Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Кафедра вычислительной техники и защиты информации

КУРСОВОЙ ПРОЕКТ

по дисциплине
«Проектирование системы информационной безопасности»

Разработка метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадра

Руководитель:
д-р техн. наук, профессор
Т.З. Аралбаев
Студент гр. 17ИБ(б)КЗОИ:
Г.Д. Тихонов

Цель и задачи работы

Цель: снижение рисков информационной безопасности на основе метода управления системой защитного видеонаблюдения зала для конфиденциальных переговоров ОГУ.

Задачи:

1. Обосновать актуальность разработки метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадра;
2. Провести обзор современной научной литературы по теме «Разработка метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадра»;
3. Разработать классификацию систем видеонаблюдения;
4. Разработать модель угроз и нарушителя для зала конфиденциальных переговоров ОГУ;
5. Разработать технико-экономическое обоснование проекта.

Задача 1. Обосновать актуальность разработки метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадра

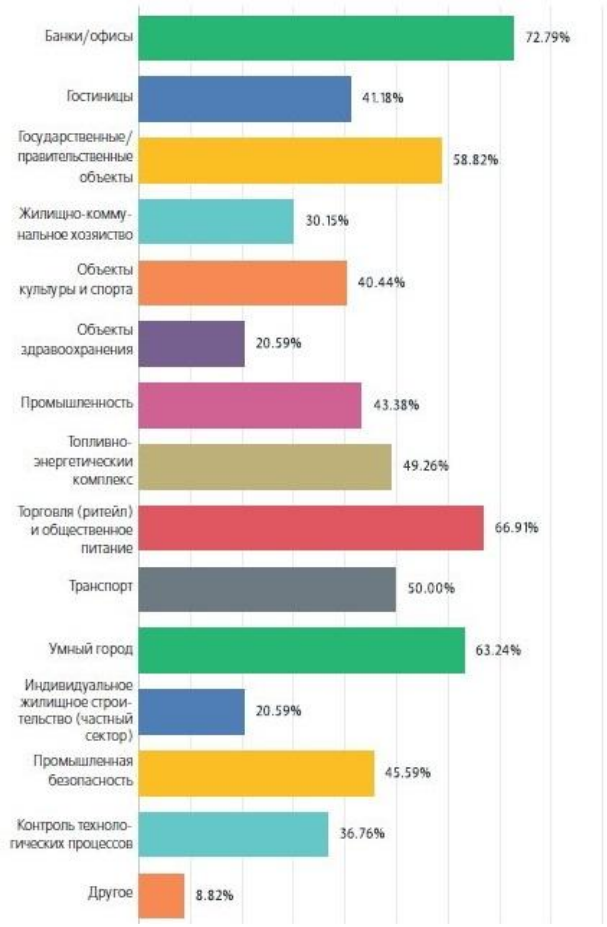

Рисунок 1 - Сферы, в которых востребовано видеонаблюдение

Задача 2. Обзор современной научной литературы по теме «Разработка метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадра»

Таблица 1- Обзор публикаций по теме управления адаптивной системой защитного видеонаблюдения

Автор и название	Описание
Е. В. Мешкова «Проектирование системы видеонаблюдения на объекте информатизации»[13]	В статье рассматривается технические средства обеспечения безопасности. Даются советы по проектированию системы видеонаблюдения до внедрения ее на производство. Более подробно рассматривается системы видеонаблюдения и ее проектирование с помощью программы IP Video System Design Tool.
К.А. Рылов «Видеоаналитика, системы и их сравнение»[14]	Работа посвящена анализу видеоаналитики, её возможностях, функциях. Показаны преимущества анализа потока видеокадров, приведены международные стандарты, сравнивается несколько систем видеоаналитики.
О.А. Калита «Основы организации адаптивных систем защиты информации»[15]	В данной статье рассматриваются общие принципы построения адаптивных систем. Также исследованы существующие подходы к организации адаптивных систем защиты информации.
Д. Ю. Жмурко «Понятие, сущность и классификация адаптивного управления системами с организационной сложностью»[16]	В статье рассматриваются понятие и сущность адаптивного управления. Разработана классификация адаптивной системы управления (АСУ). Представлен пример адаптивного управления системой со сложной организацией для интегрированных сегментов сахарного подкомплекса АПК.

Задача 3. Классификация систем видеонаблюдения

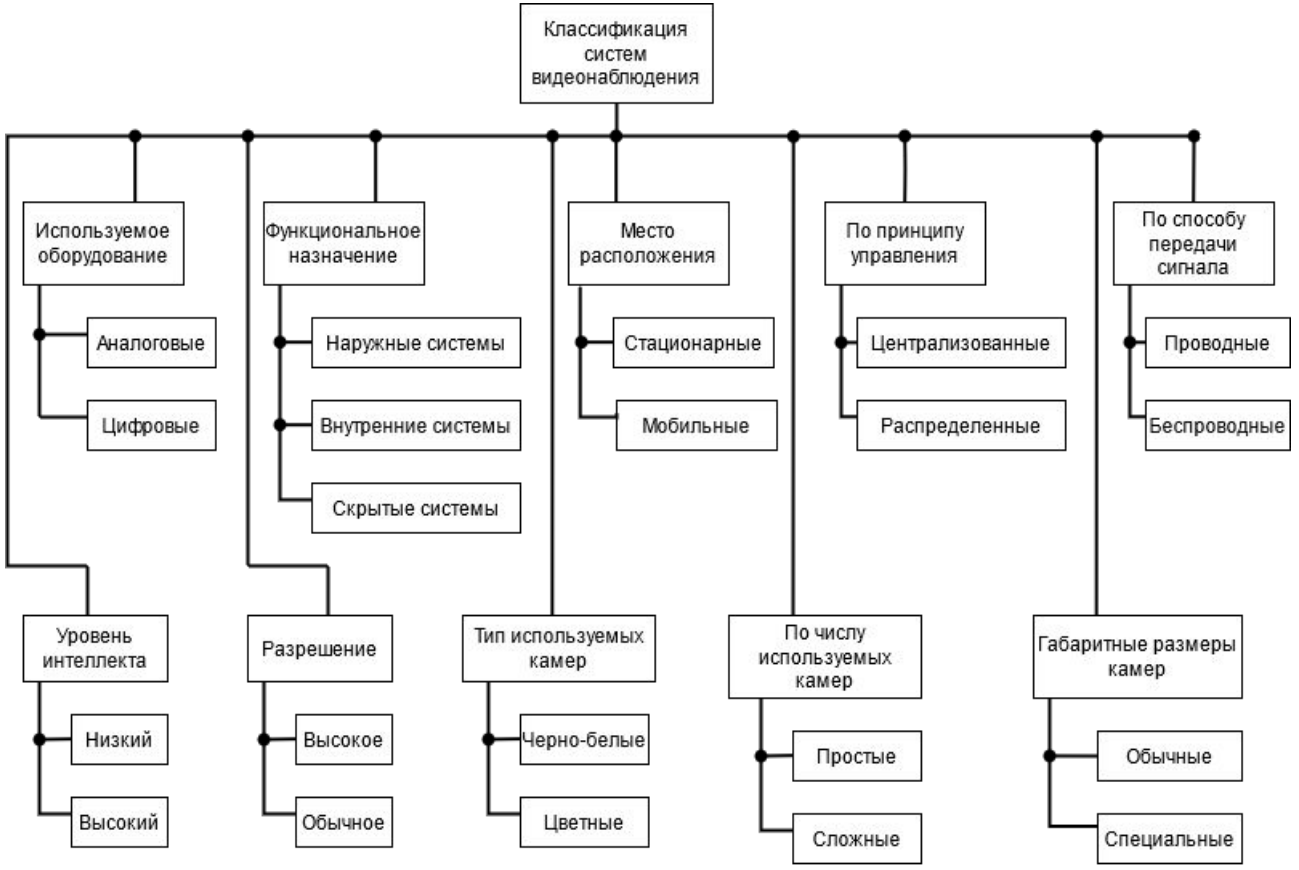

Рисунок 2 - Классификация систем видеонаблюдения

Задача 4. Разработка моделей угроз и нарушителя для зала конфиденциальных переговоров ОГУ

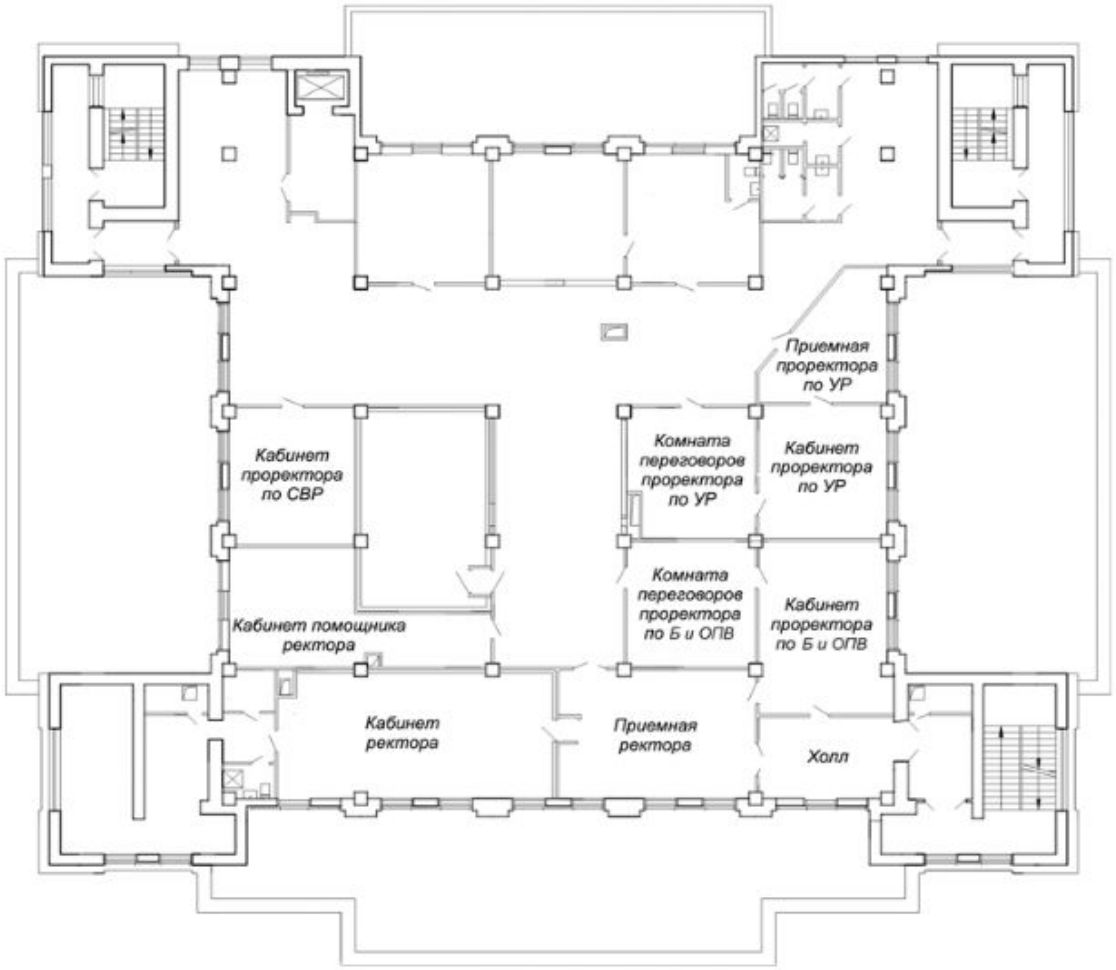

Рисунок 3 – План объекта

Задача 4. Разработка моделей угроз и нарушителя для зала конфиденциальных переговоров ОГУ

Таблица 2 – Характеристика внешних нарушителей объекта

Условное обозначение нарушителя	Наименование внешнего нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
Нарушители без доступа к контролируемой зоне и доступа к системе СКУД ОГУ		
Н1	Бывшие сотрудники университета	Месть за ранее совершенные действия; Причинение имущественного ущерба путем мошенничества или иным преступным путем.
Н2	Бывшие студенты университета	Месть за ранее совершенные действия; Причинение имущественного ущерба путем мошенничества или иным преступным путем.
Н3	Агенты конкурирующих университетов	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием.
Н4	Специальные службы иностранных государств(блоков государств)	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций
Н5	Террористические, экстремистские группировки	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики; Идеологические или политические мотивы. Организация террористического акта; Дискредитация или дестабилизация деятельности органов государственной власти, организаций.
Н6	Иные внешние субъекты(мелкие хулиганы, прохожие на улицы и т.д.)	Идеологические или политические мотивы. Любопытство или желание самореализации(подтверждение статуса).
Н7	Преступные элементы (профессиональные воры, хакеры и т.д.)	Причинение имущественного ущерба путем мошенничества или иным преступным путем; Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.

Таблица 3 – Характеристика внутренних нарушителей объекта

Условное обозначение нарушителя	Наименование внутреннего нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
Нарушители без доступа к контролируемой зоне, но имеющий доступ в системе СКУД ОГУ		
Н9	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на объект.	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
Н10	Посетители без доступа к КЗ	Любопытство или желание самореализации(подтверждение статуса). Непреднамеренные, неосторожные или неквалифицированные действия. Причинение имущественного ущерба путем мошенничества или иным преступным путем.
Н11	Студенты без доступа к КЗ	Любопытство или желание самореализации(подтверждение статуса). Непреднамеренные, неосторожные или неквалифицированные действия. Месть за ранее совершенные действия;
Н12	Сотрудники без доступа к КЗ	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.
Нарушители, имеющие ограниченный(временный) доступ к контролируемой зоне		
Н13	Сотрудники с доступом к КЗ(преподаватели, иные сотрудники, не имеющие полный	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации

Задача 4. Разработка моделей угроз и нарушителя для зала конфиденциальных переговоров ОГУ

Таблица 4 – Модель угроз безопасности

№	Наименование угрозы	Возможность	Степень ущерба, руб.	Актуальность
1	2	3	4	5
1	Угроза неправомерного ознакомления с защищаемой информацией	Высокий	Низкая	Актуальная
2	Угроза несанкционированного копирования, удаления, изменения защищаемой информации	Средняя	Высокая	Актуальная
3	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Низкая	Средняя	Неактуальная
4	Угроза преодоления физической защиты	Высокая	Средняя	Актуальная
5	Угроза использования каналов утечки для негласного съема конфиденциальной информации.	Средняя	Средняя	Актуальная
6	Угроза выхода из строя аппаратно-программных средств	Средний	Низкая	Неактуальная
7	Угроза природного характера, вызванная особенностями климата или погодных условий	Низкая	Средняя	Неактуальная
8	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Низкая	Средняя	Неактуальная
9	Угроза несанкционированного изменения параметров настройки средств защиты информации	Низкая	Средняя	Неактуальная
10	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Низкая	Средняя	Неактуальная
11	Угроза террористического акта	Средняя	Высокая	Актуальная
12	Угроза хищение материальных средства, оборудования, конфиденциальной информации объекта	Средняя	Высокая	Актуальная

Задача 5. Технико-экономическое обоснование разработки метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадров

Таблица 5 – Возможность реализации угроз до и после внедрения метода защиты

№	Наименование угрозы	Возможность реализации до внедрения метода	Возможность реализации после внедрения метода	Степень ущерба
1	Угроза преодоления физической защиты	Высокая	Низкая	Средний
2	Угроза террористического акта	Средняя	Низкая	Высокий
3	Угроза хищение материальных средства, оборудования, конфиденциальной информации объекта	Средняя	Низкая	Высокий
4	Угроза использования каналов утечки для негласного съема конфиденциальной информации	Средняя	Низкая	Средний
5	Угроза несанкционированного копирования, удаления, изменения защищаемой информации	Средняя	Низкая	Высокий

Задача 5. Технико-экономическое обоснование разработки метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадров

Внедрение метода управления СОТ на основе контроля динамики кадров позволит снизить время обнаружения нарушителя, повысит вероятность его распознавания и позволит оптимизировать вычислительные ресурсы системы.

Таблица 6 – Возможность реализации угроз до и после внедрения метода защиты

Показатели	До внедрения проекта	После внедрения проекта
Обнаружение движения	0	1
Автоматическое управление	0	1
Производительность	0	1
Вероятность ошибки	1	1
Распознавание нарушителя	0	1
Не требуется доп. оборудование	1	0
Итог:	2	5

Задача 5. Технико-экономическое обоснование разработки метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадров

5.1 Ожидаемый экономический эффект проекта

$$R_i = 10^{(S_i+V_i-4)},$$

Таблица 7 - Значения коэффициентов S_i и V_i

Ожидаемая (возможная) частота появления угрозы	Предполагаемое значение S_i
Почти никогда	0
1 раз в 1000 лет	1
1 раз 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
1–2 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7
Возможный ущерб при проявлении угрозы, руб.	Предполагаемое значение V_i
1	0
10	1
100	2
1000	3
10 000	4
100 000	5
1 000 000	6
10 000 000	7

Задача 5. Технико-экономическое обоснование разработки метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадров

5.1 Ожидаемый экономический эффект проекта

Коэффициент экономической эффективности от использования СЗФ вычисляется по формуле:

$$E_{СФЗ} = \frac{R_{до} - R_{после}}{K_{СФЗ}},$$

где $E_{СЗФ}$ – коэффициент экономической эффективности;
$K_{СЗФ}$ – затраты на СФЗ, которые включают в себя цену покупки, а также затраты на внедрение. Если $E_{СЗФ} > 1$, то данное СФЗ целесообразно использовать, и напротив, если $E_{СФЗ} \leq 1$ – то нецелесообразно.

$$E_{СФЗ} = \frac{3\,200\,000 - 320\,000}{200000} = 1{,}44$$

Заключение

В результате выполнения курсового проекта была достигнута цель: снижение рисков информационной безопасности зала для конфиденциальных переговоров ОГУ с помощью метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадров. Для достижения цели решены следующие задачи:

- Обоснована актуальность разработки метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадров;
- Проведен обзор современной научной литературы по разработке метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадров;
- Разработана классификация систем видеонаблюдения;
- Разработаны модель угроз и нарушителя для объекта защиты;
- Разработано технико-экономическое обоснование на разработку метода управления адаптивной системой защитного видеонаблюдения на основе контроля динамики изменения кадров;

Список использованных источников

1. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). [Электронный ресурс]. – Режим доступа: http://www.fstec.ru
2. Физические средства защиты объектов информатизации: методические указания к лабораторным работам/ Е.В. Бурькова;–Оренбургский гос. ун-т. –Оренбург: ОГУ, 2012. –54с.
3. Р78.36.002-99 ГУВО МВД России. Выбор и применение телевизионных систем видеоконтроля. Рекомендации.
4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Руководящий документ ФСТЭК России 14.02.2008 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380.
5. Постановление Правительства от 25 марта 2015 г. N 272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии российской федерации, и форм паспортов безопасности таких мест и объектов (территорий).
6. Р 78.36.032-2013 ГУВО МВД России. Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1. Методические рекомендации.
7. Модернизация системы физической защиты промышленного объекта. [Электронный ресурс]. – Режим доступа:https://www.secuteck.ru/articles/modernizaciya-sistemy-fizicheskoj-zashchity-promyshlennogo-obekta
8. ГОСТ Р ИСО/МЭК 17799-2005. Практические правила управления информационной безопасностью.
9. Кутузов Д.В., Белозеров В.Н., Ларченко Р.О. Методы оценки рисков, связанных с нарушением информационной безопасности предприятия. // «Прикаспийский журнал: управление и высокие технологии», № 1, 2010 г. – С. 19-25.
10. ГОСТ Р 51558-2000 Системы охранные телевизионные. Общие технические требования и методы испытаний.
11. Видеонаблюдение (мировой рынок). – Режим доступа: https://www.tadviser.ru/index.php/Статья:Видеонаблюдение_(мировой_рынок)
12. 10 глобальных трендов видеонаблюдения 2014–2020. – Режим доступа: http://secuteck.ru/articles2/videonabl/globalnyh-trendov-videonablyudeniya
13. Мешкова Е.В. Проектирование системы видеонаблюдения на объекте информатизации // Контентус. 2016. №1 (42). URL: https://cyberleninka.ru/article/n/proektirovanie-sistemy-videonablyudeniya-na-obekte-informatizatsii (дата обращения: 04.03.2021).
14. Рылов К.А. Видеоаналитика, системы и их сравнение // ТУСУР, – Томск. 2016, 4с. URL: https://storage.tusur.ru/files/11036/ТУ-1203 (дата обращения: 04.03.2021).
15. Калита А.О. Основы организации адаптивных систем защиты информации // NBI-technologies. 2019. №1. URL: https://cyberleninka.ru/article/n/osnovy-organizatsii-adaptivnyh-sistem-zaschity-informatsii (дата обращения: 04.03.2021).
16. Жмурко Д.Ю. Понятие, сущность и классификация адаптивного управления системами с организационной сложностью // Научный журнал КубГАУ. 2013. №90. URL: https://cyberleninka.ru/article/n/ponyatie-suschnost-i-klassifikatsiya-adaptivnogo-upravleniya-sistemami-s-organizatsionnoy-slozhnostyu (дата обращения: 04.03.2021).
17. Белозёрова Ангелина Андреевна, Мартынова Лариса Евгеньевна, Ковалев Станислав Андреевич, Назарова Кристина Евгеньевна, Кожевникова Ирина Сергеевна, Ананьин Евгений Викторович, Попков Сергей Михайлович, Лысенко Александр Вячеславович Угрозы систем видеонаблюдения // Вестник науки и образования. 2017. №1 (25). URL: https://cyberleninka.ru/article/n/ugrozy-sistem-videonablyudeniya (дата обращения: 04.03.2021).
18. Нокеева Роза Манаповна Исследование оптимальных методов и алгоритмов обнаружения движущихся объектов в видеопотоке // Научные исследования. 2018. №6 (25). URL: https://cyberleninka.ru/article/n/issledovanie-optimalnyh-metodov-i-algoritmov-obnaruzheniya-dvizhuschihsya-obektov-v-videopotoke (дата обращения: 04.03.2021).