

# СИТУАЦИОННАЯ БЕЗОПАСНОСТЬ

---

"Системы безопасности - реальная защита или  
самоуспокоение для клиента?"

Авторы:  
Дмитрий Борощук  
Евгений Озеров

Информационный спонсор

- ФИЗИЧЕСКАЯ ЗАЩИТА
- ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ
- ПОЖАРНАЯ БЕЗОПАСНОСТЬ
- ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

---

# КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ



### ПСИХОЛОГИЯ

- Профайлинг

Понятие, обозначающее совокупность психологических методов и методик оценки и прогнозирования поведения человека на основе анализа наиболее информативных частных признаков, характеристик внешности, невербального и вербального поведения.

- Психология толпы

раздел социальной психологии, изучающий поведение групп людей и отличия поведения групп от поведения отдельных индивидуумов.

## КЛЮЧЕВЫЕ НАВЫКИ

### КРИМИНАЛОГИЯ

«наука о преступлении», социолого-правовая наука которая изучает преступность, личность преступника, причины и условия совершения преступлений, пути и средства её предупреждения.

### КРИМИНАЛИСТИКА

прикладная юридическая, исследующая закономерности приготовления, совершения и раскрытия преступления, возникновения и существования его следов, собирания, исследования, оценки и использования доказательств, а также разрабатывающая систему основанных на познании этих закономерностей специальных приёмов, методов и средств применяемых в ходе предварительного расследования для предупреждения, раскрытия и расследования преступлений.

### СЕТЕВАЯ БЕЗОПАСНОСТЬ

Занимается изучением и разработкой методов и практических правил работы с сетью, в том числе протоколами связи и обмена данными и методами защиты информации.

### НАБЛЮДЕНИЕ И КОНТРНАБЛЮДЕНИЕ

- сбор сведений о противнике или конкуренте для обеспечения своей безопасности и получения.
- мероприятия, направленные на выявление установленного за объектом наблюдения

## ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ

### ОТКРЫТЫЕ ОБЩЕСТВЕННЫЕ ПРОСТРАНСТВА

Парки, скверы, площади, придомовая территория, общественно-рекреационные кварталы, микрорайоны, жилые комплексы.

### ЗАКРЫТЫЕ ОБЩЕСТВЕННЫЕ ПРОСТРАНСТВА

Торговые центры, Кино-Концертные комплексы, Многофункциональные общественные центры

### АДМИНИСТРАТИВНЫЕ ПРОСТРАНСТВА

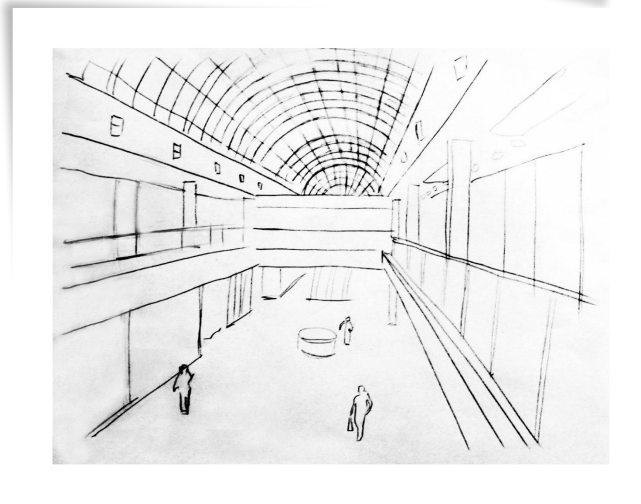
Офисные центры, Отдельные крупные офисы

### ПРОИЗВОДСТВЕННЫЕ ПЛОЩАДКИ

Стройки, Заводы, Склады

### ТРАНСПОРТНЫЕ УЗЛЫ

Вокзалы, аэропорты, станции метро



ЧТО СЛЕДУЕТ УЧИТЫВАТЬ ПРИ ПРОЕКТИРОВАНИИ КОНЦЕПЦИИ СБ:

- Территориальное расположение
- Социальный контингент
- Криминогенная обстановка
- Удаленность от транспортных артерий
- Поток людей



## ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ. РУБЕЖИ БЕЗОПАСНОСТИ

ВНЕШНЯЯ ЗОНА  
БЕЗОПАСНОСТИ

### 1. ОБЩИЙ ВНЕШНИЙ ПЕРИМЕТР

Прилегающие улицы,  
автомобильные дороги и здания

### 2. СОБСТВЕННАЯ ВНЕШНЯЯ ТЕРРИТОРИЯ

Территория прилегающая непосредственно к  
объекту

### 3. ВНУТРЕННИЙ ПЕРИМЕТР

Внутренняя территория объекта  
включающая общедоступные зоны



## ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ. РУБЕЖИ БЕЗОПАСНОСТИ

ВНУТРЕННЯЯ ЗОНА  
БЕЗОПАСНОСТИ

**4. СЛУЖЕБНАЯ ЗОНА**  
Офисы, складские помещения

**5. СЛУЖЕБНО-ТЕХНИЧЕСКАЯ ЗОНА**  
Зона размещения технического оборудования  
для жизнеобеспечения Комплекса и  
размещения технических средств систем  
безопасности.

**6. ДИСПЕТЧЕРСКИЙ ПОСТ**  
Пост управления техническими  
средствами жизнеобеспечения,  
наблюдения и безопасности  
объекта

### Естественные места безопасности:

#### Условия:

- Места естественного скопления людей
- Наличие средств связи или системы тревожного оповещения
- Наличие хорошего освещения
- Возможность закрытия периметра
- Наличие средств оказания первой помощи



#### Примеры:

- Магазины и «торговые лавки»
- Посты охраны
- Информационные пункты
- Остановки транспорта
- Пункты Банкоматов
- Подъезды домов с консьержем

### Естественные места безопасности:

#### Условия:

- Места естественного скопления людей
- Наличие средств связи или системы тревожного оповещения
- Наличие хорошего освещения
- Возможность закрытия периметра
- Наличие средств оказания первой помощи



#### Примеры:

- Магазины и «торговые лавки»
- Посты охраны
- Информационные пункты
- Остановки транспорта
- Пункты Банкоматов
- Подъезды домов с консьержем

### ВНЕШНЯЯ ЗОНА БЕЗОПАСНОСТИ

- повреждения входных дверей, решеток, ограждений, витрин, а также транспортных средств личных и служебных;
- хулиганские действия;
- технологические аварии, пожары, стихийные бедствия и т.п.;
- повреждения, угон личных транспортных средств;
- причинение вреда здоровью, побои;
- ограбления;
- поджоги;
- обстрел из огнестрельного оружия;
- нападения, вторжения, захват, пикетирования, блокирование;
- убийство, угроза убийством;
- угрозы террористического характера

### ВНУТРЕННЯЯ ЗОНА БЕЗОПАСНОСТИ

- умышленная и непредумышленная порча персоналом ТМЦ;
- хищения, кражи;
- клевета;
- подлог и подмена одного товара другим;
- потеря товарного вида в результате складских операций;
- нарушение упаковки;
- пересортица;
- порча от воздействия или неправильной эксплуатации торгового оборудования;
- неправильное хранение (не обеспечивающее сохранность и товарный вид);
- техногенные аварийные ситуации;
- повреждения, угон личных транспортных средств;
- повреждения входных дверей, решеток, ограждений, витрин;
- хулиганские действия;
- нападение с целью завладения денежными средствами, ценностями и документами.
- причинение вреда здоровью, побои;
- психологический террор, угрозы, запугивание, шантаж, вымогательство;
- убийство, угроза убийством;
- угрозы террористического характера

## ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ.

### РОЛЕВЫЕ МОДЕЛИ НАРУШИТЕЛЕЙ

В ЗАВИСИМОСТИ ОТ:

- Типа объекта
- Территориального расположения
- Охраняемых активов
- Умысла (намеренное/непреднамеренное)



РОЛЕВЫЕ МОДЕЛИ НАРУШИТЕЛЕЙ

# ТЕРРОРИЗМ



СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.

УСЛОВНЫЕ

ЗАГРАЖДЕНИЯ

ФИЗИЧЕСКИЕ



- Организация пространства
- Четкое понимание вероятностей угроз



ДАТЧИКИ



ЗВУК / ВИДЕО / ДВИЖЕНИЕ / ЗАДЫМЛЕННОСТЬ / ТЕМПЕРАТУРА / ВЛАЖНОСТЬ / ДАВЛЕНИЕ / РАДИОЭФИР

ДАТЧИКИ



ГАЗОАНАЛИЗАТОРЫ / ДЕТЕКТОРЫ МЕТАЛЛА / РЕНТГЕН

## СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.



- ВИДЕОНАБЛЮДЕНИЕ. ОХРАННОЕ ТЕЛЕВИДЕНИЕ
- ПРОТИВОПОЖАРНАЯ АВТОМАТИКА
- ОХРАННАЯ СИГНАЛИЗАЦИЯ
- СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ
- ОПОВЕЩЕНИЕ И УПРАВЛЕНИЕ ЭВАКУАЦИЕЙ
- ПРОТИВОКРАЖНАЯ СИСТЕМА
- СИСТЕМА АВТОМАТИЧЕСКОЙ ПАРКОВКИ
- СИСТЕМА АНТИТЕРРОРИСТИЧЕСКОГО КОНТРОЛЯ

# ИНТЕГРИРОВАННАЯ СИСТЕМА БЕЗОПАСНОСТИ

## ситуационный анализ



1. Разделение с общей ИС на физическом (логическом) уровне.
2. Контроль за подключенными устройствами. Правило «Белого списка»
3. Раздельные коммутационные шкафы с общей ИС
4. Раздельное размещение основных блоков устройств ИСБ и рабочих мест операторов
5. Замкнутая инфраструктура
6. Контроль за пользователями системы
7. Мультифакторная авторизация

### ПРОБЛЕМЫ

:



- Низкая квалификация
- Невыполнение своих трудовых обязанностей
- Воровство
- Зависимости (пьянство)
- Легкая цель для атак социальной инженерии

## СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.

### РЕШЕНИЯ

:

- Системное обучение
- Разделение подразделений (оперативные дежурные/ охрана на местах)
- Контроль за выполнением регламентных обязанностей.
- Контроль за работой
- Периодическое тестирование
- Четкое разделение прав доступа к ИС и к физическим объектам
- Четкая отработка сценариев взаимодействия в случае чрезвычайных ситуаций



- прогнозирование, своевременное выявление и устранение угроз безопасности персоналу и посетителям объектов безопасности, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развитию;
- отнесение информации к категории ограниченного доступа (служебной и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), а других ресурсов - к различным уровням уязвимости (опасности) и подлежащих сохранению;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявление негативных тенденций в функционировании Объектов;
- эффективное пресечение угроз персоналу и посягательств на ресурсы на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на нормальное функционирование Объектов.

- формирование целостного представления о системе безопасности Объектов и взаимодействие различных элементов этой системы;
- определение путей реализации мероприятий, обеспечивающих необходимый уровень надежной защищенности объекта;
- *повышение имиджа и популярности коммерческих и общественных объектов;*
- рост прибыли за счет гарантий безопасности имущественных прав и интересов посетителей;
- оптимизация количества сил и средств, необходимых для обеспечения безопасности;
- определение эксплуатационных издержек;
- разработка методов противодействия выявленным угрозам;
- создание структуры собственной безопасности; организация взаимодействия с государственными силовыми структурами и организациями, выполняющими надзорные и контролирующие функции.



- **универсальность**, все решения должны быть отработаны и унифицированы;
- **комплексность**, используемые приемы работы и применяемые технические средства взаимосвязаны между собой, дополняют друг друга по функциональным и техническим показателям;
- **разумная достаточность**, означающая, что мероприятия по обеспечению безопасности объекта должны быть адекватны возможным угрозам со стороны вероятного злоумышленника по финансовым, материально-техническим и кадровым ресурсам;
- **оперативность**, приоритет методов и средств защиты, обеспечивающих быстрое обнаружение и последующую нейтрализацию возможных угроз;
- **адаптивность**, средства защиты могут быть достаточно гибко приспособлены к изменениям организационных и технических условий функционирования объекта;
- **непрерывность**, систематичность, выбранные решения обеспечат достаточно эффективную круглосуточную защиту объекта;
- **целеустремленность** - сосредоточение усилий на защиту наиболее ценных ресурсов общественных площадок, жилых комплексов или торгово- административных центров и их уязвимых участков;
- **многорубежность**, использование дополнительных пространственных рубежей безопасности или методов защиты для наиболее ответственных, с точки зрения безопасности, помещений и зон объекта;

- **равнопрочность** создаваемых границ безопасности;
- **последовательность** в использовании соответствующих методов и средств обнаружения, отражения и ликвидации угроз безопасности объекта;
- **совместимость** с существующими системами;
- **простота**, экологическая чистота и незаметность ("дружественность"), предполагающие, что система безопасности не создаст дополнительных препятствий для нормального функционирования общественных площадок, жилых комплексов или торгово- административных центров не потребует очень высокой квалификации и длительной подготовки обслуживающего персонала, не причинит вреда защищаемым ценностям объекта;
- **неуязвимость** - способность противостоять предпринимаемым попыткам выведения системы из строя;
- **документированность**, регистрация интересующих событий, связанных с защищаемым объектом, что необходимо для последующего анализа тревожных и нештатных ситуаций и достигнутого уровня защищенности;
- **правомерность**, означающая, что все применяемые меры организационного и технического характера легальны и юридически обоснованы.

СДЕРЖИВАНИЕ

ПАРИРОВАНИЕ

ПРЕСЕЧЕНИЕ

- ЧЕТКОЕ РАЗДЕЛЕНИЕ УРОВНЕЙ ДОСТУПА
- КОНТРОЛЬ ВЫПОЛНЕНИЯ РЕГЛАМЕНТА
- ФИКСАЦИЯ ДЕЙСТВИЙ
- КОНТРОЛЬ ЗА ДЕЙСТВИЯМИ СОТРУДНИКОВ
- ИСПОЛЬЗОВАНИЕ РАЗДРАЖИТЕЛЕЙ
- РОТАЦИЯ НАБЛЮДАТЕЛЕЙ ПО ЛОКАЦИЯМ

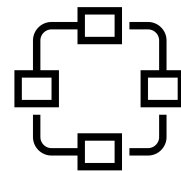
### МОНИТОРИНГ:

- ЭМОЦИОНАЛЬНОГО СОСТОЯНИЯ СОТРУДНИКОВ
- ПОВЕДЕНЧЕСКИХ АНОМАЛИЙ
- БЭКГРАУНДА (долги, суды, правонарушения)



ИСПОЛЬЗОВАНИЕ SIEM (Security information and event management) систем

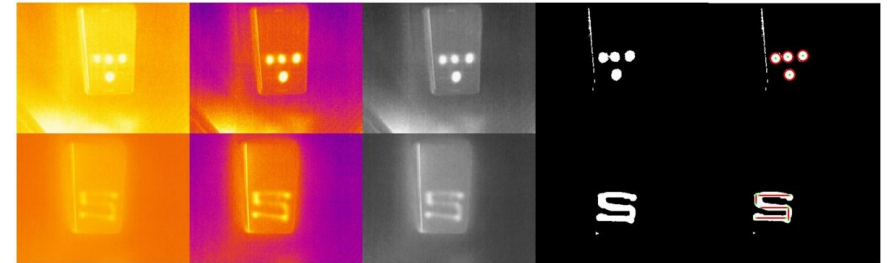
- Максимально разграничить доступ к тем или иным функциям управления системы безопасности.
- Настроить систему контроля и идентификации пользователей в системе.
- Осуществлять анализ действий пользователя в системе с уведомлением о действиях которые могут привести к образованию дыры в безопасности.
- Организовать многофакторную авторизацию пользователей. При этом надо понимать что способы аутентификации должны быть максимально просты и понятны со стороны пользователя.
- Сегментировать сеть



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



### КОПИРОВАНИЕ ИДЕНТИФИКАТОРОВ (карточки, отпечатки, пароли)





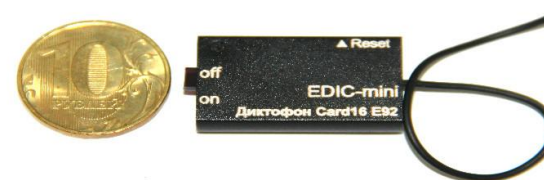
### ОБХОД ИЗВЕЩАТЕЛЕЙ (маскировка, глушение, подмена управляющих команд)



MITM атаки / Проникновение в сеть



Запись и трансляция переговоров



ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ

ЗАЩИТА ДАННЫХ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАЩИТА ОТ ДУРАКА

КОНТРОЛЬ РАБОТЫ СОТРУДНИКОВ СБ


ПРОАКТИВНАЯ ЗАЩИТА

(цель: предотвращение, а не фиксация происшествий)

РАЗУМНАЯ ДОСТАТОЧНОСТЬ

**ВОПРОСЫ ?**

beholderishere@gmail.com

+7 925 8584075  

t.me/eozerovRU