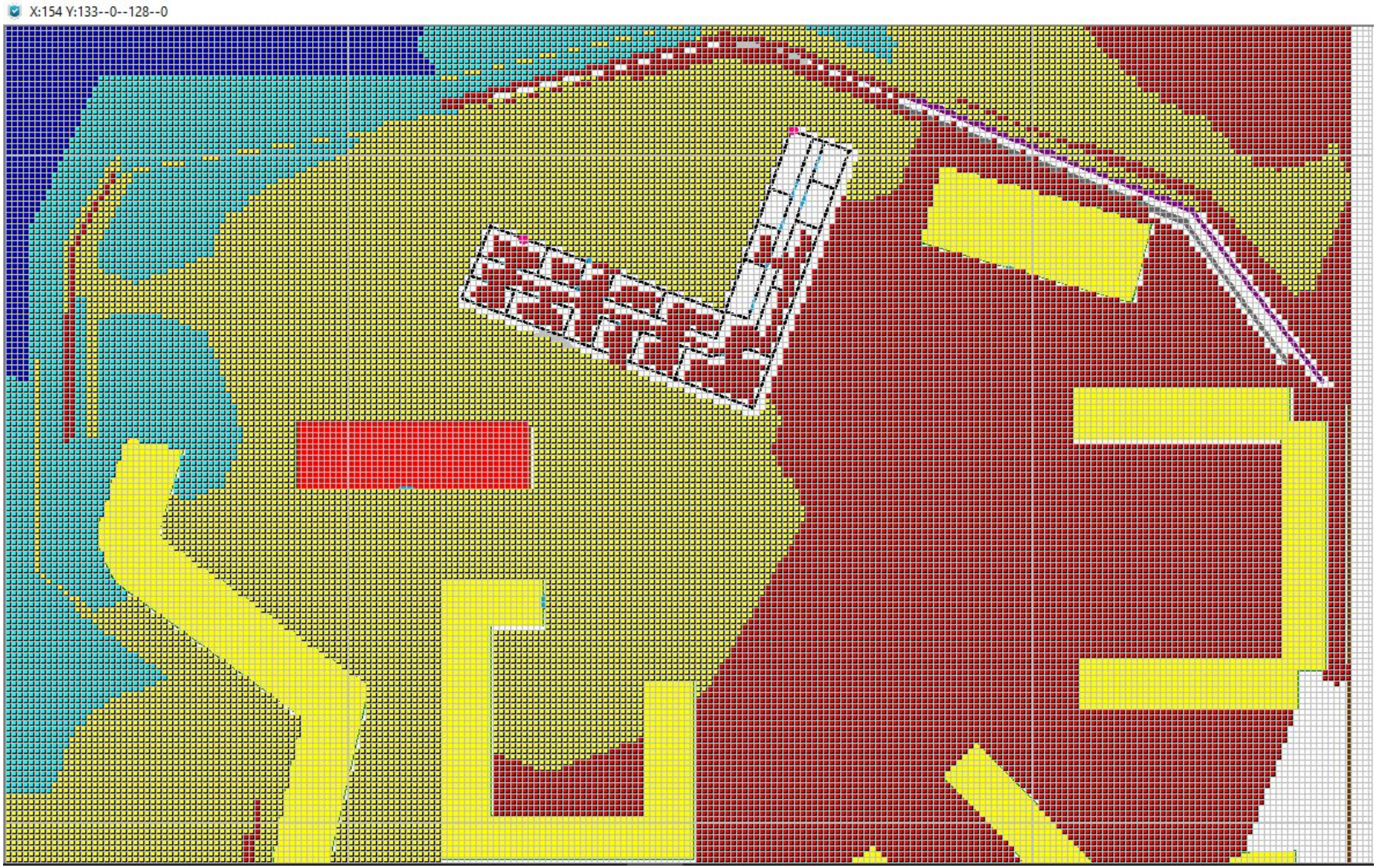


Задача	Описание	Вероятность обнаружения (Po)	Местопо-ложение ("B","M","E")	Среднее время задержки (Tsz),сек (или средн. время для прохождения участков пути нарушителем)	Стандартн. отклонение времени задержки (Sz),сек (приблизит. 30% от ср. знач)
1	Добежать до здания 2	0	B	60	18
2	Взломать внешние двери	0,7	B	120	36
3	Проникновение в кабинет	0	B	30	9
4	Кража информации	0,8	B	300	90
5	Уход с объекта	0	B	360	108

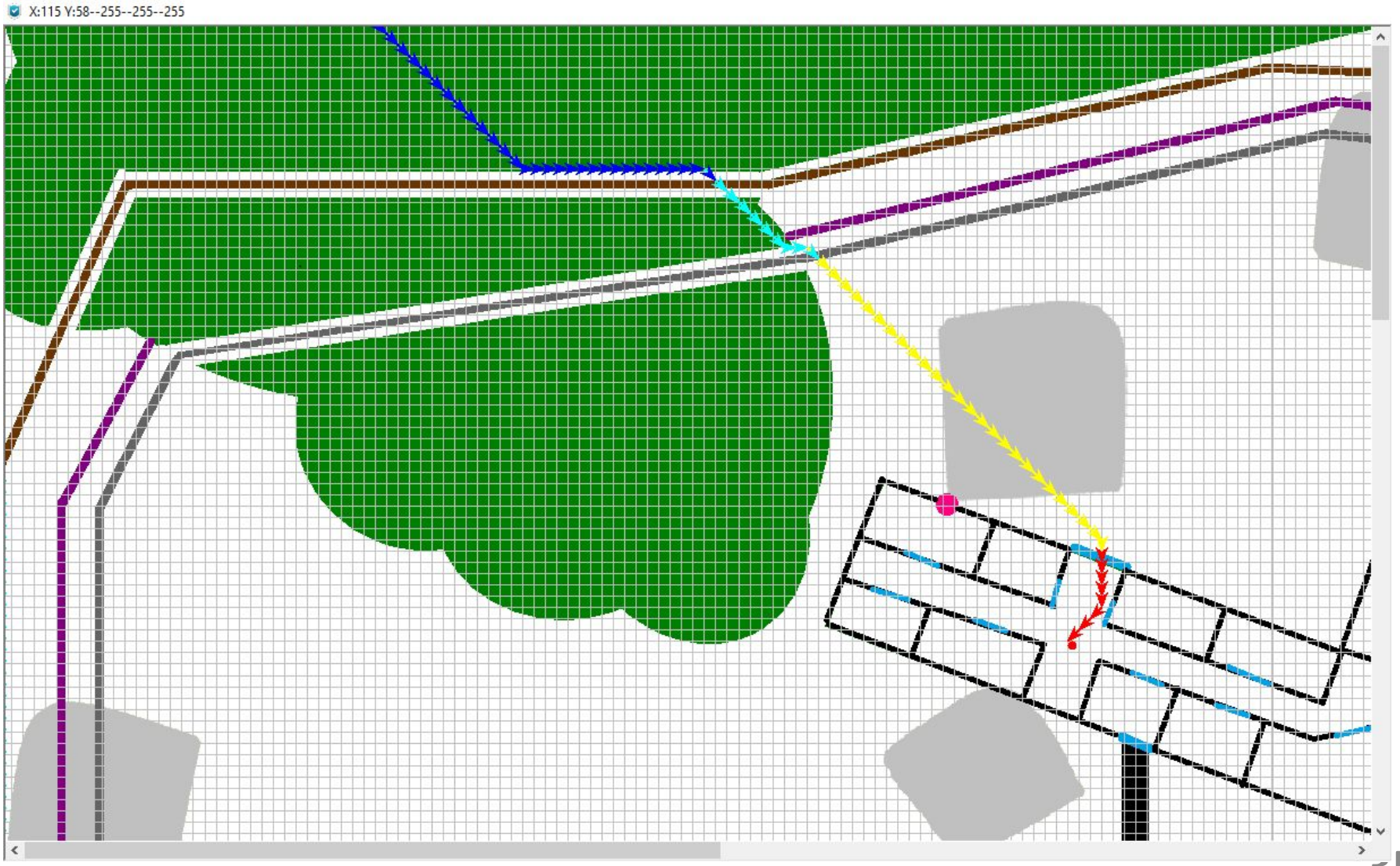
Область предполагаемого места нахождения злоумышленника (50 сек.)



Область предполагаемого места нахождения злоумышленника (5 мин.)



Прогнозируемый маршрут злоумышленника



Анализ прогнозируемого маршрута злоумышленника