Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

РАБОТА ПРОВЕРЕНА
Рецензент, начальник отдела ИБ
ООО «ЧТЗ – Уралтрак»
_____ В.В. Соболев
_____ 2018 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к. т. н., доцент
_____ А.Н. Соколов
_____ 2018 г.

Математическое моделирование и оценка угроз физического доступа к объекту критической информационной инфраструктуры ООО «ЧТЗ – Уралтрак»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ–10.05.05.2018.527 ПЗ ВКР

Консультанты:

Безопасность жизнедеятельности,
к. т. н., доцент
_____ Н.В. Глотова
_____ 2018 г.

Руководитель работы,
доцент
_____В.Ю. Бердюгин
_____ 2018 г.

Автор работы,
студент группы КЭ-532
_____ В.В. Царенко
_____ 2018 г.

Нормоконтролер,
к. т. н., доцент
_____В.П. Мартынов
_____ 2018 г.

Челябинск 2018

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

Специальность 10.05.05 «Безопасность информационных технологий
в правоохранительной сфере»

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Н. Соколов
_____ 2018 г.

З А Д А Н И Е
на выпускную квалификационную работу студента

Царенко Василия Владимировича

Группа КЭ-532

1 Тема работы

Математическое моделирование и оценка угроз физического доступа к объекту критической информационной инфраструктуры ООО «ЧТЗ – Уралтрак»

Утверждена приказом ректора ЮУрГУ от 4 апреля 2018 г. № 580
(утверждена, протокол заседания кафедры от 15 марта 2018 г. № 7)

2 Срок сдачи студентом законченной работы 27 мая 2018 г.

3 Исходные данные к работе

Отчет о преддипломной практике, нормативные правовые документы в области защиты информации, документация предприятия

4 Содержание расчетно-пояснительной записки

4.1 Концепция инженерно-технической защиты информации.
4.2. Инженерно-техническое обеспечение систем физической защиты.
4.3. Моделирование и оценка угроз физического доступа.

5 Перечень графического материала

Презентация к выпускной квалификационной работе на тему:
«Математическое моделирование и оценка угроз физического доступа
к объекту критической информационной инфраструктуры
ООО «ЧТЗ – Уралтрак»

Всего _____ листов

6 Консультанты по работе, с указанием относящихся к ним разделов работы

Раздел	Консультант	Подпись, дата	
		Задание выдал (консультант)	Задание принял (студент)
Безопасность жизнедеятельности	Н.В. Глотова		

7 Дата выдачи задания 25 января 2018 г.

Руководитель,
доцент _____ В.Ю. Бердюгин

Задание принял к исполнению _____ В.В. Царенко

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы	Срок выполнения этапов работы	Отметка о выполнении руководителя
Введение		
Концепция инженерно-технической защиты информации		
Инженерно-техническое обеспечение систем физической защиты		
Моделирование и оценка угроз физического доступа		
Безопасность жизнедеятельности		
Заключение		
Библиографический список		
Предзащита ВКР		
Защита ВКР		

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ В.Ю. Бердюгин

Студент _____ В.В. Царенко

АННОТАЦИЯ

Царенко, В.В. Математическое моделирование и оценка угроз физического доступа к объекту критической информационной инфраструктуры ООО «ЧТЗ – Уралтрак». – Челябинск: ЮУрГУ, ВШ ЭКН, КЭ-532, 2018, 91 с., 4 ил., 3 табл., библиогр. список – 22 наименования, 9 прил.

В первой главе внимание уделено рассмотрению самой концепции инженерно-технической информации, сформулированы основные положения, а также цели и задачи, которые должна решать эффективная система инженерно-технической защиты информации. Уделено внимание основным принципам защиты, а также принципам построения эффективной системы.

Во второй главе внимание уделено рассмотрению целей функционирования систем физической защиты с выделением и классификацией угроз подсистем обнаружения. Рассмотрены особенности построения периметровой охраны и использования инженерно-технических систем и технических средств охраны для увеличения задержки времени проникновения злоумышленника, и тем самым увеличения времени для его обнаружения.

В третьей главе работы на базе системы компьютерной алгебры Wolfram Mathematica создано представление в виде графа исследуемой территории, сопровождающееся весовыми коэффициентами, позволяющими вести расчет возможных маршрутов злоумышленника. Для каждой точки возможного исхода злоумышленника найдены наиболее оптимальные пути подхода к объекту защиты, вычислены соответствующие им вероятности успеха. Для полученного множества оптимальных для злоумышленника путей выявлена общая составляющая маршрута. Данное позволяет обозначить направление, представляющее наибольшую угрозу для объекта защиты с точки зрения реализации угроз физического доступа и сделать акцент на контроле соответствующего участка выявленных маршрутов с целью пресечения и/или минимизации угроз физического доступа со стороны злоумышленника в текущей обстановке.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современном мире информационные системы (ИС) входят в состав большинства предприятий и организаций функционирующих в разных сферах деятельности. Среди них объекты критической информационной инфраструктуры (КИИ). Согласно Федеральному закону от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» под «объектами критической информационной инфраструктуры понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры». В свою очередь «субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей». Таким субъектом, по определению, является организация ООО «ЧТЗ – Уралтрак», входящее в структуру оборонно-промышленного комплекса Российской Федерации.

В последнее время важность и актуальность защиты КИИ и составляющих ее объектов подтверждается пристальным вниманием к ней со стороны Российского правительства.

Среди всех угроз, направленных на ИС можно выделить угрозы, связанные с возможностью физического проникновения на объект, с целью несанкционированного доступа к защищаемой информации и техническим средствам объекта защиты. Средствами противодействия угрозам такого рода являются системы физической защиты (СФЗ). СФЗ представляют собой объединение сил охраны и технического оснащения – комплекса инженерно-технических средств охраны. Проектирование СФЗ – это сложный процесс. Если при проектировании допускаются ошибки, то полученная система, либо не сможет противодействовать угрозам, либо превысит необходимый уровень защищенности для объекта информатизации и затраты на ее создание и обслуживание будут необоснованно высоки.

Несмотря на широкое развитие и распространение систем физической защиты (СФЗ) для различных категорий объектов, очень часто их разработка осуществляется без привлечения соответствующих теоретических научных результатов, что в конечном итоге может привести к нарушению безопасности охраняемых объектов. Ошибки разработчиков могут привести к серьезным последствиям для КИИ как таковой. Таким образом необходимо развивать инструментальные средства

экспертной поддержки принятия решений в задачах разработки и оценки СФЗ. Данный момент находит отражение, в частности, в диссертациях А.С. Боровских [3] и А.Д. Тарасова [4].

Теоретические основы построения оптимальных технических систем, к которым относится и СФЗ, крайне сложны и, несмотря на интенсивные исследования в данной области, далеки от совершенства.

В связи с тем, что процесс разработки и оценки СФЗ ИС требует знания экспертов, которые отражают неопределенность, неточность, неполноту, неоднозначность данной предметной области исследования, то и вопросы, касающиеся информационной поддержки принятия решений, в задачах разработки и оценки СФЗ объектов в условиях неопределенности остаются малоисследованными. Необходимость в таких оценках возникает при анализе защищенности ИС от угроз с целью выработки как стратегических, так и тактических решений при организации его защиты.

Объектом данной работы является СФЗ ООО «ЧТЗ – Уралтрак».

Предметом – моделирование угроз физического доступа, реализуемых внешним нарушителем, к объекту защиты.

Цель работы – выявление наиболее вероятных путей реализации угроз физического доступа к объекту защиты и их оценка.

1 КОНЦЕПЦИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Концепция – это система взглядов на что-либо. Если речь идет об инженерно-технической защите информации, то ее концепция – это система взглядов на защиту информации с помощью инженерных и технических средств.

Необходимыми условиями успешного решения любой задачи, в том числе и инженерно-технической защиты информации, являются постановка задачи и определение принципов ее решения. Содержание этих двух условий составляют основу концепции инженерно-технической защиты информации.

Задачи инженерно-технической защиты представляют собой задачи противоборства органов и специалистов по информационной безопасности, с одной стороны, и злоумышленников, с другой стороны. Под злоумышленниками в дальнейшем понимаются органы и сотрудники зарубежных спецслужб, конкуренты, криминал и любые другие люди, которые незаконным путем пытаются добыть, изменить или уничтожить информацию законных владельцев или пользователей.

1.1 Системный подход к инженерно-технической защите информации

1.1.1 Основные положения системного подхода к инженерно-технической защите информации

Слабоформализуемые задачи, к которым относится большинство задач инженерно-технической защиты, характеризуются следующими основными особенностями:

– наличием большого числа факторов, влияющих на эффективность решения задачи;

– отсутствием количественных достоверных исходных данных об этих факторах;

– отсутствием формальных (математических) методов получения оптимальных результатов решения слабоформализованных задач по совокупности исходных данных.

Эти особенности исключают возможность формального получения оптимального (наилучшего) результата решения задачи. Но даже формальный аппарат при недостоверных исходных данных не гарантирует получение точного результата.

Слабоформализуемые задачи наиболее часто приходится решать на практике. Несмотря на огромные достижения науки, число проблем и задач, которые удается свести к формальным и решить строго математически, существенно меньше, чем не имеющих такого решения.

Слабоформализуемые задачи решаются в основном эвристическими методами. Однако эти методы не обеспечивают получение оптимального результата, а определяют область рациональных решений, т. е. тех, которые с определенными допусками соответствуют постановке задачи. Как правило, задача имеет несколько

рациональных решений, которые в пространстве результатов образуют область, внутри которой расположено оптимальное решение.

Эвристические методы реализуют на подсознательном уровне знания и опыт специалистов. Тем не менее эвристические методы решения слабоформализуемых задач часто обеспечивают более точные результаты, чем формальные на основе грубых математических моделей или при недостоверных и недостаточных исходных данных.

Однако возможности эвристических методов имеют ограничения, определяемые числом учитываемых при решении задачи факторов влияния. В силу этих же ограничений должностные лица, которым приходится оперативно решать многофакторные задачи, имеют помощников, которые готовят им информацию в сжатом систематизированном виде.

Если число факторов влияния велико, что имеет место при решении задач инженерно-технической защиты информации, то точность эвристических методов низка. В общем случае задачи инженерно-технической защиты информации характеризуются большим количеством и многообразием факторов, влияющих на результат решения, причем это влияние часто не удается однозначно выявить и строго описать. К ним, в первую очередь, относятся задачи, результаты решения которых зависят от людей. Только в отдельных простейших случаях удается однозначно и формально описать реакции человека на внешние воздействия. В большинстве других вариантов сделать это не удается. Однако из этого утверждения не следует, что организация эффективной защиты информации зависит исключительно от искусства специалистов по защите информации. Человечеством накоплен достаточно большой опыт по решению слабоформализуемых проблем.

Решение любых задач производится на основе моделей исследуемых объектов и процессов. Решаемая задача или проблема представляет собой разницу между реальным объектом или процессом и тем, что надо достигнуть или получить. Наиболее универсальной моделью любого объекта или процесса является представление его в виде системы. Системный подход – это исследование объекта или процесса с помощью модели, называемой системой.

Этот подход предусматривает самый высокий уровень описания объекта исследования – системный. Самым низким уровнем является уровень описания параметров объекта – параметрический. Между ними располагаются структурный и функциональный уровни.

Сущность системного подхода состоит в следующем:

– совокупность сил и средств, обеспечивающих решение задачи, представляется в виде модели, называемой системой;

– система описывается совокупностью параметров;

– любая система рассматривается как подсистема более сложной системы, влияющей на структуру и функционирование рассматриваемой;

– любая система имеет иерархическую структуру, элементами и связями которой нельзя пренебрегать без достаточных оснований;

– при анализе системы необходим учет внешних и внутренних влияющих факторов, принятие решений на основе части из них без рассмотрения остальных может привести к неверным результатам;

– свойства системы превышают сумму свойств ее элементов за счет качественно новых свойств, отсутствующих у ее элементов – системных свойств.

Эффективность реализации системного подхода на практике зависит от умения специалиста выявлять и объективно анализировать все многообразие факторов и связей достаточно сложного объекта исследования, каким является, например, организация как объект защиты. Необходимым условием такого умения является наличие у специалиста так называемого системного мышления, формируемого в результате соответствующего обучения и практики решения слабоформализуемых задач. Системное мышление – важнейшее качество не только специалиста по защите информации, но и любого организатора и руководителя. Если руководитель не может быстро выявить факторы, влияющие на то или иное решение, и оценить их вес, то неучтенные или необоснованно отброшенные факторы постоянно будут о себе напоминать. Такой руководитель превращается в борца с им же создаваемыми проблемами. Системное мышление – это форма мышления, характеризующая способность человека на бессознательном уровне решать задачи дедуктивным методом. Эти методы применительно к инженерно-технической защите информации предусматривают:

– четкую постановку задачи, включающую определение тематических вопросов защищаемой информации и ее источников как объектов защиты, выявление угроз этой информации и формулирование целей и задач защиты информации;

– разработку принципов и путей решения задачи;

– разработку методов решения задач;

– создание программного, технического и методического обеспечения решения задачи.

Если системный поход характеризует концептуальные взгляды на пути решения слабоформализуемых задач, то основу их решения составляет системный анализ.

Системный анализ предусматривает применение комплекса методов, методик и процедур, позволяющих выработать в результате анализа модели системы рациональные рекомендации по решению проблем системы. Математическим обеспечением системного анализа является аппарат исследования операций. Исследование операций представляет собой комплекс научных методов для решения задач эффективного управления организационными системами, в которых основным элементом является человек. Один из создателей аппарата исследования операций Т. Саати определил его как «искусство давать плохие ответы на те практические вопросы, на которые даются еще худшие ответы другими методами». Следует сразу оговориться, что при решении слабоформализуемых задач методами системного анализа в большинстве случаев удается найти только область рацио-

нальных решений, внутри которой находится наилучший (оптимальный) для конкретных исходных данных результат.

В соответствии с требованиями системного подхода совокупность взаимосвязанных элементов, функционирование которых направлено на обеспечение безопасности информации, образует систему защиты информации. Такими элементами являются люди, инженерные конструкции и технические средства, обеспечивающие защиту информации независимо от их принадлежности к другим системам. Ядро системы защиты образуют силы и средства, основными функциями которых является обеспечение информационной безопасности. Однако они составляют лишь часть сил и средств системы защиты информации. Следовательно, структура (элементы и их взаимосвязь) системы защиты информации государства, ведомства, организации пронизывает структуру государства, ведомства, организации.

1.1.2 Цели, задачи и ресурсы системы защиты информации

Формулирование целей и задач защиты информации представляет начальный и значимый этап обеспечения безопасности информации.

Цели защиты информации сформулированы в ст. 16 Закона РФ «Об информации, информационных технологиях и о защите информации»:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

В общем виде цель защиты информации определяется как обеспечение безопасности информации, содержащей государственную или иные тайны.

Для системы защиты информации очень трудно точно указать места входов и выходов. Входами любой системы являются силы и воздействия, изменяющие состояние системы. Такими силами и воздействиями являются угрозы. Угрозы могут быть внутренними и внешними, в том числе такие трудно локализуемые как слабая правовая дисциплина сотрудников, некачественная эксплуатация средств

обработки информации или наличие в помещении радио и электрических приборов, побочные физические процессы в которых способствуют несанкционированному распространению защищаемой информации. Источниками угроз могут быть злоумышленники, технические средства внутри организации, сотрудники организации, внутренние и внешние поля, стихийные силы и т. д.

Выходы системы представляют собой реакцию системы на входы. Выходами системы являются меры по защите информации. Однако локализовать в пространстве выходы системы так же сложно, как и входы. Каждый сотрудник, например, в меру своей ответственности обязан заниматься задачами защиты информации и принимать меры по обеспечению ее безопасности. Меры по защите информации также включают разнообразные способы и средства, в том числе документы, определяющие доступ сотрудников к защищаемой информации в конкретном структурном подразделении организации.

Следовательно, система защиты информации представляет собой модель системы, объединяющей силы и средства организации, обеспечивающие защиту информации. Она описывается параметрами на рис. 1.

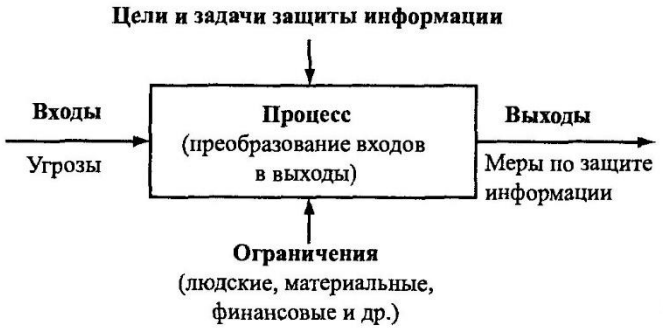


Рисунок 1 – Параметры системы защиты информации

К параметрам системы относятся:

– цели и задачи (конкретизированные в пространстве и во времени цели);

– входы и выходы системы;

– ограничения, которые необходимо учитывать при построении (модернизации, оптимизации) системы;

– процессы внутри системы, обеспечивающие преобразование входов в выходы.

Цели представляют собой ожидаемые результаты функционирования системы защиты информации, а задачи то, что надо сделать для того, чтобы система могла обеспечить достижение поставленных целей. Возможность решения задач зависит от ресурса, выделяемого на защиту информации. Ресурс включает в себя людей, решающих задачи защиты информации, финансовые, технические и другие средства, расходуемые на защиту информации. Входами системы защиты информации являются угрозы информации, а выходами – меры, которые надо применить для предотвращения угроз или снизив их до допустимого уровня. Наконец, мероприя-

тия, действия и технологии, определяющие меры защиты, соответствующие угрозам, образуют процесс.

Угроза может быть реализована с различной вероятностью. Вероятность реализации угрозы безопасности информации определяет риск ее владельца.

Риск владельца информации зависит от уровня инженерно-технической защиты информации, который, в свою очередь, определяется ресурсами системы. Ресурс может быть определен в виде количества людей, привлекаемых к защите информации, в виде инженерных конструкций и технических средств, применяемых для защиты, денежных сумм для оплаты труда людей, строительства, разработки и покупки технических средств, их эксплуатационных и других расходов.

Чем больше ресурс на защиту информации, тем более высокий уровень безопасности информации может он обеспечить. В принципе, при неограниченном ресурсе можно получить сколь угодно малую вероятность реализации угрозы.

Задачи инженерно-технической защиты, как любые иные задачи – четкое и конкретное описание того, что надо сделать для достижения цели. Сформулировать задачи можно только тогда, когда определена защищаемая информация и угрозы ей. В постановке задачи указывается необходимость определения рациональных мер для конкретной защищаемой информации и угрозы ей с учетом имеющегося ресурса.

1.2 Основные положения концепции инженерно-технической защиты информации

Основные положения концепции инженерно-технической защиты информации определяют ее принципы, которые конкретизируются в методах, способах и средствах инженерно-технической защиты информации. Если цель отвечает на вопрос, что надо достичь в результате инженерно-технической защиты информации, а задачи – что надо сделать для этого, то принципы дают общее представление о подходах к решению поставленных задач. Принципы можно разделить на принципы инженерно-технической защиты информации как процесса и принципы построения системы инженерно-технической защиты информации.

1.2.1 Принципы инженерно-технической защиты информации

Любая технология, в том числе защиты информации, должна соответствовать набору определенных общих требований, которые можно рассматривать как общие принципы защиты информации. К ним относятся:

– надежность защиты информации;
– непрерывность защиты информации;
– скрытность защиты информации;
– целеустремленность защиты информации;
– рациональность защиты;
– активность защиты информации;

– гибкость защиты информации;

– многообразие способов защиты;

– комплексное использование различных способов и средств защиты информации;

– экономичность защиты информации.

Надежность защиты информации предусматривает обеспечение требуемого уровня ее безопасности независимо от внешних и внутренних факторов, влияющих на безопасность информации. При рациональной защите на ее уровень не должны влиять как преднамеренные действия злоумышленника, например выключение электропитания, так и стихийные силы, например пожар.

Непрерывность защиты информации характеризует постоянную готовность системы защиты к отражению угроз информации. Так как место и время угрозы информации априори неизвестны, то в инженерно-технической защите не может быть перерывов в работе, в том числе в ночное время.

Затраты на изменения системы защиты минимизируются в случае скрытности защиты информации. Чем выше скрытность, тем больше неопределенность исходных данных у злоумышленника и тем меньше у него возможностей по добыванию информации. Скрытность защиты информации достигается скрытным (тайным) проведением мер по защите информации и существенным ограничением допуска сотрудников организации (предприятия, учреждения) к информации о конкретных способах и средствах инженерно-технической защиты информации в организации.

Так как ресурса на нейтрализацию всех угроз, как правило, не хватает, то целеустремленность защиты информации предусматривает сосредоточение усилий по предотвращению угроз наиболее ценной информации.

Инженерно-техническая защита информации должна быть рациональной, которая предполагает минимизацию ресурса, расходуемого на обеспечение необходимого уровня безопасности информации.

Недостоверность и недостаточность информации об угрозах информации могут быть в какой-то степени компенсированы ее поиском. Необходимым условием эффективной защиты информации является ее активность, которая обеспечивается, прежде всего, прогнозированием угроз и созданием превентивных мер по их нейтрализации.

Добывание и защита информации – это процесс борьбы противоположных сил. Учитывая, что основным источником угроз является человек – злоумышленник, победа в ней возможна при гибкости защиты информации. Необходимость ее обусловлена, прежде всего, свойством информации к растеканию в пространстве. Со временем все больше деталей системы защиты становятся известны большему числу сотрудников и, следовательно, будут более доступными и злоумышленнику. Гибкость защиты предполагает возможность оперативно изменять меры защиты, особенно в случае, если принимаемые меры станут известны злоумышленнику. Гибкость защиты информации можно обеспечить, если система имеет набор разнообразных мер защиты, из которого можно оперативно выбрать эффективные

для конкретных угроз и условий. Гибкость обеспечивается многообразием способов и средств инженерно-технической защиты информации.

Так как нет универсальных методов и средств защиты информации, то существует необходимость в их таком комплексном применении, при котором недостатки одних компенсируются достоинствами других.

Защита информации должна быть экономичной. Это значит, что затраты на защиту информации не должны превышать возможный ущерб от реализации угроз.

Рассмотренные общие принципы инженерно-технической защиты информации не дают конкретных рекомендаций по инженерно-технической защите информации. Однако они ориентируют специалиста на требования, которым должна соответствовать инженерно-техническая защита информации.

1.2.2 Принципы построения системы инженерно-технической защиты информации

Система защиты информации должна содержать:

– рубежи вокруг источников информации, преграждающих распространение сил воздействия к источникам информации и ее носителей от источников;

– силы и средства достоверного прогнозирования и обнаружения угроз;

– механизм принятия решения о мерах по предотвращению или нейтрализации угроз;

– силы и средства нейтрализации угроз, преодолевших рубежи защиты.

Основу построения такой системы составляют следующие принципы:

– многозональность пространства, контролируемого системой инженерно-технической защиты информации;

– многорубежность системы инженерно-технической защиты информации;

– равнопрочность рубежа контролируемой зоны;

– надежность технических средств системы защиты информации;

– ограниченный контролируемый доступ к элементам системы защиты информации;

– адаптируемость (приспособляемость) системы к новым угрозам;

– согласованность системы защиты информации с другими системами организации.

Многозональность защиты предусматривает разделение (территории государства, организации, здания) на отдельные контролируемые зоны, в каждой из которых обеспечивается уровень безопасности, соответствующий цене находящейся там информации. Уровень безопасности в любой зоне должен соответствовать максимальной цене находящейся в ней информации. Если в ней одновременно размещены источники информации с меньшей ценой, то для этой информации уровень безопасности, а следовательно, затраты будут избыточными. Так как уровень безопасности в каждой зоне определяется исходя из цены находящейся в ней

информации, то многозональность позволяет уменьшить расходы на инженерно-техническую защиту информации. Чем больше зон, тем более рационально используется ресурс системы, но при этом усложняется организация защиты информации. Зоны могут быть независимыми, пересекающимися и вложенными (рис. 2).

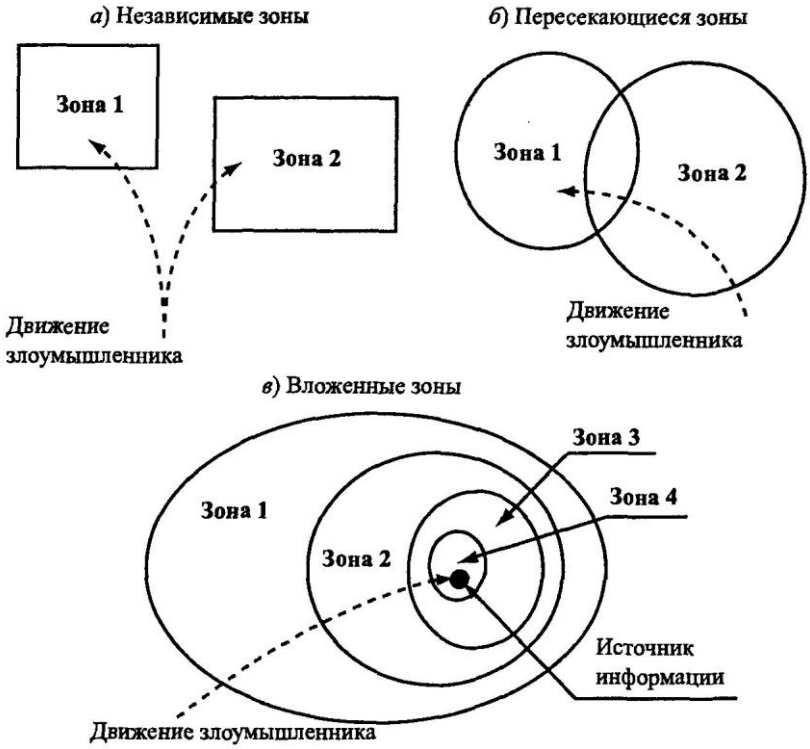


Рисунок 2 – Виды контролируемых зон

Для независимых зон уровень безопасности информации в одной зоне не зависит от уровня безопасности в другой. Они создаются для разделения зданий и помещений, в которых выполняются существенно отличающиеся по содержанию и доступу работы. Например, администрация организации размещается в одном здании, научно-исследовательские лаборатории – в другом, а производственные подразделения – в третьем.

Примером пересекающихся зон является приемная руководителя организации, которая, с одной стороны, принадлежит зоне с повышенными требованиями к безопасности информации, источниками которой являются руководящий состав организации и соответствующие документы в кабинете, а с другой стороны, в приемную имеют доступ все сотрудники и посетители организации. Требования к безопасности информации в пересекающейся зоне являются промежуточными между требованиями к безопасности в пересекающихся зонах. Например, уровень безопасности в приемной должен быть выше, чем в коридоре, но его нельзя практически обеспечить на уровне безопасности информации в кабинете.

Вложенные зоны наиболее распространены, так как позволяют экономнее обеспечивать требуемый уровень безопасности информации. Безопасность ин-

формации i-й вложенной зоны определяется не только ее уровнем защиты, но и уровнями защиты в предшествующих зонах, которые должен преодолеть злоумышленник для проникновения в i-ю зону.

Каждая зона характеризуется уровнем безопасности находящейся в ней информации. Безопасность информации в зоне зависит от:

– расстояния от источника информации (сигнала) до злоумышленника или его средства добывания информации;

– количества и уровня защиты рубежей на пути движения злоумышленника или распространения иного носителя информации (например, поля);

– эффективности способов и средств управления допуском людей и автотранспорта в зону;

– мер по защите информации внутри зоны.

Чем больше удаленность источника информации от места нахождения злоумышленника или его средства добывания и чем больше рубежей защиты, тем большее время движения злоумышленника к источнику и ослабление энергии носителя в виде поля или электрического тока. Количество и пространственное расположение зон и рубежей выбираются таким образом, чтобы обеспечить требуемый уровень безопасности защищаемой информации как от внешних (находящихся вне территории организации), так и внутренних (проникших на территорию злоумышленников и сотрудников). Чем более ценной является защищаемая информация, тем большим количеством рубежей и зон целесообразно окружать ее источник и тем сложнее злоумышленнику обеспечить разведывательный контакт с ее носителями. Вариант классификация зон по условиям доступа приведен в табл. 1.

Таблица 1 – Классификация зон по уровням доступа

Категория зоны	Наименование зоны	Функциональное значение зоны	Условия доступа сотрудников	Условия доступа посетителей
1	2	3	4	5
0	Свободная	Места свободного посещения	Свободный	Свободный
I	Наблюдаемая	Комнаты приема посетителей	Свободный	Свободный
II	Регистрационная	Кабинеты сотрудников	Свободный	По удостоверению личности с регистрацией
III	Режимная	Секретариат, компьютерные залы, архивы	По идентификационным картам	По разовым пропускам

Продолжение таблицы 1

1	2	3	4	5
IV	Усиленной защиты	Кассовые операционные залы, материальные склады	По спецдокументам	По спецпропускам
V	Высшей защиты	Кабинеты высших руководителей, комнаты для ведения переговоров, специальные хранилища	По спецдокументам	По спецпропускам

Из анализа этой таблицы следует, что по мере увеличения категории зоны усложняются условия допуска как сотрудников, так и посетителей.

На границах зон и особо опасных направлений создаются рубежи защиты. Очевидно, что чем больше рубежей защиты и чем они надежнее (прочнее), чем больше времени и ресурса надо потратить злоумышленнику или стихийным силам на их преодоления. Рубежи защиты создаются и внутри зоны на пути возможного движения злоумышленника или распространения иных носителей, прежде всего, электромагнитных и акустических полей. Например, для защиты акустической информации от подслушивания в помещении может быть установлен рубеж защиты в виде акустического экрана.

Типовыми зонами организации, указанными на рис. 3, являются:

– территория, занимаемая организацией и ограничиваемая забором или условной внешней границей;

– здание на территории;

– коридор или его часть;

– помещение (служебное, кабинет, комната, зал, техническое помещение, склад и др.);

– шкаф, сейф, хранилище.

Соответственно, рубежи защиты:

– забор;

– стены, двери, окна здания;

– двери, окна (если они имеются), стены, пол и потолок (перекрытия) коридора;

– двери, окна, стены, пол и потолок (перекрытия) помещения;

– стены и двери шкафов, сейфов, хранилищ.

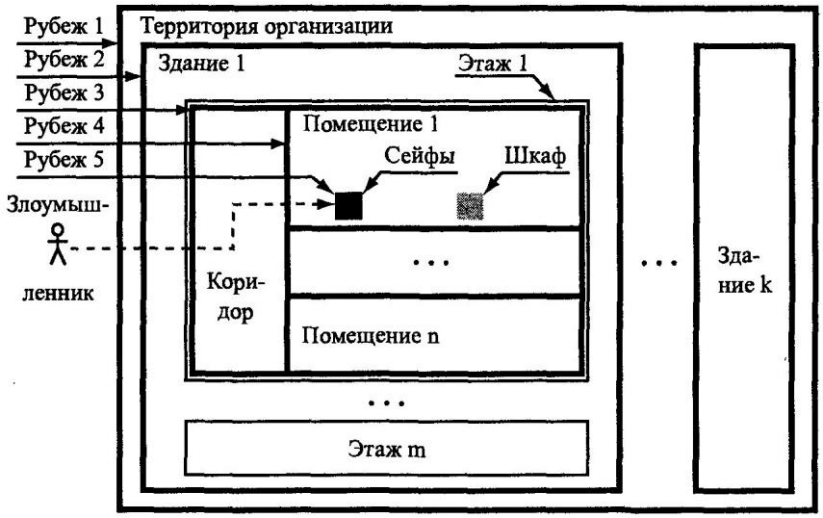


Рисунок 3 – Типовые зоны и рубежи организации

Необходимым условием и принципом эффективной инженерно-технической защиты информации является равнопрочность рубежа контролируемой зоны. Наличие бреши в защите может свести на нет все затраты. Выполнение принципа равнопрочности рубежа требует выявления и анализа всех потенциальных угроз с последующей нейтрализацией угроз с уровнем выше допустимого.

Непрерывность защиты информации может быть обеспечена при условии безотказной работы сил и средств системы защиты. Надежность любого технического средства всегда ниже 100%. Поэтому через некоторое время, усредненное значение которого называется временем безотказной работы, в нем возникает неисправность. Ущерб от неисправности технических средств защиты может быть очень высокий, равный цене информации. Если техническое средство охраны своевременно не среагирует на угрозу, например пожара в помещении ночью, то за время, когда его обнаружит дежурная смена в другом конце здания или посторонние лица за забором, могут сгореть все документы, находящиеся в этом помещении. Ложные срабатывания средств защиты при отсутствии угроз менее опасны, но они способствуют формированию у охраны психологической установки на то, что причиной срабатывания средства защиты является его неисправность. Такая установка увеличивает время реакции сотрудника охраны на угрозу. Этим пользуются иногда преступники, которые перед проникновением в контролируемую зону вызывают многократные срабатывания средств защиты, в результате которых сотрудники охраны перестают на них реагировать. Поэтому к надежности технических средств защиты предъявляются повышенные, по сравнению с другими средствами, требования, а сами средства многократно дублируются. Например, в помещении устанавливается, как правило, несколько датчиков (извещателей) пожарной сигнализации.

Необходимым условием обеспечения скрытности защиты информации является жесткий контроль и управление допуском к элементам системы защиты, в том числе к ее техническим средствам. Выполнение этого принципа построения си-

стемы защиты требует скрытности и дополнительной укрепленности мест размещения технических средств защиты информации.

Гибкость защиты информации обеспечивается адаптируемостью системы к новым угрозам и изменением условий ее функционирования. Для оперативной адаптации необходимы механизмы быстрого изменения структуры системы и резерв ее сил и средств.

Система защиты информации функционирует совместно с другими системами государства и организации любого уровня. Поэтому она должна функционировать согласованно с другими системами. В противном случае эти системы будут мешать друг другу. Следовательно, необходимы иные решения по обеспечению безопасности информации, существенно не затрудняющие работу организации по иным видам деятельности. Конечно, меры по защите информации в той или иной степени ужесточают режим организации, но чем незаметнее система защиты информации решает свои задачи, тем более она рациональна. Следовательно, рационально построенная система инженерно-технической защиты информации должна минимизировать дополнительные задачи и требования, вызванные мерами по защите информации, к сотрудникам организации.

Чем более универсальной является любая система, тем она менее эффективно решает конкретные задачи по сравнению с узко специализированной системой. «Плату» за универсальность можно снизить введением в систему механизма адаптации ее конфигурации и алгоритма функционирования ее к изменившимся условиям.

Адаптируемость системы защиты информации достигается прогнозированием угроз и заложенной при ее создании возможности производить без капитальных вложений изменения элементов как физической защиты, так и скрытия источников информации.

Кроме защиты информации в любой организации решается множество других задач по безопасности сотрудников не только на рабочем месте, но и в иных местах, по защите материальных ценностей, размещенных в разных местах ее территории (во дворе, на складах, в помещениях и др.). Поэтому наряду с системой защиты информации в организации создаются и иные системы. Автономное их функционирование распыляет средства, что в условиях их ограниченности снижает эффективность любой из этих систем.

1.3 Выводы по первой главе

1. Инженерно-техническая защита информации является одним из основных направлений обеспечения информационной безопасности. Технический прогресс способствует повышению роли инженерно-технической защиты. Она охватывает большое количество областей знаний и сфер практической деятельности, при ее обеспечении необходимо учитывать большое число факторов, информация о которых недостаточная и часто недостоверная. Определяющую роль при инженерно-технической защите играет человек, действия которого пока не поддаются

формализации. Задачи инженерно-технической защиты информации относятся к так называемым слабоформализуемым задачам, не имеющим формальных (строго математических) методов решения. Получение рациональных (удовлетворяющих поставленным требованиям) результатов при решении слабоформализуемых задач достигается на основе системного подхода.

2. Отсутствие формального математического аппарата оптимизации решения слабоформализуемых задач не позволяет находить оптимальные решения. Результаты решения, удовлетворяющие требованиям, образуют область рациональных решений, внутри которых находится оптимальный результат.

Задачи защиты информации, как любые иные слабоформализуемые задачи, решаются путем выбора специалистом рациональных вариантов решения на основе результатов системного анализа. Рациональный вариант выбирается по значениям показателей эффективности защиты информации.

3. Основной целью инженерно-технической защиты информации является обеспечение ее безопасности, при которой риск изменения, уничтожения или хищения информации не превышает допустимого значения.

Задачи инженерно-технической защиты информации определяют то, что надо выполнить с учетом данного ресурса для предотвращения (нейтрализации) конкретных угроз в интересах поставленных целей.

4. Входы системы представляют собой угрозы безопасности информации. Угрозы проявляются в виде угроз преднамеренных и случайных (непреднамеренных) воздействий на источники информации и угроз утечки информации.

5. Выходы системы защиты информации – меры по обеспечению инженерно-технической защиты. Меры инженерно-технической защиты информации представляют собой совокупность технических средств и способов их использования, которые обеспечивают требуемый уровень безопасности информации при минимуме ресурса. Каждому набору угроз соответствует рациональный набор мер защиты. Определение такого набора является основной задачей инженерно-технической защиты информации. При отсутствии формальных методов определение набора средств задача решается путем выбора этих мер специалистами по локальным и глобальным показателям эффективности.

6. Основными принципами инженерно-технической защиты информации являются:

– надежность, предусматривающая обеспечение требуемого уровня безопасности защищаемой информации;

– непрерывность защиты во времени и пространстве, характеризующая постоянную (в любое время) готовность системы защиты к предотвращению (нейтрализации) угроз информации;

– активность, предусматривающая упреждающее предотвращение (нейтрализация) угроз;

– скрытность, исключающая возможность ознакомления лиц с информацией о конкретных способах и средствах защиты в рассматриваемой структуре в объеме, превышающем служебную необходимость;

– целеустремленность, предполагающая расходование ресурса на предотвращение угроз с максимальным потенциальным ущербом;

– рациональность, требующая минимизации расходования ресурса на обеспечение необходимого уровня безопасности информации;

– комплексное использование различных способов и средств защиты информации, позволяющее компенсировать недостатки одних способов и средств достоинствами других;

– экономичность защиты, предусматривающая, что расходы на защиту не превысят ущерба от реализации угроз.

7. К основным принципам построения инженерно-технической защиты информации относятся:

– многозональность пространства, контролируемого системой инженерно-технической защиты информации, позволяющая обеспечить согласование затрат на защиту и цены информации;

– многорубежность системы инженерно-технической защиты информации, увеличивающей время движения источников угроз и уменьшающей энергию сил воздействия и носителей информации при ее утечке;

– равнопрочность рубежей контролируемой зоны, исключающая появление в них «дырок», через которые возможно проникновение источников угроз и утечки информации;

– надежность технических средств системы защиты, обеспечивающая их постоянную работоспособность;

– ограниченный контролируемый доступ к элементам системы защиты информации, исключающий «растекание» информации о способах и средствах защиты;

– адаптируемость (приспосабливаемость) системы к новым угрозам и изменениям условий ее функционирования;

– согласованность системы защиты информации с другими системами, минимизирующая дополнительные задачи и требования к сотрудникам организации, вызванные необходимостью защиты информации.

2 ИНЖЕНЕРНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ

Как известно, что самый эффективный путь нейтрализации угроз безопасности – их предупреждение. При наличии соответствующих технических средств оно достигается их профессиональным обслуживанием.

Само наличие и вид трудно преодолеваемых разнообразных комбинированных средств физической защиты может заставить злоумышленника отложить проникновение или отказаться от него вообще. В этом случае время задержки системой злоумышленника возрастает до момента следующей попытки проникновения.

Максимально эффективная физическая защита источников информации должна обеспечивать:

– задержку злоумышленника или другого источника угрозы на время, большее времени необходимого для нейтрализации угрозы;

– обнаружение злоумышленника до момента проникновения в места хранения и обработки ценной информации или источника иной угрозы;

– нейтрализацию самих угроз воздействия на непосредственно источник информации.

Если злоумышленник решается на проникновение, то скорость его продвижения зависит от длины пути от места вторжения до места нахождения источника, количества и прочности механических препятствий на этом пути. И здесь возможны различные варианты обеспечения требуемого времени задержки путем комбинирования различных сочетаний количества рубежей (на границах зон) и их укрепленности. Одно и то же время задержки обеспечивается небольшим количеством хорошо укрепленных и большим количеством более слабо укрепленных рубежей. Рациональный вариант находится в результате минимизации стоимости.

С целью обеспечения увеличения времени задержки злоумышленника и уменьшения времени необходимого для нейтрализации угроз целесообразно принимать следующие меры:

– разнесение на максимально возможное расстояние от забора мест сосредоточения источников хранения наиболее ценной информации;

– размещение охранных постов, а также нахождение дежурной смены нахождения дежурной смены возле мест сосредоточения ценной информации;

– установка, создание дополнительных рубежей защиты на наиболее вероятных и менее поддающихся контролю путях движения злоумышленника к местам сосредоточения ценной информации;

– создание полос свободных от строений, растительности и мест складирования, хорошо просматриваемых по обе стороны от забора, и освещенных;

– установка заборов, дверей, окон, калиток соответствующей степени защищенности, а также ограничение доступа к люкам технических систем и подвалов.

2.1 Цели функционирования системы инженерно-технической защиты

Современная система защиты объекта – это комплекс, совокупность целенаправленных организационных, инженерно-технических, контрольных средств и мер, направленных на обеспечение полной, частичной или выборочной сохранности материальных ценностей, персонала и информации, находящихся на объекте.

Одним из основных направлений реализации указанных мер является противодействие угрозам безопасности объекта. Следовательно, данные меры направлены на выполнение задач, таких как: обнаружение, отражение и ликвидация различных угроз.

Следует отметить, что реализация выделенных задач невозможна без использования технических средств охраны (ТСО). Их применение направлено на достижение следующих целей:

1) предотвращение несанкционированного проникновения посторонних лиц на территорию и помещения объекта;

2) регулирование санкционированного доступа, обеспечение пропускного режима на территорию, в здания и помещения объекта;

3) предупреждение несанкционированного доступа к защищаемым ресурсам (человеческим, материальным, информационным) объекта;

4) предупреждение несанкционированного использования ресурсов объекта;

5) сигнализация о попытке несанкционированного действия;

6) регистрация сведений о попытках несанкционированных действий и о функционировании самой системы инженерно-технической защиты (СИТЗ);

7) отражение несанкционированных действий;

8) наблюдение, обнаружение, фиксация отклонений от нормальных условий, необходимых и достаточных для функционирования объекта;

9) контроль за системами, их сохранностью, ликвидация угроз безопасности объекту;

10) предупреждение возможных повреждений и нарушений безопасности объекту действиями персонала объекта.

Перечисленные цели представляются как функции, которые выполняют ТСО системы защиты объекта. Реализация этих функций зависит от характеристик защищаемого объекта.

В данном случае «объект» охраны представляет собой предприятие, учреждение или иную организацию, которая характеризуется следующими свойствами:

– наличие конкретных целей функционирования;

– наличие четко определенной организационно-штатной структуры;

– наличие четко определенной технологии функционирования;

– расположение на четко определенной и обозначенной территории;

– наличие системы информационного обеспечения деятельности;

– наличие системы информационного обмена внутри защищаемого объекта и с другими объектами;

– оснащение современными средствами сбора, накопления, хранения, обработки, выдачи, приема и передачи информации.

2.2 Подсистемы инженерно-технических средств обеспечения безопасности

В структуре инженерно-технических средств обеспечения безопасности можно выделить несколько основных подсистем.

Подсистема контроля и ограничения доступа персонала (владельцев, гостей и т. д.) объекта и посетителей в помещения и зоны защиты обеспечивает идентификацию человека по различным критериям (индивидуальные магнитные, кодовые и радио-карты; индивидуальные параметры человека) и содержит оперативную базу данных с расписанием доступа каждого человека. Для гарантии устойчивости подсистемы ее элементы функционируют как в комплексе, так и автономно.

Подсистема видеоконтроля позволяет на дистанции визуально следить за обстановкой в различных зонах объекта, достоверно поддерживает или опровергает факт совершения нарушения (любой внештатной ситуации), повышает устойчивость системы безопасности по отношению к сотрудникам самой службы безопасности в случае их противозаконных действий.

Подсистема охраной сигнализации обеспечивает автоматический контроль за целостностью границ зон охраны и за неизменностью состояния внутри каждой зоны, выдает сообщение о срабатывании конкретного датчика. Подсистема может содержать в одном шлейфе датчики, работающие на разных физических принципах, что позволяет повысить надежность системы. Подсистема также может периодически контролировать собственную работоспособность.

Подсистема пожарной сигнализации служит для надежного адресного оповещения службы безопасности о возникновении пожара и предпожарного состояния. Принципы ее построения аналогичны принципам устройства подсистемы охранной сигнализации.

Для достижения комплексности все составные элементы системы инженерно-технической защиты должны быть соединены в единый комплекс с возможностью взаимного обмена информацией. Состоящий из современного оборудования комплекс должен иметь в своем арсенале компьютер. С его помощью можно не только программно управлять СИТЗ, но и избавлять оператора от постоянного напряженного наблюдения за множеством мониторов, что, в свою очередь, уменьшает влияние человеческого фактора и тем самым обеспечивает объективность в оценке ситуации на объекте.

Чтобы решить проблему оптимизации выбора ТСО для конкретного объекта или его рубежа защиты, что может составить отдельный проект при проектировании системы инженерно-технической защиты, необходимо определить характеристики инженерно-технических средств охраны и провести их классификацию.

2.3 Классификация угроз подсистемы обнаружения

Можно выделить следующие классы угроз, обнаруживаемых подсистемой обнаружения:

– перемещение по охраняемой территории: движение нарушителя внутри и снаружи зданий;

– преодоление технических средств задержки, к которым относится все, что замедляет перемещение и действия нарушителя на объекте: забор, решетки, окна, двери, сейфы и др.;

– доступ нарушителя к объектам, защищаемым системой физической защиты (СФЗ) (документам, материальным ценностям, людям);

– угрозы, связанные с работой подсистемы обнаружения: действия нарушителя, связанные с обманом, обходом или нарушением функционирования подсистемы обнаружения.

Угрозы, связанные с работой подсистемы обнаружения проникновения нарушителя на объект, привязаны к конкретным ТСО и способу их установки. Выделяют следующие типы угроз, связанные с работой ТСО:

– обход – нарушитель реализует угрозу, для обнаружения которой предназначено ТСО, не попадая в зону обнаружения ТСО или не воздействуя на чувствительный элемент;

– обман – нарушитель реализует угрозу, для обнаружения которой предназначено ТСО, попадая в зону обнаружения ТСО или воздействуя на чувствительный элемент, но параметры воздействия нарушителя не входят в диапазон обнаружения ТСО;

– вывод из строя – нарушитель воздействует на ТСО так, что временно или постоянно ТСО перестает обнаруживать угрозы.

Угрозы, связанные с преодолением технических средств задержки (ТСЗ):

– преодоление ТСЗ – нарушитель преодолевает определенным способом средство задержки. ТСО обнаруживает нарушителя непосредственно в момент преодоления. Способы преодоления зависят от конкретного средства задержки;

– проникновение – нарушитель успешно преодолевает средство задержки. Например, нарушитель преодолевает ограждение и проникает на территорию объекта. В момент проникновения на территорию он может быть обнаружен ТСО, находящимся непосредственно за ТСЗ;

– приближение – нарушитель приближается к средству задержки. Расстояние от средства задержки, на котором будет обнаружен нарушитель, зависит от конкретного ТСО.

Следует отметить, что для того, чтобы преодолеть рубеж технических средств задержки, нарушитель обязательно должен осуществить угрозы приближения, преодоления и проникновения.

Угрозы доступа к объектам непосредственно реализуют риски, которые должно обнаруживать ТСО. Выделены следующие классы угроз:

– угрозы материальным ценностям, документам:

– приближение: нарушитель приближается к объекту. Расстояние от объекта, на котором будет обнаружен нарушитель, находится в зависимости от зоны обнаружения конкретного ТСО;

– перемещение: нарушитель перемещает объект.

– угрозы людям.

2.4 Обеспечение безопасности объектов

2.4.1 Особенности задач и общие принципы обеспечения безопасности

Особенности задач системы охраны объекта определяются также исходным положением нарушителя. Внешний нарушитель находится за территорией объекта, на котором недопустимо присутствие посторонних лиц.

Физические средства представляют собой первую линию защиты информации и элементов вычислительных систем, и поэтому обеспечение физической целостности таких систем и их устройств является непременным условием защищенности информации.

Основные задачи, решаемые физическими средствами:

1. Охрана территории.
2. Охрана оборудования и перемещаемых носителей информации.
3. Охрана внутренних помещений и наблюдение за ними.
4. Осуществление контролируемого доступа в контролируемые зоны.
5. Нейтрализация наводок и излучений.
6. Препятствия визуальному наблюдению.
7. Противопожарная защита.
8. Блокирование действий злоумышленника.

Территория по возможности должна быть окружена забором, а периметр здания иметь просматриваемую контролируемую зону. Наблюдение за контролируемой зоной может осуществляться различными телевизионными, радиолокационными, лазерными, оптическими, акустическими, кабельными и другими системами, а также системами различных датчиков, которые соединяются с центральным пультом, откуда подаются сигналы тревоги. Назначение заборов, решеток, ставней, экранов, специального остекления очевидно.

В помещении центрального пульта могут размещаться мониторы, наглядные схемы охраняемой территории с идентификацией места нарушения, а также ЭВМ, предназначенная для обработки сигналов от различных устройств управления, связанных с датчиками и другими системами охранной сигнализации, и других целей. ЭВМ поочередно опрашивает периферийные устройства управления.

В общем случае обеспечение безопасности объекта базируется на двух принципах:

1) определение и оценка угроз объекту;

2) разработка и реализация адекватных мер защиты.

Меры предусматривают:

– тотальный контроль несанкционированного проникновения на территорию объекта, в здания и помещения;

– ограничение и контроль доступа людей в «закрытые» здания и помещения с возможностью документирования результатов контроля;

– обнаружение злоумышленника на самых ранних этапах его продвижения к цели акции;

– оценку ситуации;

– создание на пути продвижения нарушителя физических препятствий, обеспечивающих задержку, необходимую силам охраны для его перехвата;

– принятие немедленных действий по развертыванию сил охраны и пресечению действий злоумышленников;

– видеодокументирование действий персонала на особо ответственных участках объекта.

Значительная роль в обеспечении реализации отмеченных мер отводится периметровым системам охраны.

2.4.2 Особенности построения периметровой охраны

Современные электронные системы охраны весьма разнообразны и в целом достаточно эффективны. Однако большинство из них имеют общий недостаток: они не всегда могут достоверно обеспечить раннее обнаружение вторжения на территорию объекта. Такие системы, как правило, ориентированы на обнаружение нарушителя, который уже проник на охраняемую территорию или в здание. Это касается, в частности, систем видеонаблюдения; они зачастую с помощью устройства видеозаписи лишь фиксируют факт вторжения после того, как он уже свершился. Опытный нарушитель всегда рассчитывает на определенное временное «окно», которое проходит от момента проникновения его на объект до момента обнаружения охранными средствами. Минимизация этого интервала времени является основным свойством, определяющим эффективность любой охранной системы, и в этом смысле преимущества периметровой охранной сигнализации неоспоримы.

Периметровая граница объекта является наилучшим местом для раннего обнаружения вторжения, так как нарушитель сталкивается прежде всего с физическим периметром и создает возмущения, которые можно зарегистрировать специальными датчиками. Если периметр представляет собой ограждение в виде металлической решетки, то ее приходится перерезать или преодолевать сверху; если это стена или барьер, то через них нужно перелезть; если это стена или крыша здания, то их нужно разрушить; если это открытая территория, то ее нужно пересечь.

Все это вызывает физическое взаимодействие нарушителя с периметром, который предоставляет хорошую возможность для электронного обнаружения, так как нарушитель создает определенный уровень вибраций, содержащих специфический звуковой «образ» вторжения.

При определенных условиях нарушитель может избежать физического контакта с периметром. В этом случае применяют «объемные» датчики вторжения, играющие роль вторичной линии защиты.

Датчик любой периметровой системы реагирует на появление нарушителя в зоне охраны или определенные действия нарушителя. Сигналы датчика анализируются электронным блоком (анализатором или процессором), который, в свою очередь, генерирует сигнал тревоги при превышении заданного порогового уровня активности в охраняемой зоне. Периметровый рубеж, проходящий по внешней границе территории объекта, первый и обязательный в системе охраны.

Периметровая система охраны должна отвечать определенному набору требований, часть из которых перечислена ниже:

1. Возможность раннего обнаружения нарушителя (еще до его проникновения на объект).
2. Точное следование контурам периметра, отсутствие «мертвых» зон.
3. По возможности скрытая установка датчиков системы.
4. Независимость параметров системы от сезона (зима, лето) и погодных условий (дождь, ветер, град и т. д.).
5. Невосприимчивость к внешним факторам «нетревожного» характера – индустриальные помехи, шум проходящего рядом транспорта, мелкие животные и птицы.
6. Устойчивость к электромагнитным помехам – грозовые разряды, источники мощных электромагнитных излучений и т. п.

Особенность периметровых систем состоит в том, что обычно они конструктивно интегрированы с ограждением и формируемые охранной системой сигналы в сильной степени зависят как от физико-механических характеристик ограды (материал, высота, жесткость и др.), так и от правильности монтажа датчиков (выбор места крепления, метод крепления, исключение случайных вибраций ограды и т. п.). Большое значение имеет правильный выбор типа охранной системы, наиболее полно отвечающей конкретному типу ограды.

Периметровые системы используют, как правило, систему распределенных или дискретных датчиков, общая протяженность которых может составлять несколько километров. Такая система должна обеспечивать высокую надежность при большом диапазоне изменения окружающей температуры и внешних условий (дождь, снег, сильный ветер). Поэтому любая система должна обладать свойством автоматической адаптации к погодным условиям и возможности дистанционной диагностики.

Периметровая система должна интегрироваться с другими охранными системами, в частности, с системой видеонаблюдения.

Периметровые средства охраны (СО) используются в тех случаях, когда:

– вокруг объекта нужно организовать четко регламентированную зону обеспечения возможности адекватного воздействия на злоумышленников для их обезвреживания на подступах к объекту охраны;

– необходимо четко очертить границы территории объекта, в том числе для повышения дисциплины и порядка на предприятии.

Обычно периметровые средства охраны используются совместно с ограждениями, которые обозначают границу территории объекта и тем самым создают вокруг него некую зону для обеспечения возможности адекватного воздействия на злоумышленника для его нейтрализации, т. е. обеспечивают юридическую правомерность действий охраны внутри огороженной территории.

В пользу необходимости сооружения периметровых сигнализационных рубежей объектов говорит следующий факт: отсутствие сигнализационных периметровых рубежей может привести к тому, что злоумышленник будет обнаружен несвоевременно и силам охраны просто не хватит времени для его нейтрализации. Кроме того, рубежи препятствуют несанкционированному выносу с объекта материальных ценностей.

При создании периметровой охраны объекта его внутренняя территория (охраняемая площадь) должна быть условно разделена на несколько функциональных зон: обнаружения, наблюдения, сдерживания, поражения, в которых располагаются соответствующие технические средства.

Зона обнаружения (ЗО) – зона, в которой непосредственно располагаются периметровые средства обнаружения, выполняющие автоматическое обнаружение нарушителя и выдачу сигнала «Тревога». Размеры зоны в поперечном сечении могут изменяться от нескольких сантиметров до нескольких метров.

Зона наблюдения (ЗН) – предназначена для слежения с помощью технических средств (телевидение, радиолокация и т. д.) за обстановкой на подступах к границам охраняемой зоны и в ее пространстве, начиная от рубежей.

Зона физического сдерживания (ЗФС) предназначена для задержания нарушителя при продвижении к цели или при побеге. Организуется с помощью инженерных заграждений, создающих физические препятствия перемещению злоумышленника. Инженерные заграждения представляют собой различные виды заборов, козырьков, спиралей из колючей ленты и проволоки, рвов, механических задерживающих преград и т. п. Во многих случаях ЗО и ЗФС совмещаются.

Зона средств физической нейтрализации и поражения (ЗНП) предназначена соответственно для нейтрализации и поражения злоумышленников.

2.5 Выводы

Очевидным кажется, что задачи охраны могут быть эффективно решены путем отдаления внешнего ограждения, поскольку в этом случае злоумышленнику потребуется больше времени для преодоления расстояния до цели и, соответственно, больше времени остается для действий сил охраны. Однако в этом случае удлиняется периметр объекта. Соответственно увеличиваются затраты на дорогостоящие технические средства и их эксплуатацию, а также необходимая численность сил охраны.

На практике в подавляющем числе случаев приходится иметь дело с уже существующим, а не с проектируемым объектом. Поэтому при построении СОБ в первую очередь ставится задача минимизации расходов на создание и эксплуатацию СО, ФБ и содержание персонала охраны при заданной эффективности защиты и особенностей (конфигурации, длины и т. д.) имеющегося периметра.

Зачастую более целесообразно использовать с этой целью периметровые СО, расположенные с внутренней стороны ограждения на максимально допустимом расстоянии от него. Такое расположение СО обеспечивает наилучшие условия задержания как злоумышленников, пытающихся перебросить материальные ценности за пределы объекта или покинуть с ними охраняемую территорию, так и внешних нарушителей. Это объясняется тем, что по очередности срабатывания СО, расположенных на различных рубежах, силы охраны могут определить направление движения нарушителя.

Таким образом, при построении эффективной системы охранной безопасности (СОБ) объекта необходимо решить задачу оптимизации конфигурации и длины периметра, количества рубежей, выбора СО, физических барьеров (ФБ), средств нейтрализации и поражения, дислокации персонала охраны и т. п.

3 МОДЕЛИРОВАНИЕ И ОЦЕНКА УГРОЗ ФИЗИЧЕСКОГО ДОСТУПА

Объектом данной работы является информационная система «АС «ГосОборонЗаказ» ООО «ЧТЗ – Уралтрак». Сведения о данной системе приведены в приложениях А, Б, В (технический паспорт на автоматизированную систему, описание технологического процесса, сведения о системе как об объекте критической информационной инфраструктуры). Ситуационный план и план этажа с месторасположением сервера, отвечающим за обработку и хранение информации, и который находится в центре обработки данных (ЦОД) организации, приведены в приложении Д.

3.1 Модель нарушителя

Модель нарушителей была составлена в соответствии с методическим документом «Методика определения угроз безопасности информации в информационных системах» ФСТЭК 2015 год.

Согласно ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения», под нарушителем информационной безопасности организации понимается физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.

Относительно прав и возможностей доступа к информации нарушители делятся на два типа:

– внешние нарушители – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

– внутренние нарушители – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

В данной работе рассматриваются внешние нарушители. Угрозы безопасности информации в информационной системе соответственно могут быть реализованы следующими видами нарушителей:

– специальные службы иностранных государств (блоков государств);

– террористические, экстремистские группировки;

– преступные группы (криминальные структуры);

– внешние субъекты (физические лица);

– конкурирующие организации;

– бывшие работники (пользователи).

В качестве возможных целей (мотивации) реализации нарушителями угроз безопасности информации в информационной системе могут быть:

– нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;

– реализация угроз безопасности информации по идеологическим или политическим мотивам;

– организация террористического акта;

– причинение имущественного ущерба путем мошенничества или иным преступным путем;

– дискредитация или дестабилизация деятельности органов государственной власти, организаций;

– получение конкурентных преимуществ;

– любопытство или желание самореализации;

– выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.

– реализация угроз безопасности информации из мести;

На основании видов нарушителей и возможных целей реализации угроз была составлена соответствующая таблица (см. приложение Г).

Необходимо учитывать то, что потенциальные нарушители могут иметь разный потенциал, а также, что нарушители разных видов могут вступать в сговор друг с другом, что ведет к повышению вероятности возникновения угрозы безопасности.

3.2 Структурно-логическая модель объекта и формализованное представление

Объект был описан в части структурно-логической модели посредством понятий «зона» и «рубеж»: зона – часть территории объекта, представляющая собой ограниченное замкнутое пространство, имеющее физические границы; рубеж – физический барьер (часть физической границы зоны), затрудняющий проход или проникновение из одной зоны в другую. Рубеж связывает две зоны.

Зоны между собой взаимодействуют через рубежи защиты: инженерные средства защиты (барьеры по периметру: ограждения, ворота, противотранспортные барьеры, конструкционные барьеры: стены, двери, окна, потолки, полы) с установленными на них техническими средствами обнаружения, наблюдения и контроля: внешними и внутренними датчиками обнаружения, телевизионными системами наблюдения, СКУД.

Формализованное представление структуры объекта описано с помощью теории графов. Данное позволило учесть пространственную модель объекта защиты, т. е. его топологию.

Отметим, что в данном представлении тождественны следующие понятия: граф объекта и структура объекта, вершина графа и зона объекта, ребро графа и рубеж (связь) между зонами объекта.

Граф записывается следующим образом: $G = \{X, A\}$, где X – множество вершин, является множеством зон объекта, A – множество ребер, является множеством рубежей.

Граф представляет объект защиты, и описывает пути проникновения.

Направление перемещения нарушителя по объекту может быть произвольным. Путь ведет от точки проникновения на объект до цели. Движение в обратную сторону (пути отхода нарушителя в случае неудачных попыток проникновения или после совершения запланированных противоправных действий) не рассматриваются. Нарушитель всегда использует рациональный путь, возможно, не самый лучший, но без попыток прохождения по одному и тому же ребру или вершине более одного раза. Таким образом, в графе отсутствуют петли, а пути всегда содержат неповторяющиеся ребра и вершины.

Практически на любом объекте существует возможность проникновения из одной зоны в другую несколькими путями. Различными нарушителями в зависимости от их подготовленности и целей могут быть использованы любые возможные пути. Отсюда следует, что пара вершин может соединяться несколькими ребрами.

Любой проход из одной зоны в другую может преодолеваться в обе стороны. Кроме того, даже из одной точки проникновения пути до различных критических элементов (КЭ) – целей нарушителя – могут включать в себя одинаковые ребра, пройденные в разных направлениях. Таким образом, все ребра в графе считаются неориентированными.

В итоге объект физической защиты описывается неориентированным мультиграфом без петель следующим образом: $G = G\{X, \Gamma\}$, где X – конечное множество вершин графа G; Γ – отображение $\Gamma: X \to X \times z_+$, заданное конечным подмножеством ребер $U \subset X \times X \times z_+$; z_+ – множество неотрицательных целых чисел.

В терминологии теории графов, каждая вершина $x_i \in X$ определяет входящую в модель зону i, а каждое ребро $u_{i,j,n} = \langle x_i, x_j, n \rangle$ определяет связь между вершинами x_i, x_j, соответствующих зонам объекта.

3.3 Графовая модель объекта

Основной принцип построения СФЗ заключается в обеспечении реального уровня защищенности объекта, отражающего степень эффективности и надежности реализованных средств защиты и их соответствия задачам защиты. Следуя этому принципу, требуется найти наиболее уязвимые «места», под которыми понимаются КЭ объекта, включая элементы системы его физической защиты, в отношении которых в силу их недостаточной защищенности или устойчивости могут быть успешно спланированы и реализованы несанкционированные действия, и рекомендовать для них необходимый уровень защиты.

Принципы построения СФЗ рассматриваются в рамках разработанной на этапе проектирования математической модели объекта, которая описывает его структуру, количественный и качественный состав инженерно-технических средств охраны (ИТСО).

Структурная защищенность – степень недостижимости КЭ по выбранному пути от точки проникновения нарушителей.

Структурная защищенность КЭ дает качественную оценку его расположению в структуре системы (объекта). Структурная защищенность позволяет судить о том, насколько безопасно расположение КЭ в структуре системы относительно точки проникновения в период совершения несанкционированных действий.

Оценкой структурной защищенности является мера структурной защищенности КЭ как защищенность наиболее уязвимого пути от точки проникновения на объект до КЭ, рассчитываемая как $P_{\text{стр}} = P_{\text{обн}} \cdot P_{\text{зад}}$.

Для определения вероятностей, составляющих меру структурной защищенности, были определены: составляющие ИТСО, которые препятствуют нарушителям, целью которых является рассматриваемый КЭ. Эти составляющие находятся на выбранном нарушителями пути. Каждый защищенный участок пути (рубеж защиты), который должны преодолеть нарушители, влияет на значение вероятностей $P_{\text{обн}}$ и $P_{\text{зад}}$ данного КЭ. Различные возможные пути нарушителя показывают разные вероятности $P_{\text{обн}}$ и $P_{\text{зад}}$. При анализе эффективности СФЗ выбирается наиболее пессимистический вариант развития событий, т. е. перемещение нарушителя по самым слабозащищенным участкам.

Таким образом, необходимо определить все возможные пути и выбрать среди них наиболее уязвимый (наименее защищенный), т. е. такой, что вероятности $P_{\text{обн}}$ и $P_{\text{зад}}$ на этом пути будут минимальны. Вероятность обнаружения нарушителя на выбранном пути рассчитывается через величину обратную ей – вероятность необнаружения $Q_{\text{обн}} = 1 - P_{\text{обн}}$. Для пути из нескольких рубежей эта величина рассчитываться как вероятность проникновения через все рубежи одновременно. По теории вероятности для оценки одновременного выполнения двух событий их вероятности перемножаются. При известных вероятностях $P_{\text{обн}\,i}$ для каждого i-го рубежа пути из n рубежей, вероятность обнаружения нарушителя $P_{\text{обн}}$ для всего пути равна $1 - Q_{\text{обн}}$, где $Q_{\text{обн}}$ – вероятность необнаружения нарушителя на всем пути. Так как для необнаружения на всем пути нарушитель должен пройти незамеченным все рубежи, то $Q_{\text{обн}}$ равно произведению вероятностей необнаружения на каждом рубеже, соответственно:

$$P_{\text{обн}} = 1 - Q_{\text{обн}} = 1 - \prod_{i=1}^{n} Q_{\text{обн}\,i} = 1 - \prod_{i=1}^{n}(1 - P_{\text{обн}\,i}). \quad (1)$$

Аналогично определяется вероятность $P_{\text{зад}}$ для всего пути:

$$P_{\text{зад}} = 1 - Q_{\text{зад}} = 1 - \prod_{i=1}^{n} Q_{\text{зад}\,i} = 1 - \prod_{i=1}^{n}\left(1 - P_{\text{зад}\,i}\right), \quad (2)$$

где $Q_{\text{зад}}$ и $Q_{\text{зад}\,i}$ – вероятности того, что нарушитель не будет задержан на всем пути и на i-ом рубеже соответственно.

Решение задачи определения меры структурной защищенности всех КЭ объекта требует выявления путей проникновения на объект и оценку характеристик всех рубежей защиты. Оценка вероятностей $P_{\text{обн}}$ и $P_{\text{зад}}$ основана экспертной информации.

Рубежами защиты являются защищенные связи между зонами – ребра графа. В СФЗ средства защиты установлены не только на связях – ребрах, но и в самих зонах – вершинах. Например, защита ребра – это дверь с замком – ФБ, выполняющий свои функции только при попытке прохода из зоны в зону в указанной точке.

Защита вершины – это детектор движения в комнате, который охватывает площадь всего помещения и активируется при перемещении в самой зоне. Таким образом, если зона содержит средство защиты, то это будет увеличивать защищенность проходящего через зону пути. Соответственно вероятности $P_{обн}$ и $P_{зад}$ одинаково заданы и для ребер, и для вершин графа объекта для последующих расчетов.

Описание объекта в терминах структурно-логической модели и поставленными им в соответствие элементами формализованного представления с соответствующими оценками $P_{обн}$ и $P_{зад}$ приведены в приложениях Е, Ж.

3.4 Метод поиска наименее защищенного пути

Поиск наименее защищенного пути из точки проникновения в зону объекта проводился через модифицированный алгоритм Дейкстры, который ищет кратчайшее расстояние от одной из вершин графа до всех остальных.

Алгоритм работает следующим образом: выбирается исходная вершина, минимальные расстояния от которой до остальных вершин требуется найти. Каждой вершине графа сопоставляется метка – минимальное известное расстояние от этой вершины до исходной. На каждом шаге алгоритма анализируется одна вершина, и метки получают новые значения. Когда все вершины проанализированы, значения меток будут равны искомым кратчайшим путям от всех вершин до исходной. В начале работы алгоритма метка исходной вершины приравнивается к 0, а метки остальных вершин к бесконечности, т. к. расстояния до других вершин неизвестны. Все вершины графа помечаются как непосещенные. Далее выполняется следующий шаг алгоритма. Из непосещенных вершин выбирается вершина *U*, имеющая минимальную метку. Рассматриваются всевозможные маршруты, в которых *U* является предпоследним пунктом. Вершины, в которые ведут ребра из *U*, называются соседями этой вершины. Для каждого соседа вершины *U*, кроме посещенных, определяется новая длина пути, равная сумме значений текущей метки *U* и длины ребра, соединяющего *U* с данным соседом. Если полученное значение длины меньше значения метки соседа, происходит замена значения метки соседа полученным значением длины. Проанализировав все соседние вершины, помечаем вершину *U* как посещенную. Если все вершины посещены, алгоритм завершается, иначе описанный шаг алгоритма повторяется.

Данный алгоритм работает для графов без петель и дуг отрицательного веса. Петли в мультиграфе объекта отсутствуют, также, как и отрицательные значения вероятностей. При наличии двух или более ребер, соединяющих одну пару вершин, исключаются из рассмотрения ребра с большим значением рассматриваемой вероятности, т. о. мультиграф превращается в обычный граф. Для разных вероятностей $P_{обн}$ и $P_{зад}$ могут быть исключены разные ребра, т. к. каждое ребро может иметь одну низкую вероятность и вторую высокую.

В мультиграфе объекта каждое ребро – рубеж защиты – обладает двумя показателями $P_{обн}$ и $P_{зад}$ (числовые значения в диапазоне [0, 1]). Чем меньше значение

этих чисел, тем менее защищен путь, в составе которого будет ребро. Поиск пути проводится дважды – по каждому показателю в отдельности. Процедура поиска «вероятности $P_{\text{обн}}$ пути» производится по формуле (1). Значения меток на вершинах (промежуточные значения вероятности $P_{\text{обн}}$ пути) в процессе работы алгоритма определяются через формулу: $P_{\text{мн обн}} = 1 - (1 - P_{\text{м обн}}) \cdot (1 - P_{\text{обн } i}) \cdot (1 - P_{\text{з обн}})$, где $P_{\text{мн обн}}$ – новое значение метки, $P_{\text{м обн}}$ – предыдущее значение метки, $P_{\text{обн } i}$ – значение вероятности на ребре, которое добавляется в путь, $P_{\text{з обн}}$ – значение вероятности на вершине.

С помощью данного алгоритма найдены пути с наименьшими вероятностями $P_{\text{обн}}$. Аналогично – для вероятности $P_{\text{зад}}$. Данная задача решена для всех возможных точек проникновения (в рамках модели).

В приложении И показана блок-схема алгоритма.

3.5 Выводы

В рамках произведенного исследования по выявлению наименее защищенных путей, способствующих успешной реализации угроз физического доступа со стороны нарушителя, и их оценки была проделана следующая работа и получены результаты для практического использования:

1. Описана структурно-логическая модель объекта, и задано ее формализованное представление.
2. Для «зон» и «рубежей» объекта определены на основе экспертной информации вероятности обнаружения и задержки нарушителя.
3. Указаны цель нарушителя, возможные точки проникновения нарушителя на территорию организации.
4. Для каждой возможной точки проникновения нарушителя выявлен наименее защищенный путь (путь проникновения к КЭ), представлена мера структурной защищенности объекта (приложение К).

4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

С развитием научно-технического прогресса немаловажную роль играет возможность безопасного исполнения людьми своих трудовых обязанностей. В связи с этим была создана и развивается наука о безопасности труда и жизнедеятельности человека.

Круг практических задач БЖД прежде всего обусловлен выбором принципов защиты, разработкой и рациональным использованием средств защиты человека и природной среды от воздействия техногенных источников и стихийных явлений, а также средств, обеспечивающих комфортное состояние среды жизнедеятельности.

Охрана здоровья трудящихся, обеспечение безопасности условий труда, ликвидация профессиональных заболеваний и производственного травматизма составляет одну из главных забот человеческого общества.

В связи с тем фактом, что работа с информационной системой производится с использованием средств вычислительной техники, необходимо обеспечить соответствие рабочих мест сотрудников телерадиокомпании действующим нормам стандартов по безопасности жизнедеятельности. Требования санитарных правил направлены на предотвращение неблагоприятного влияния на здоровье человека вредных факторов производственной среды и трудового процесса при работе с ПЭВМ.

4.1 Общие требования к организации и оборудованию рабочих мест

Рабочее место оператора ЭВМ проектируется согласно требованиям СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы»:

1. При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м.
2. Рабочие места с ПЭВМ при выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5–2,0 м.
3. Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600–700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.
4. Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5–0,7.

5. Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ.

Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

6. Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

7. Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680–800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм.

8. Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм.

9. Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм.

10. Конструкция рабочего стула должна обеспечивать:

– ширину и глубину поверхности сиденья не менее 400 мм;

– поверхность сиденья с закругленным передним краем;

– регулировку высоты поверхности сиденья в пределах 400–550 мм и углам наклона вперед до 15 град., и назад до 5 град.;

– высоту опорной поверхности спинки 300 +/- 20 мм, ширину – не менее 380 мм и радиус кривизны горизонтальной плоскости – 400 мм;

– угол наклона спинки в вертикальной плоскости в пределах +/- 30 градусов;

– регулировку расстояния спинки от переднего края сиденья в пределах 260–400 мм;

– стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50–70 мм;

– регулировку подлокотников по высоте над сиденьем в пределах 230 +/- 30 мм и внутреннего расстояния между подлокотниками в пределах 350–500 мм.

11. Рабочее место пользователя ПЭВМ следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности под-

ставки до 20 град. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм.

12. Клавиатуру следует располагать на поверхности стола на расстоянии 100–300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

4.2 Требования к помещениям для размещения рабочих мест

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное помещение, в котором будут располагаться рабочие места, оборудование ЭВМ с ВДТ.

По требованиям СанПиН 2.2.2/2.4.1340-03 помещения для эксплуатации ПЭВМ должны отвечать следующим требованиям:

1. Помещения для эксплуатации ПЭВМ должны иметь естественное и искусственное освещение.

2. Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации.

Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.

3. Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные) должна составлять не менее 4,5 $м^2$.

4. Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка – 0,7-0,8; для стен – 0,5-0,6; для пола – 0,3–0,5.

5. Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации.

6. Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

4.3 Требования к уровню шума на рабочих местах

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03, предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах. Источниками шума в данной

организации являются рабочие станции и сервер. На основании СанПиН 2.2.4.3359-16, нормативным эквивалентным уровнем звука на рабочих местах является 80 дБА.

В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест оснащенных ПЭВМ, шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений ПЭВМ.

4.4 Требования к освещению на рабочих местах

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления.

Согласно СанПиН 2.2.2/2.4.1340-03 предъявляются следующие требования к освещению на рабочих местах:

1. Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.

2. Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами, следует применять системы комбинированного освещения.

3. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300–500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк.

4. Следует ограничивать прямую блесткость от источников освещения, при этом яркость светящихся поверхностей (окна, светильники и др.), находящихся в поле зрения, должна быть не более 200 кд/м^2.

5. Яркость светильников общего освещения в зоне углов излучения от 50 до 90 градусов с вертикалью в продольной и поперечной плоскостях должна составлять не более 200 кд/м^2, защитный угол светильников должен быть не менее 40 градусов.

6. Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении видеодисплейных терминалов. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору.

7. Коэффициент пульсации не должен превышать 5%.

8. Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и све-

тильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

4.5 Требования к микроклимату

Для рабочих мест, на которых работа с использованием ПЭВМ является основной и связана с непрерывным нервно-эмоциональным напряжением, согласно СанПиН 2.2.2/2.4.1340-03 должны обеспечиваться оптимальные параметры микроклимата для категории работ 1а.

Нормативные требования к показателям микроклимата рабочих мест производственных помещений приведены в СанПиН 2.2.4.3359-16.

Оптимальные величины параметров микроклимата для категории работ 1а приведены в таблице 7.

В соответствии с СанПиН 2.2.2/2.4.1340-03, в помещениях оборудованных ПЭВМ, должна проводиться ежедневная влажная уборка, а также проветривание после каждого часа работы на ПЭВМ.

Таблица 2 – Оптимальные величины параметров микроклимата

Период года	Категория работ по уровням энергозатрат, Вт	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	1а (до 139)	22−24	21−25	60−40	0,1
Теплый	1а (до 139)	23−25	22−26	60−40	0,1

4.6 Требования к электробезопасности

По степени опасности поражения электрическим током согласно Правилам Устройства Электроустановок (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью, так как имеется возможность одновременного прикосновения человека к имеющим соединения с землей металлоконструкциям здания с одной стороны и металлическим корпусам электрооборудования с другой.

Если физический доступ к токоведущим частям оборудования затруднен, то основной причиной возникновения данного опасного фактора может являться прикосновение к металлическим нетоковедущим частям (например, корпусу ПЭВМ), которые могут оказаться под напряжением в результате повреждения изоляции. В соответствии с правилами электробезопасности, должен осуществляться постоянный контроль состояния электропроводки, предохранительных

щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Для предотвращения образования и защиты от статического электричества в помещениях с ПЭВМ необходимо использовать аэроионизаторы и увлажнители воздуха. В отделке помещений следует отдавать предпочтение антистатическим материалам. Полы должны иметь антистатическое покрытие.

Согласно документу «Правила устройства электроустановок» (ПУЭ) электробезопасность работающих обеспечивается конструкцией электроустановок; техническими способностями и средствами защиты, организационными средствами защиты. Предусмотрены следующие технические способы и средства защиты от поражения электрическим током:

1. Обеспечение недоступности токоведущих частей, находящихся под напряжением для случайного прикосновения.

2. Устранение опасности поражения при появлении напряжения на нетоковедущих частях электрооборудования посредством заземления (зануления).

4.7 Пожарная безопасность

Постановление Правительства РФ от 25.04.2012 N 390 (ред. от 30.12.2017) «О противопожарном режиме» устанавливают следующие правила:

1. В отношении каждого объекта (за исключением индивидуальных жилых домов) руководителем (иным уполномоченным должностным лицом) организации (индивидуальным предпринимателем), в пользовании которой на праве собственности или на ином законном основании находятся объекты (далее – руководитель организации), утверждается инструкция о мерах пожарной безопасности в соответствии с требованиями.

2. Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности.

Обучение лиц мерам пожарной безопасности осуществляется путем проведения противопожарного инструктажа и прохождения пожарно-технического минимума.

Порядок и сроки проведения противопожарного инструктажа и прохождения пожарно-технического минимума определяются руководителем организации. Обучение мерам пожарной безопасности осуществляется в соответствии с нормативными документами по пожарной безопасности.

3. Руководитель организации назначает лицо, ответственное за пожарную безопасность, которое обеспечивает соблюдение требований пожарной безопасности на объекте.

4. В складских, производственных, административных и общественных помещениях, местах открытого хранения веществ и материалов, а также размещения технологических установок руководитель организации обеспечивает наличие табличек с номером телефона для вызова пожарной охраны.

5. На объекте с массовым пребыванием людей (кроме жилых домов), а также на объекте с рабочими местами на этаже для 10 и более человек руководитель организации обеспечивает наличие планов эвакуации людей при пожаре.

6. На объекте с массовым пребыванием людей руководитель организации обеспечивает наличие инструкции о действиях персонала по эвакуации людей при пожаре, а также проведение не реже 1 раза в полугодие практических тренировок лиц, осуществляющих свою деятельность на объекте защиты.

7. Хранение огнетушителя осуществляется в соответствии с требованиями инструкции по его эксплуатации.

8. Запрещается на территориях общего пользования, прилегающих к объектам защиты, в том числе к жилым домам, а также к объектам садоводческих, огороднических и дачных некоммерческих объединений граждан, оставлять емкости с легковоспламеняющимися и горючими жидкостями, горючими газами.

9. Руководитель организации обеспечивает наличие на дверях помещений производственного и складского назначения и наружных установках обозначение их категорий по взрывопожарной и пожарной опасности.

10. Руководитель организации обеспечивает устранение повреждений средств огнезащиты для строительных конструкций, инженерного оборудования зданий и сооружений, а также осуществляет проверку состояния огнезащитной обработки (пропитки) в соответствии с инструкцией изготовителя и составляет акт (протокол) проверки состояния огнезащитной обработки (пропитки). Проверка состояния огнезащитной обработки (пропитки) при отсутствии в инструкции сроков периодичности проводится не реже 1 раза в год.

11. Руководитель организации организует проведение работ по заделке негорючими материалами, обеспечивающими требуемый предел огнестойкости и дымогазонепроницаемость, образовавшихся отверстий и зазоров в местах пересечения противопожарных преград различными инженерными (в том числе электрическими проводами, кабелями) и технологическими коммуникациями.

12. На объектах защиты запрещается:

а) хранить и применять на чердаках, в подвалах и цокольных этажах легковоспламеняющиеся и горючие жидкости, порох, взрывчатые вещества, пиротехнические изделия, баллоны с горючими газами, товары в аэрозольной упаковке, целлулоид и другие пожаровзрывоопасные вещества и материалы, кроме случаев, предусмотренных иными нормативными документами по пожарной безопасности в сфере технического регулирования;

б) использовать чердаки, технические этажи, вентиляционные камеры и другие технические помещения для организации производственных участков, мастерских, а также для хранения продукции, оборудования, мебели и других предметов;

в) устраивать в подвалах и цокольных этажах мастерские, а также размещать иные хозяйственные помещения, размещение которых не допускается нормативными документами по пожарной безопасности, если нет самостоятель-

ного выхода или выход из них не изолирован противопожарными преградами от общих лестничных клеток;

г) снимать предусмотренные проектной документацией двери эвакуационных выходов из поэтажных коридоров, холлов, фойе, тамбуров и лестничных клеток, другие двери, препятствующие распространению опасных факторов пожара на путях эвакуации;

д) размещать мебель, оборудование и другие предметы на подходах к пожарным кранам внутреннего противопожарного водопровода и первичным средствам пожаротушения, у дверей эвакуационных выходов, люков на балконах и лоджиях, в переходах между секциями и выходами на наружные эвакуационные лестницы, демонтировать межбалконные лестницы, а также заваривать люки на балконах и лоджиях квартир;

е) проводить уборку помещений и стирку одежды с применением бензина, керосина и других легковоспламеняющихся и горючих жидкостей, а также производить отогревание замерзших труб паяльными лампами и другими способами с применением открытого огня;

ж) остеклять балконы, лоджии и галереи, ведущие к незадымляемым лестничным клеткам;

з) устраивать в лестничных клетках и поэтажных коридорах кладовые и другие подсобные помещения, а также хранить под лестничными маршами и на лестничных площадках вещи, мебель и другие горючие материалы;

и) устраивать в производственных и складских помещениях зданий (кроме зданий V степени огнестойкости) антресоли, конторки и другие встроенные помещения из горючих материалов и листового металла;

к) устанавливать в лестничных клетках внешние блоки кондиционеров;

л) загромождать и закрывать проходы к местам крепления спасательных устройств.

13. Руководитель организации обеспечивает содержание наружных пожарных лестниц и ограждений на крышах (покрытиях) зданий и сооружений в исправном состоянии, организует не реже 1 раза в 5 лет проведение эксплуатационных испытаний пожарных лестниц и ограждений на крышах с составлением соответствующего протокола испытаний, а также периодического освидетельствования состояния средств спасения с высоты в соответствии с технической документацией или паспортом на такое изделие.

14. Приямки у оконных проемов подвальных и цокольных этажей зданий (сооружений) должны быть очищены от мусора и посторонних предметов.

15. Руководитель организации обеспечивает сбор использованных обтирочных материалов в контейнеры из негорючего материала с закрывающейся крышкой и удаление по окончании рабочей смены содержимого указанных контейнеров.

16. В зданиях с витражами высотой более одного этажа не допускается нарушение конструкций дымонепроницаемых негорючих диафрагм, установленных в витражах на уровне каждого этажа.

17. Руководителем организации, на объекте которой возник пожар, обеспечивается доступ пожарным подразделениям в закрытые помещения для целей локализации и тушения пожара.

18. Руководитель организации при расстановке в помещениях технологического, выставочного и другого оборудования обеспечивает наличие проходов к путям эвакуации и эвакуационным выходам.

19. Запрещается оставлять по окончании рабочего времени не обесточенными электроустановки и бытовые электроприборы в помещениях, в которых отсутствует дежурный персонал, за исключением дежурного освещения, систем противопожарной защиты, а также других электроустановок и электротехнических приборов, если это обусловлено их функциональным назначением и (или) предусмотрено требованиями инструкции по эксплуатации.

20. Запрещается:

а) эксплуатировать электропровода и кабели с видимыми нарушениями изоляции;

б) пользоваться розетками, рубильниками, другими электроустановочными изделиями с повреждениями;

в) обертывать электролампы и светильники бумагой, тканью и другими горючими материалами, а также эксплуатировать светильники со снятыми колпаками (рассеивателями), предусмотренными конструкцией светильника;

г) пользоваться электроутюгами, электроплитками, электрочайниками и другими электронагревательными приборами, не имеющими устройств тепловой защиты, а также при отсутствии или неисправности терморегуляторов, предусмотренных конструкцией;

д) применять нестандартные (самодельные) электронагревательные приборы;

е) оставлять без присмотра включенными в электрическую сеть электронагревательные приборы, а также другие бытовые электроприборы, в том числе находящиеся в режиме ожидания, за исключением электроприборов, которые могут и (или) должны находиться в круглосуточном режиме работы в соответствии с инструкцией завода-изготовителя;

ж) размещать (складировать) в электрощитовых (у электрощитов), у электродвигателей и пусковой аппаратуры горючие (в том числе легковоспламеняющиеся) вещества и материалы;

з) при проведении аварийных и других строительно-монтажных и реставрационных работ использовать временную электропроводку, включая удлинители, сетевые фильтры, не предназначенные по своим характеристикам для питания применяемых электроприборов.

21. Руководитель организации обеспечивает исправное состояние знаков пожарной безопасности, в том числе обозначающих пути эвакуации и эвакуационные выходы.

22. Запрещается пользоваться неисправными газовыми приборами, а также устанавливать (размещать) мебель и другие горючие предметы и материалы на

расстоянии менее 0,2 метра от бытовых газовых приборов по горизонтали и менее 0,7 метра – по вертикали (при нависании указанных предметов и материалов над бытовыми газовыми приборами).

23. В соответствии с инструкцией завода-изготовителя руководитель организации обеспечивает проверку огнезадерживающих устройств (заслонок, шиберов, клапанов и др.) в воздуховодах, устройств блокировки вентиляционных систем с автоматическими установками пожарной сигнализации или пожаротушения, автоматических устройств отключения вентиляции при пожаре.

24. При эксплуатации систем вентиляции и кондиционирования воздуха запрещается:

а) оставлять двери вентиляционных камер открытыми;

б) закрывать вытяжные каналы, отверстия и решетки;

в) подключать к воздуховодам газовые отопительные приборы;

г) выжигать скопившиеся в воздуховодах жировые отложения, пыль и другие горючие вещества.

25. Руководитель организации определяет порядок и сроки проведения работ по очистке вентиляционных камер, циклонов, фильтров и воздуховодов от горючих отходов с составлением соответствующего акта, при этом такие работы проводятся не реже 1 раза в год.

26. Руководитель организации обеспечивает укомплектованность пожарных кранов внутреннего противопожарного водопровода пожарными рукавами, ручными пожарными стволами и вентилями, организует перекатку пожарных рукавов (не реже 1 раза в год).

27. Руководитель организации обеспечивает исправное состояние систем и средств противопожарной защиты объекта (автоматических (автономных) установок пожаротушения, автоматических установок пожарной сигнализации , установок систем противодымной защиты, системы оповещения людей о пожаре, средств пожарной сигнализации, противопожарных дверей, противопожарных и дымовых клапанов, защитных устройств в противопожарных преградах) и организует не реже 1 раза в квартал проведение проверки работоспособности указанных систем и средств противопожарной защиты объекта с оформлением соответствующего акта проверки.

28. Выбор типа и расчет необходимого количества огнетушителей следует производить в зависимости от огнетушащей способности, предельной площади, класса пожара горючих веществ и материалов защищаемом помещении или на объекте согласно СП 9.13130.2009 «Техника пожарная. Огнетушители. Требования к эксплуатации».

Для помещений компании актуальны следующие классы пожаров:

Класс А – пожары твердых веществ, основном органического происхождения, горение которых сопровождается тлением (древесина, текстиль, бумага).

Класс Е – пожары, связанные с горением электроустановок.

Для данных классов пожаров, исходя из рекомендаций СП 9.13130.2009, следует применять порошковые огнетушители.

Огнетушители следует располагать на защищаемом объекте в соответствии с требованиями ГОСТ 12.4.009 таким образом, чтобы они были защищены от воздействия прямых солнечных лучей, тепловых потоков, механических воздействий и других неблагоприятных факторов (вибрация, агрессивная среда, повышенная влажность и т.д.). Они должны быть хорошо видны и легкодоступны в случае пожара. Предпочтительно размещать огнетушители вблизи мест наиболее вероятного возникновения пожара, вдоль путей прохода, а также около выхода из помещения. Огнетушители не должны препятствовать эвакуации людей во время пожара.

Огнетушители, введенные в эксплуатацию, должны подвергаться техническому обслуживанию, которое обеспечивает поддержание огнетушителей в постоянной готовности к использованию и надежную работу всех узлов огнетушителя в течение всего срока эксплуатации. Техническое обслуживание включает в себя периодические проверки, осмотры, ремонт, испытания и перезарядку огнетушителей.

4.8 Сравнение параметров рабочего места с допустимыми нормами

Для того чтобы определить соответствие условий труда требованиям нормативных документов необходимо провести сравнительный анализ требований, установленных к рабочим местам, оборудованным ПЭВМ и фактических параметров рабочего места. Схема размещения рабочего места приведена на рисунке 1. Площадь помещения 18 м^2, оконный проем, шириной 1,4 м размещается слева. В помещении присутствует естественное и искусственное освещение.

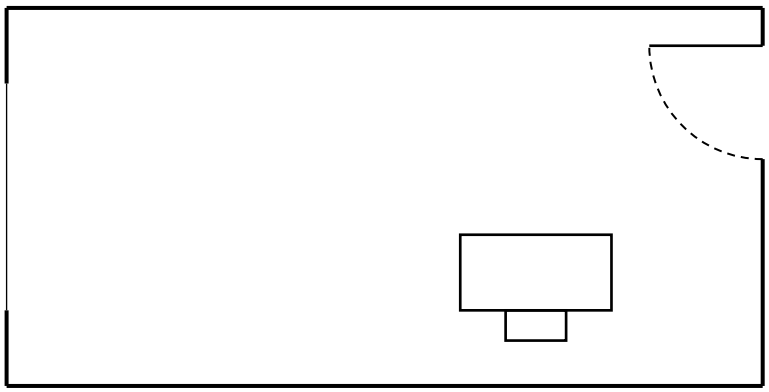


Рисунок 4 – Схема рабочего места

Перечень нормируемых параметров для рабочего места, сравнение их допустимых норм и фактических значений на рабочем месте представлены в табл. 7.

Таблица 3 – Сравнение параметров рабочего места с допустимыми нормами

Нормируемые параметры	Допустимые нормы	Фактические значения
Высота рабочей поверхности стола	от 680 до 800мм, либо 725мм	725мм
Модульные размеры рабочей поверхности стола	ширина 800, 1000, 1200, 1400мм, глубина 800 и 1000мм	ширина 1400 мм глубина 600 мм
Ширина и глубина поверхности сиденья	не менее 400мм	ширина 500 мм глубина 450 мм
Наличие подставки для ног	ширина не менее 300 мм, глубина не менее 400 мм	отсутствует
Регулировка сиденья по высоте	в пределах 400–550 мм	500 мм
Площадь на одно рабочее место	не менее 4,5м2	18м2
Падение естественного света	преимущественно слева	слева
Освещенность поверхности стола	300–500 лк	395 лк
Уровень звука	80 дБА	51 дБА
Параметры микроклимата (кат. 1а)	Температура воздуха 22-24 °С Влажность воздуха 40-60%	Температура 22 °С Влажность воздуха 55%

4.9 Выводы

В результате проведенного анализа требований были выявлены общие требования к организации рабочих мест пользователей, требования к помещениям для работы с ПЭВМ, основные требования к освещению на рабочих местах, уровню шума и микроклимату. На основе проведенного анализа было установлено, что условия труда на рабочем месте соответствуют вышеперечисленным требованиям за исключением глубины рабочего места и наличия подставки для ног.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы были промоделированы возможные пути внешнего нарушителя для получения физического доступа к объекту защиты, выявлены наиболее оптимальные из них (гарантирующие с высокой вероятностью получение доступа к объекту защиты) и предоставлены соответствующие показатели меры структурной защищенности. Полученные результаты были учтены в организации подхода к решению задач по снижению вероятностей реализации угроз физического доступа.

В теоретической части уделено внимание рассмотрению самой концепции инженерно-технической информации, сформулированы основные положения, а также цели и задачи, которые должна решать эффективная система инженерно-технической защиты информации. Уделено внимание основным принципам защиты, а также принципам построения эффективной системы. Большое внимание уделено рассмотрению целей функционирования систем физической защиты с выделением и классификацией угроз подсистем обнаружения. Рассмотрены особенности построения периметровой охраны и использования инженерно-технических систем и ТСО для увеличения задержки времени проникновения злоумышленника, и тем самым увеличения времени для его обнаружения.

С учетом принципов и подходов в теоретической части была произведена практическая работа по моделированию и оценке угроз физического доступа.

В практической части работы описана структурно-логическая модель объекта (сведения о котором приведены в приложениях А, Б, В). Описана модель внешнего нарушителя (приложение Г). На базе системы компьютерной алгебры Wolfram Mathematica создано формализованное представление в виде графа, сопровождающееся весовыми коэффициентами, для расчета меры структурной защищенности критического элемента системы (объекта). Исходные планы территории и этажа с критическим элементом объекта приведены в приложении Д. Визуальное представление исследуемой структуры (графа) в проекции на план-схемы организации приведены в приложении Е, его описание – описание рубежей и зон – приложении Ж.

Для каждой точки проникновения нарушителя найдены наиболее оптимальные пути подхода к объекту защиты, вычислены соответствующие им показатели структурной защищенности. Поиск путей проникновения произведен по алгоритму блок-схема которого представлена в приложении И. Граф объекта, точки проникновения, соответствующие им пути и показатели меры структурной защищенности представлены таблицей в приложении К и сопровождены визуальным представлением.

Для полученного множества оптимальных для нарушителя путей выявлена общая составляющая маршрута. Данное позволяет обозначить направление, представляющее наибольшую угрозу для объекта защиты с точки зрения реализации угроз физического доступа и сделать акцент на контроле соответствующего

участка выявленных путей с целью пресечения и/или минимизации угроз физического доступа со стороны нарушителя в текущей обстановке.

Данный подход позволяет для каждого объекта защиты выявить пути обеспечение контроля которых позволит пресечь и/или минимизировать угрозы физического доступа с наименьшими затратами ресурсов по сравнению с тем если бы осуществлялся контроль всевозможных подступов к объекту защиты. Последнее безусловно максимально снизит вероятность реализации угроз физического доступа к объекту, но несет в себе достаточно высокую нагрузку на ресурсное обеспечение.

Последовательное применение данного алгоритма позволяет решать задачу максимально эффективного размещения ТСО на территории организации с целью минимизации угроз физического доступа.

Проведенная работа позволяет говорить об актуальности использования методов теории графов в оценке угроз физического доступа и ее практической значимости. Система представления рубежей защиты, методы работы с ней, а также широкий потенциал прикладного программного обеспечения с реализованными методами работы с различного рода объектами, в том числе с графами, и их унифицированным представлением позволяет максимально полно учитывать факторы, влияющие на качество результата.

Данный подход позволяет дать оценку угрозам физического доступа (оценить защищенность объекта), указать пути их реализации, выработать рекомендации для их пресечения и/или минимизации. Модели в виде графов в меру просты, универсальны, обеспечены мощным фундаментальным и прикладным аппаратом, а также системами работы с ними, и имеют высокую практическую значимость в различных областях науки и деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) «Об информации, информационных технологиях и о защите информации» // СПС КонсультантПлюс [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/.

2. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС КонсультантПлюс [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.

3. Боровских, А.С. Модели, методы и алгоритмы интеллектуальной поддержки принятия решений в задачах разработки и оценки систем физической защиты объектов информатизации: автореферат дис. … д-ра техн. наук / А.С. Боровских. – СПб., 2015. – 33 с.

4. Тарасов, А.Д. Метод и алгоритмы проектирования систем физической защиты объектов информатизации на основе обработки нечеткой информации: автореферат дис. … канд. техн. наук / А.Д. Тарасов. – Уфа, 2017. – 16 с.

5. Боровский, А.С. Автоматизированное проектирование и оценка систем физической защиты потенциально-опасных (структурно-сложных) объектов. Часть 2. Модели нечетких систем принятия решений в задачах проектирования систем физической защиты / А.С. Боровский, А.Д. Тарасов. – Оренбург: Издательский центр ОГАУ, 2013. – 247 с.

6. Бузов, Г.А. Защита от утечки информации по техническим каналам: Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия – Телеком, 2005. – 416 с.

7. Технические средства и методы защиты информации. Учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. – 4 изд., испр. и доп. – М.: Горячая линия – Телеком, 2012. – 616 с.

8. Торокин, А.А. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

9. Мосолов, А.С. Изучение универсального метода проектирования систем инженерно-технической защиты объектов: учебное пособие / А.С. Мосолов, Е.А. Беляева, А.В. Бадиков. – М.: НИЯУ МИФИ, 2010. – 84 с.

10. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний // СПС Кодекс [Электронный ресурс]. – URL: http://docs.cntd.ru/document/1200071688.

11. ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний // СПС Кодекс [Электронный ресурс]. – URL: http://docs.cntd.ru/document/1200113776.

12. ГОСТ Р 12.1.046-2014. Система стандартов безопасности труда. Строительство. Нормы освещения строительных площадок // СПС Кодекс [Электронный ресурс]. – URL: http://docs.cntd.ru/document/1200114236.

13. Р 78.36.005-2011 Выбор и применение систем контроля управления доступом. – М.: ФГУ НИЦ «Охрана» МВД России, 2011. – 95 с.

14. Башуров, В.В. Математические модели безопасности / В.В. Башуров, Т.И. Филимоненкова. – Новосибирск: Наука, 2009. – 85 с.

15. Кормен, Томас Х. Алгоритмы: вводный курс / Томас Х. Кормен; пер. с англ. И.В. Красикова. – М.: ООО «И. Д. Вильямс», 2013. – 1328 с.

16. Левитин, Ананий В. Алгоритмы: введение в разработку и анализ / Ананий В. Левитин; пер. с англ. С.Г. Тригуб, И.В. Красикова. – М.: Издательский дом «Вильямс», 2006. – 576 с.

17. Булатов, Д.К. Применение алгоритма волновой трассировки в задачах моделирования инженерно-технической защиты информации / Д.К. Булатов, А.Н. Соколов // Вестник УрФО. Безопасность в информационной сфере. Секция «Инженерно-техническая защита информация». – 2014. – № 2 (12). – С. 4–8.

18. СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы: Санитарно-эпидемиологические правила и нормативы. – М.: Федеральный центр госсанэпиднадзора Минздрава России, 2003. – 54 с.

19. СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих места: Санитарно-эпидемиологические правила и нормативы // СПС КонсультантПлюс [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_203183/.

20. СП 9.13130.2009. Техника пожарная. Огнетушители. Требования к эксплуатации // СПС Кодекс [Электронный ресурс]. – URL: http://docs.cntd.ru/document/1200071152.

21. Постановление Правительства РФ от 25.04.2012 N 390 (ред. от 30.12.2017) «О противопожарном режиме» // СПС КонсультантПлюс [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_129263/.

22. ГОСТ 12.4.009-83. Система стандартов безопасности труда. Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание // СПС Кодекс [Электронный ресурс]. – URL: http://docs.cntd.ru/document/1200003611.

ПРИЛОЖЕНИЕ А

УТВЕРЖДАЮ
Директор ООО «ЧТЗ – Уралтрак»
_____/_____
«____» _____ 2017 г.

ООО «ЧТЗ – Уралтрак»

ТЕХНИЧЕСКИЙ ПАСПОРТ

Автоматизированная система

«АС «ГосОборонЗаказ»

2017 г.

Уч. № _____-ДСП

Страница **1** из **12**

1. Общие сведения об АС

1.1. Наименование АС: «АС «ГосОборонЗаказ» ООО «ЧТЗ – Уралтрак».

1.2. Расположение АС: ******, г. Челябинск, …

1.3. Класс АС: 1Г («Акт классификации автоматизированной системы», № _____-ДСП от _____._____.2017).

2. Состав оборудования АС

2.1. Перечень ОТСС входящих в состав АС.

№ п/п	Тип	Наименование	Серийный номер
Кабинет № * здания «С»**			
АРМ 1			
1.	ПК	HP ProDesk 400 G4, корпус Microtower	
2.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
3.	Клавиатура	HP USB Slim Business Keyboard	
4.	Мышь	HP USB 1000dpi Laser Mouse	
АРМ 2			
5.	ПК	HP ProDesk 400 G4, корпус Microtower	
6.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
7.	Клавиатура	HP USB Slim Business Keyboard	
8.	Мышь	HP USB 1000dpi Laser Mouse	
АРМ 3			
9.	ПК	HP ProDesk 400 G4, корпус Microtower	
10.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
11.	Клавиатура	HP USB Slim Business Keyboard	
12.	Мышь	HP USB 1000dpi Laser Mouse	
АРМ 4			
13.	ПК	HP ProDesk 400 G4, корпус Microtower	
14.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
15.	Клавиатура	HP USB Slim Business Keyboard	
16.	Мышь	HP USB 1000dpi Laser Mouse	
Периметр ЛВС			
17.	Коммутатор	Cisco SG350-10MP-K9	
18.	Принтер	HP LaserJet Pro M501dn	
Кабинет № * здания «В»**			
АРМ 5			
19.	ПК	HP ProDesk 400 G4, корпус Microtower	
20.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
21.	Клавиатура	HP USB Slim Business Keyboard	
22.	Мышь	HP USB 1000dpi Laser Mouse	

№ п/п	Тип	Наименование	Серийный номер
АРМ 6			
23.	ПК	HP ProDesk 400 G4, корпус Microtower	
24.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
25.	Клавиатура	HP USB Slim Business Keyboard	
26.	Мышь	HP USB 1000dpi Laser Mouse	
АРМ 7			
27.	ПК	HP ProDesk 400 G4, корпус Microtower	
28.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
29.	Клавиатура	HP USB Slim Business Keyboard	
30.	Мышь	HP USB 1000dpi Laser Mouse	
АРМ 8			
31.	ПК	HP ProDesk 400 G4, корпус Microtower	
32.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
33.	Клавиатура	HP USB Slim Business Keyboard	
34.	Мышь	HP USB 1000dpi Laser Mouse	
АРМ 9			
35.	ПК	HP ProDesk 400 G4, корпус Microtower	
36.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
37.	Клавиатура	HP USB Slim Business Keyboard	
38.	Мышь	HP USB 1000dpi Laser Mouse	
АРМ 10			
39.	ПК	HP ProDesk 400 G4, корпус Microtower	
40.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
41.	Клавиатура	HP USB Slim Business Keyboard	
42.	Мышь	HP USB 1000dpi Laser Mouse	
Периметр ЛВС			
43.	Коммутатор	Cisco SG350-10MP-K9	
44.	МФУ	HP LaserJet Enterprise MFP M527c	
Кабинет № * здания «А»**			
АРМ 11			
45.	ПК	HP ProDesk 400 G4, корпус Microtower	
46.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
47.	Клавиатура	HP USB Slim Business Keyboard	
48.	Мышь	HP USB 1000dpi Laser Mouse	
49.	Принтер	HP LaserJet Pro M501dn	
АРМ 12			
50.	ПК	HP ProDesk 400 G4, корпус Microtower	
51.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
52.	Клавиатура	HP USB Slim Business Keyboard	

№ п/п	Тип	Наименование	Серийный номер
53.	Мышь	HP USB 1000dpi Laser Mouse	
54.	Принтер	HP LaserJet Pro M501dn	
АРМ 13			
55.	ПК	HP ProDesk 400 G4, корпус Microtower	
56.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
57.	Клавиатура	HP USB Slim Business Keyboard	
58.	Мышь	HP USB 1000dpi Laser Mouse	
59.	Принтер	HP LaserJet Pro M501dn	
АРМ 14			
60.	ПК	HP ProDesk 400 G4, корпус Microtower	
61.	Монитор	HP ProDisplay P240va 23.8-inch Monitor	
62.	Клавиатура	HP USB Slim Business Keyboard	
63.	Мышь	HP USB 1000dpi Laser Mouse	
64.	Принтер	HP LaserJet Pro M501dn	
Периметр ЛВС			
65.	Коммутатор	Cisco SG350-10MP-K9	
66.	МФУ	HP LaserJet Enterprise MFP M527c	

2.2. Перечень ВТСС входящих в состав АС.

№ п/п	Тип	Наименование	Серийный номер
Кабинет № * здания «С»**			
АРМ 1			
1.	Телефон	Panasonic KX-TS2365RUW	
АРМ 2			
2.	Телефон	Panasonic KX-TS2365RUW	
АРМ 3			
3.	Телефон	Panasonic KX-TS2365RUW	
АРМ 4			
4.	Телефон	Panasonic KX-TS2365RUW	
Кабинет № * здания «В»**			
АРМ 5			
5.	Телефон	Panasonic KX-TS2365RUW	
АРМ 6			
6.	Телефон	Panasonic KX-TS2368RUW	
АРМ 7			
7.	Телефон	Panasonic KX-TS2365RUW	
АРМ 8			
8.	Телефон	Panasonic KX-TS2365RUW	

№ п/п	Тип	Наименование	Серийный номер
АРМ 9			
9.	Телефон	Panasonic KX-TS2365RUW	
АРМ 10			
10.	Телефон	Panasonic KX-TS2365RUW	
Кабинет № * здания «А»**			
АРМ 11			
11.	Телефон	Panasonic KX-TS2368RUW	
АРМ 12			
12.	Телефон	Panasonic KX-TS2365RUW	
АРМ 13			
13.	Телефон	Panasonic KX-TS2365RUW	
АРМ 14			
14.	Телефон	Panasonic KX-TS2365RUW	
Прочее (в общем, на кабинеты АС зданий «С», «В», «А»)			
15.		Извещатель пожарный дымовой оптико-электронный (6 шт.)	
16.		Извещатель охранный объемный (3 шт.)	
17.		Извещатель охранный магнито-контактный (3 шт.)	

2.3. Структура, топология и размещение технических средств АС относительно границ контролируемой зоны объекта.

АС состоит из 14 АРМ, объединенных через сетевое оборудование в ЛВС, и взаимодействие которых осуществляется на сетевой архитектуре типа «клиент-сервер». Информация обрабатывается и хранится на удаленном сервере, расположенном ЦОД ООО «ЧТЗ – Уралтрак». АС не имеет точки доступа в сеть общего пользования.

АС расположена в трех кабинетах зданий «С», «В», «А» соответственно (см. рис. 1). Контролируемой зоной является территория ООО «ЧТЗ – Уралтрак».

Схемы размещения и расположения ОТСС, ВТСС, а также проводных линий и коммуникаций объекта приведены в приложении 1.

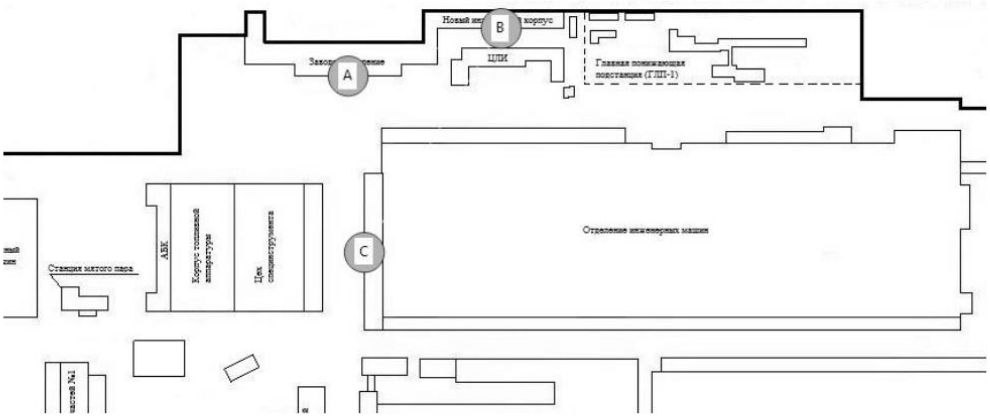


Рисунок 1 – Условное расположение АС

2.4. Системы электропитания и заземления.

Для электропитания технических средств АС применена схема TN-C-S с глухозаземленной нейтралью на трансформаторной подстанции (ТП). ТП расположена за пределами контролируемой зоны и имеет подключения сторонних потребителей со стороны низшего напряжения. Питающие кабели от ТП к АС проходят за пределами контролируемой зоны. Вводно-распределительное устройство расположено за пределами контролируемой зоны.

Выделенный контур заземления отсутствует. Заземляющее устройство повторного заземления здания расположено за пределами КЗ.

2.5. Перечень СЗИ установленных в АС.

№ п/п	СЗИ, лицензия	Заводской номер	Сведения о сертификации	Место, дата установки
1	Kaspersky Endpoint Security 10		ФСТЭК России, № 3025 до 25.11.2019	АРМ 1–14, _____._____.2017

2.6. Перечень используемого в АС программного обеспечения.

№ п/п	Наименование программного обеспечения	Примечания
АРМ 1–4		
	Microsoft Windows 7 Professional	
	Microsoft Office 2010 Standard	
	WinRAR 5.50	
АРМ 5–10		
	Microsoft Windows 7 Professional	

№ п/п	Наименование программного обеспечения	Примечания
	Microsoft Office 2010 Standard	
	AutoCAD 2016 Mechanical	
	Matlab R2016a	
	WinRAR 5.50	
АРМ 11–14		
	Microsoft Windows 7 Professional	
	Microsoft Office 2010 Standard	
	1С: Управление производственным предприятием 8. Редакция 1.3	
	WinRAR 5.50	

3. Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации

Уч. № _____-ДСП

Страница **7** из **12**

Результаты периодического контроля

№ п/п	Дата проведения проверки	Наименование организации проводящей проверку	Результаты проверки. Номер отчетного документа

Уч. № _____-ДСП

Страница **8** из **12**

Лист регистрации изменений

№ п/п	Дата внесения изменения	Описание вносимого изменения	Подпись ответственного за эксплуатацию

ПРИЛОЖЕНИЕ 1

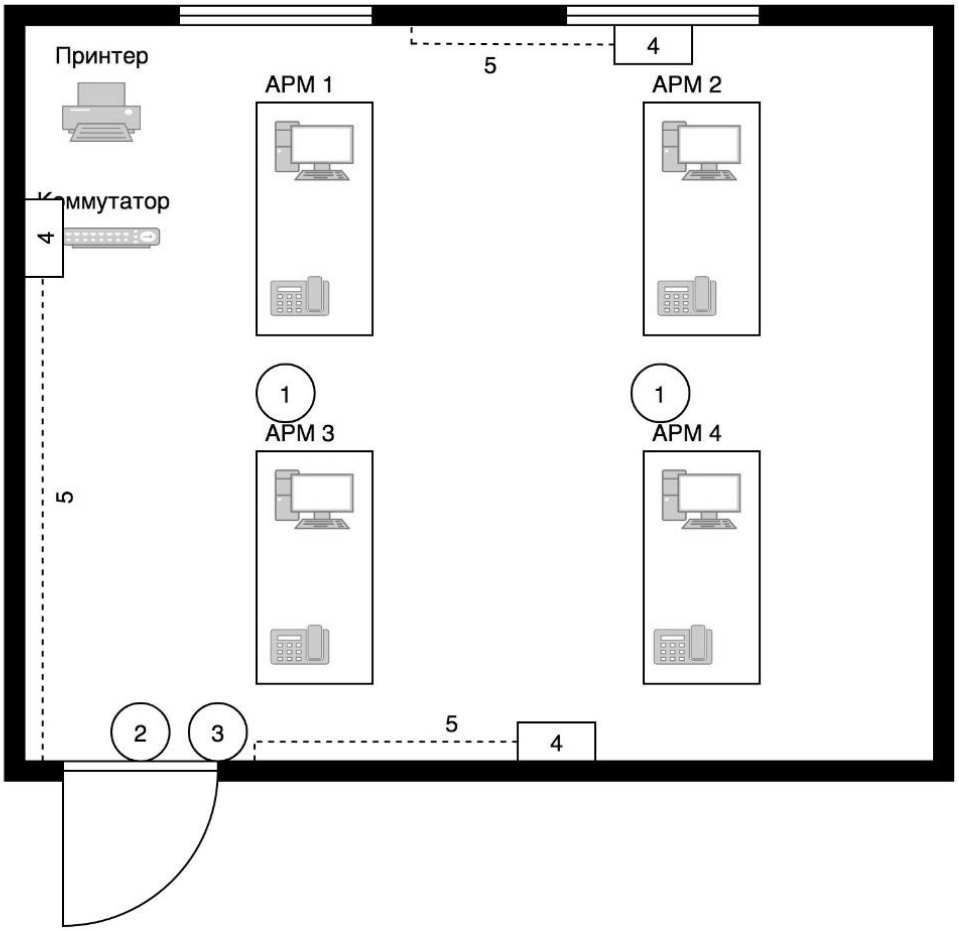


Рисунок 2 – Кабинет № *** здания «С»

1 – извещатель пожарный дымовой оптико-электронный; 2 – извещатель охранный объемный; 3 – датчик охранный магнито-контактный; 4 – сетевой фильтр; 5 – линии электропитания.

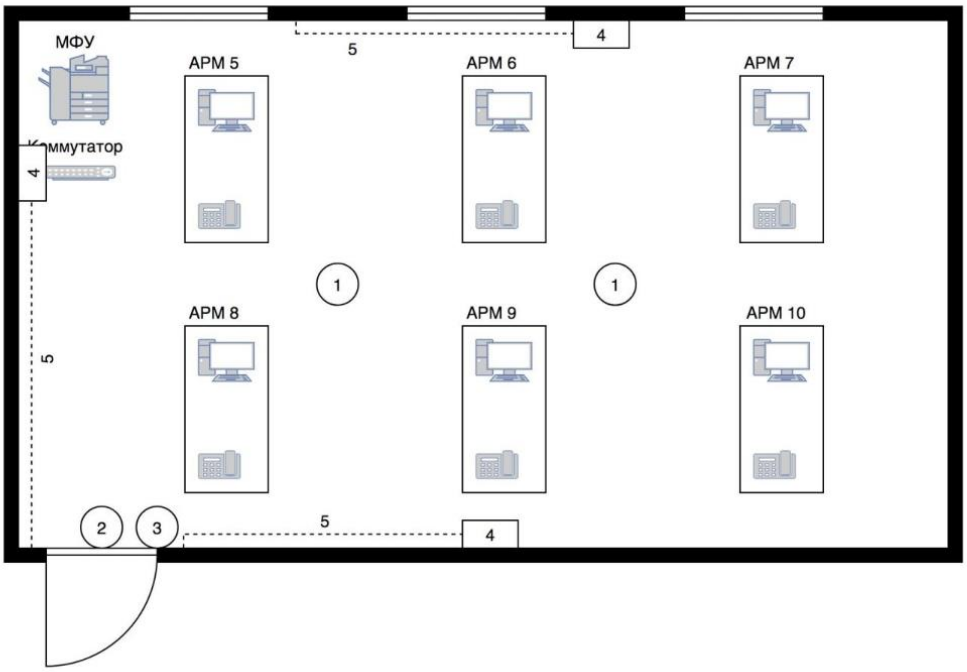


Рисунок 3 – Кабинет № *** здания «В»

1 – извещатель пожарный дымовой оптико-электронный; 2 – извещатель охранный объемный; 3 – датчик охранный магнито-контактный; 4 – сетевой фильтр; 5 – линии электропитания.

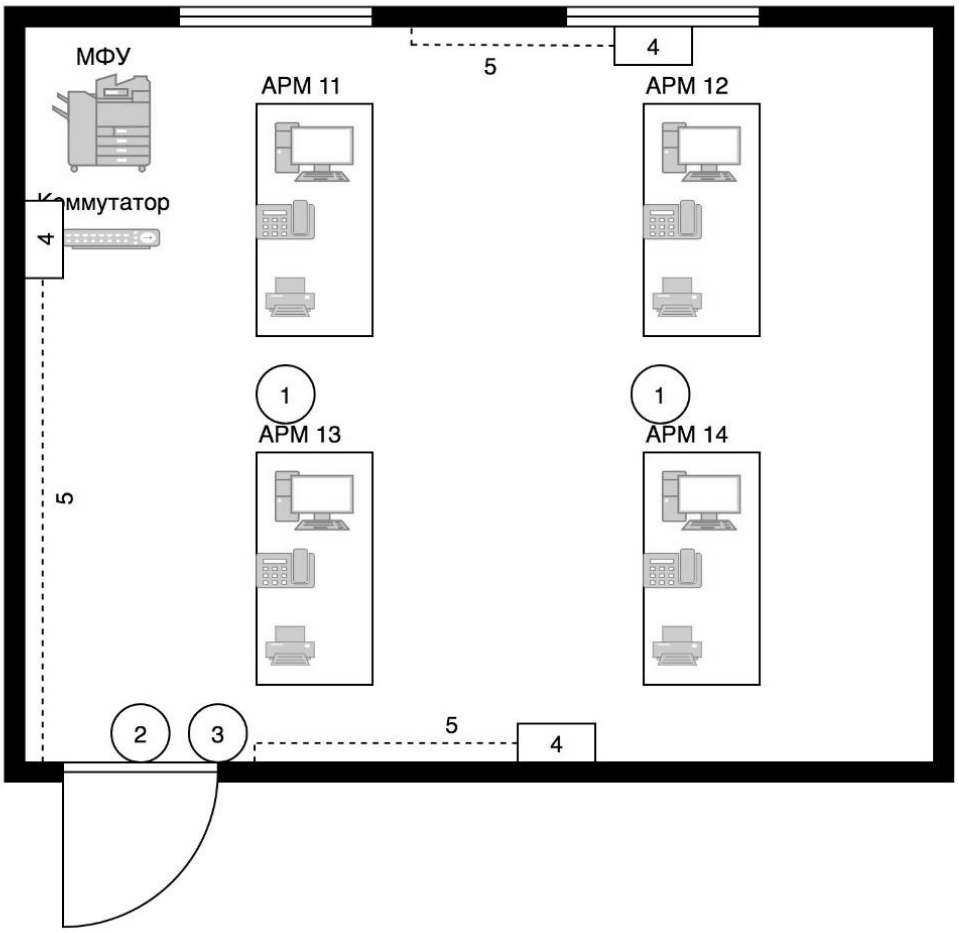


Рисунок 4 – Кабинет № *** здания «А»

1 – извещатель пожарный дымовой оптико-электронный; 2 – извещатель охранный объемный; 3 – датчик охранный магнито-контактный; 4 – сетевой фильтр; 5 – линии электропитания.

ПРИЛОЖЕНИЕ Б

УТВЕРЖДАЮ
Директор ООО «ЧТЗ – Уралтрак»
_____/_____
«____» _____ 2017 г.

ООО «ЧТЗ – Уралтрак»

ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

Автоматизированная система

«АС «ГосОборонЗаказ»

2017 г.

Уч. № _____-ДСП

Страница **1** из **4**

1. Общее описание

АС расположена по адресу: ******, г. Челябинск, …

В АС «АС «ГосОборонЗаказ» обрабатываются информация ограниченного доступа, в целях обеспечения производственных задач и обеспечения бесперебойного производства.

АС состоит из 14 АРМ, объединенных через сетевое оборудование в ЛВС. В АС отсутствует точка доступа в сеть общего пользования.

Защищаемая информация хранятся в виде записей баз данных на удаленном сервере, расположенном ЦОД ООО «ЧТЗ – Уралтрак». Доступ пользователей к информации, находящейся на сервере, осуществляется посредством терминального доступа. Системным и прикладным ПО данной АС предусмотрены механизмы идентификации и аутентификации пользователей и разграничения прав доступа.

Защищаемая информация имеет в АС ряд форм фиксации:

– в виде записей баз данных;

– в виде файлов баз данных;

– в виде изображений на экране монитора;

– в виде твердой бумажной копии;

– в виде побочных электромагнитных излучений и наводок;

– в виде сигналов в оперативной памяти технических средств.

КЗ АС являются помещения ООО «ЧТЗ – Уралтрак». В пределах КЗ находятся отдельные помещения, рабочие места пользователей, сетевое и телекоммуникационное оборудование АС. Контролируемая зона вложенного типа.

Для АС определен перечень лиц, доступ которых к защищаемой информации необходим для выполнения служебных обязанностей.

Организован порядок доступа в помещения с техническими средствами АС.

2. Описание технологического процесса обработки информации

2.1. Подготовка к обработке информации.

1) Получение исходной информации для обработки в системе

Первичный ввод информации в АС осуществляется с бумажных носителей информации.

Исходная информация может находиться на документах в бумажном виде, на отчуждаемых носителях.

2) Вход пользователя в систему:

Режим работы пользователей – многопользовательский. Пользователи АС работают в базе данных, расположенной на удаленном сервере. Вход пользователя в систему осуществляется по идентификатору пользователя (логин доступа в АС) и проверки подлинности субъекта доступа по паролю условно-постоянного действия, набираемому с клавиатуры.

2.2. Обработка информации.

3) Ввод обрабатываемых исходных данных в систему:

Ввод информации – перенос информации с бумажных на внутренние электронные носители АС.

Ввод в систему обрабатываемой информации производится вручную с клавиатуры.

Ввод данных осуществляется пользователями АС при помощи закрепленных за ними АРМ.

4) Обработка конфиденциальной информации:

Обработка информации – преобразование входной информации к формату, необходимому для ее хранения, преобразование хранимой информации к формату, соответствующему требованиям вывода документа на экран монитора либо на принтер.

Обработка конфиденциальной информации осуществляется с помощью программ пакета «1С: УПП», Microsoft Office, AutoCAD, Matlab.

Последовательность обработки информации пользователями:

– запуск ПЭВМ;

– регистрация в АС (предъявление идентификатора и пароля);

– авторизация в АС;

– работа с записями баз данных посредством прикладного программного обеспечения;

– работа с файлами ПО Microsoft Office;

– выход из АС.

Права доступа к локальным ресурсам АС назначаются администратором безопасности с использованием средств операционной системы.

Доступ к файлам настроек механизмов защиты информации разрешен только администратору безопасности АС.

5) Временное хранение обрабатываемой информации между сеансами работы пользователя в системе:

Хранение обрабатываемой информации между сеансами работы осуществляется на удаленном сервере.

2.3. Сохранение результатов обработки информации.

6) Распечатка защищаемых документов (данных)

Распечатка защищаемых документов (данных) осуществляется на МФУ и локальных принтерах в составе АС.

Право печати документов, содержащих защищаемые данные, предоставляется всем пользователям АС. За каждым из пользователей закреплено право печати с на любом из средств печати (в пределах кабинета), входящих в состав АС: МФУ, принтеры.

7) Сохранение окончательных результатов работы:

Готовые данные в электронном виде остаются для хранения на удаленном сервере. Результаты деятельности сохраняются в электронном и бумажном виде.

8) Регистрация времени работы и действий пользователя в системе

Время работы пользователя и его действия в ходе сеанса работы в системе регистрируются автоматически средствами ОС.

2.4. Служебные операции.

9) Управление доступом пользователей к АС:

Под управлением доступом пользователей к ресурсам АС понимается назначение, изменение и удаление учетных реквизитов пользователей (идентификаторы, пароли), а также установка, изменение и прекращение прав пользователей на доступ к ресурсам АС (аппаратным, программным, информационным).

Управление доступом к локальным ресурсам осуществляется штатными средствами ОС и соответствующего прикладного ПО.

10) Обновление ПО:

Под обновлением понимается замена ПО устаревшей версии на новую версию этого же ПО.

Обновление ПК осуществляется администратором. В процессе обновления ПК допускается ввод информации с оптических дисков и накопителей типа USB-flash.

11) Устранение сбоев аппаратного и программного обеспечения:

Устранение сбоев – восстановление работоспособности как отдельных элементов АС, так и всей АС в целом.

Для защиты от сбоев в АС предприняты следующие меры:

– ограничение физического доступа к техническим средствам АС;

– выполнение технического обслуживания уполномоченным лицом.

При выходе из строя технических средств АС, выполнение операций технологического процесса прекращается. Устранение сбоев осуществляется администратором.

ПРИЛОЖЕНИЕ В

Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

1. Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта	АИС «ГосОборонЗаказ»
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	Территория организации, здания «А», «В», «С»
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	Оборонная
1.4.	Назначение объекта	Обеспечение производственных задач и бесперебойного функционирования производства
1.5.	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	Управленческие, финансово-экономические
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	Клиент-серверная система

2. Сведения о субъекте критической информационной инфраструктуры

2.1.	Наименование субъекта	ООО «ЧТЗ – Уралтрак»
2.2.	Адрес местонахождения субъекта	454007, г. Челябинск, пр. Ленина, 3
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	Руководитель…

2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	Начальник отдела информационной безопасности…
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	Отдел информационной безопасности

3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Выделенная
3.2.	Наименование оператора связи	Компания «Интерсвязь»
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Оперативный обмен информацией и документооборотом
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	Проводной, волоконно-оптическая линия связи Протоколы взаимодействия TCP/IP

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	–
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	–
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	–

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры

5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	АРМ 1–14 Выделенный сервер (в ЦОД) Коммутационное оборудование
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	Операционные системы: Microsoft Windows 7 Professional
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	Microsoft Office 2010 Standard Adobe Acrobat Reader DC WinRAR 5.50 AutoCAD 2016 Mechanical Matlab R2016a
5.4.	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации.	Средство антивирусной защиты Kaspersky Endpoint Security 10 – Сертификат ФСТЭК России № 3025 действителен до 25.11.2019

6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	Внешний нарушитель: − специальные службы иностранных государств; − террористические и экстремистские группировки; − преступные группы; − физические лица; − конкурирующие организации; − разработчики, производители, поставщики программных, технических и программно-технических средств; − бывшие работники. Внутренний нарушитель: − пользователи информационной системы; − системные администраторы и администраторы информационной безопасности; − лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ. Организация многоуровневая система физической защиты, охрана и контролируемая зона по периметру организации позволяют исключить присутствие внешнего нарушителя. Реализация угроз со стороны внутреннего нарушителя сведена к минимуму, так как сотрудники предприятия проходят многоступенчатый отбор и проинструктированы о работе с АС «АС «ГосОборонЗаказ» и ответственности за нарушения, что исключает возможность реализации угроз внутренним нарушителем.
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	Угрозы из банка данных угроз неактуальны, ввиду наличия многоуровневой системы физической защиты, многоступенчатого отбора и обучения сотрудников, применения сертифицированных средств антивирусной защиты, и отсутствия доступа в сеть общего пользования. Реализовано разграничение прав доступа к системным и пользовательским файлам, проводится своевременное обновление ПО и резервное копирование файлов АС «АС «ГосОборонЗаказ».

7. Возможные последствия в случае возникновения компьютерных инцидентов

7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	Отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта.
7.2.	Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" или обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов	Ущерб оценен в пределах 5–10% от прогнозируемого дохода предприятия ввиду срыва переговоров или подписания договоров с заказчиками и контрагентами, например, из-за выхода из строя АС «АС «ГосОборонЗаказ». Снижение объема работ в части оборонного заказа на 5–10%, и увеличение времени, требуемого на выполнение заказов на 3–10% ввиду прекращения работы АС «АС «ГосОборонЗаказ».

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры

8.1.	Категория значимости, которая присвоена объекту	III категория
8.2.	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	В следующем абзаце, цифра – это номер показателя критерия значимости, согласно постановлению Правительства №127. 1 – неприменим. Причинение ущерба жизни и здоровью людей исключено; 2 – неприменим. Нарушение функционирования объектов обеспечения жизнедеятельности населения исключено; 3 – неприменим. Отсутствуют ограничения функционирования транспортной системы; 4 – неприменим. АС «АС «ГосОборонЗаказ» не способствует прекращению или нарушению функционирования сети связи; 5 – неприменим. Объект не связан с оказанием государственных услуг; 6 – неприменим. Субъект не является государственным органом; 7 – неприменим. Объект не задействуется в деятельности, сопровождающейся международными переговорами и подписанием международных договоров; 8 – ущерб оценен в пределах 5–10% от прогнозируемого дохода предприятия ввиду срыва переговоров или подписания договоров с заказчиками и контрагентами, например, из-за выхода из строя АС «АС «ГосОборонЗаказ»; 9 – неприменим. Возникновение ущерба бюджетам Российской Федерации в масштабах деятельности субъекта невозможно; 10 – неприменим. Прекращение или нарушение проведения клиентами операций по банковским счетам невозможно. Субъект не осуществляет деятельность в сфере оказания банковских услуг, не является организацией финансового рынка; 11 – неприменим. Вредные воздействия на окружающую среду исключены; 12 – неприменим. Субъект не является пунктом управления (ситуационным центром); 13 – снижение объема работ в части оборонного заказа на 5–10%, и увеличение времени, требуемого на выполнение заказов на 3–10% ввиду прекращения работы АС «АС «ГосОборонЗаказ»; 14 – неприменим. АС «АС «ГосОборонЗаказ» напрямую не функционирует в области обеспечения обороны страны, безопасности государства и правопорядка.

9. Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры

9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	Установлена контролируемая зона – территория организации. Физический доступ осуществляется через КПП по пропускам, также доступ к объекту ограничен списками лиц, постоянно работающих в помещении, где обрабатывается защищаемая информация. Производится постоянный контроль за выполнением работниками установленного комплекса мероприятий по обеспечению безопасности в АС «АС «ГосОборонЗаказ» и обеспечению уровня защищенности информации. Проводятся инструктажи с пользователями АС «АС «ГосОборонЗаказ» по выполнению требований информационной безопасности. Ежеквартально производится проверка работоспособности аппаратных и программных средств защиты информации. Проводится контроль правил генерации и смены паролей пользователей, реализации правил разграничения доступом, полномочий пользователей в АС «АС «ГосОборонЗаказ».
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	Антивирусная защита реализована средствами Kaspersky Endpoint Security 10

ПРИЛОЖЕНИЕ Г
Модель нарушителя (внешнего)

№ п/п	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
1	Специальные службы иностранных государств (блоков государст)	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
4	Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием
7	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия

ПРИЛОЖЕНИЕ Д
Ситуационный план объекта

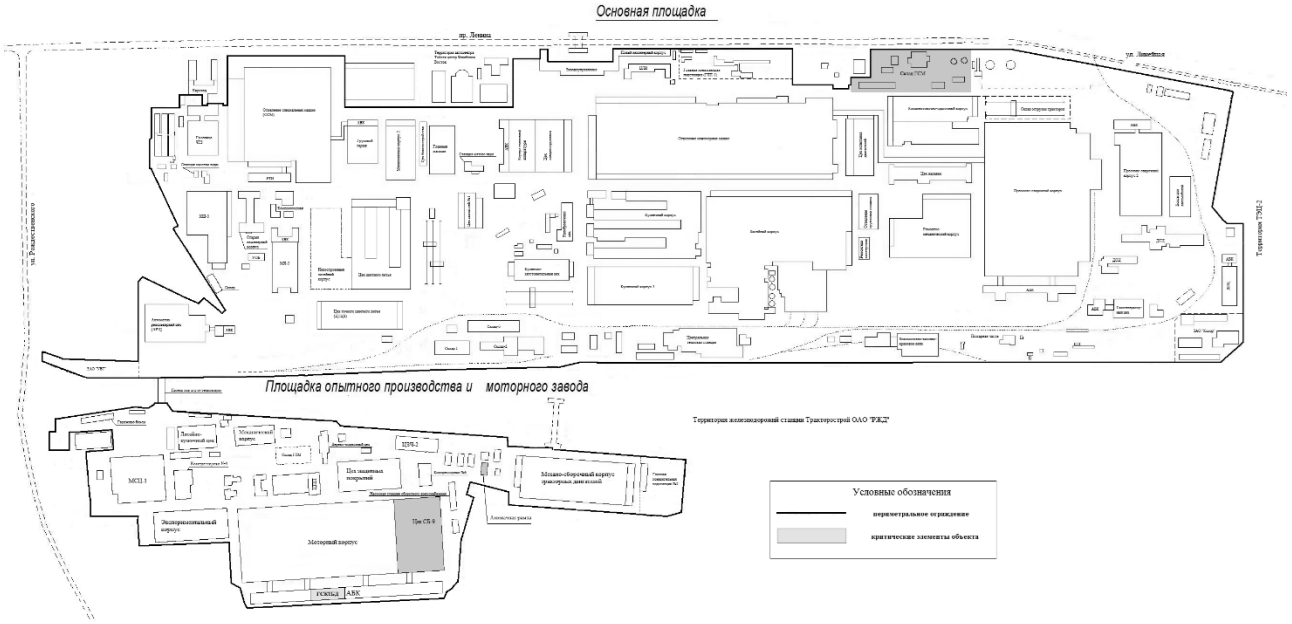


Рисунок Д.1 – Ситуационный план

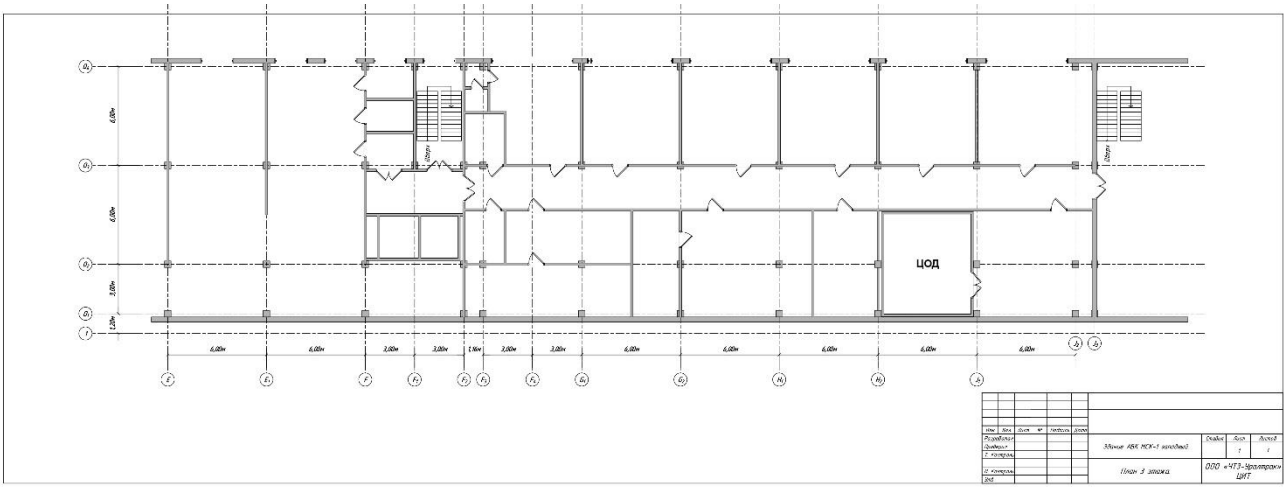


Рисунок Д.2 – План 3 этажа

ПРИЛОЖЕНИЕ Е
Рубежи и зоны объекта. Проекция

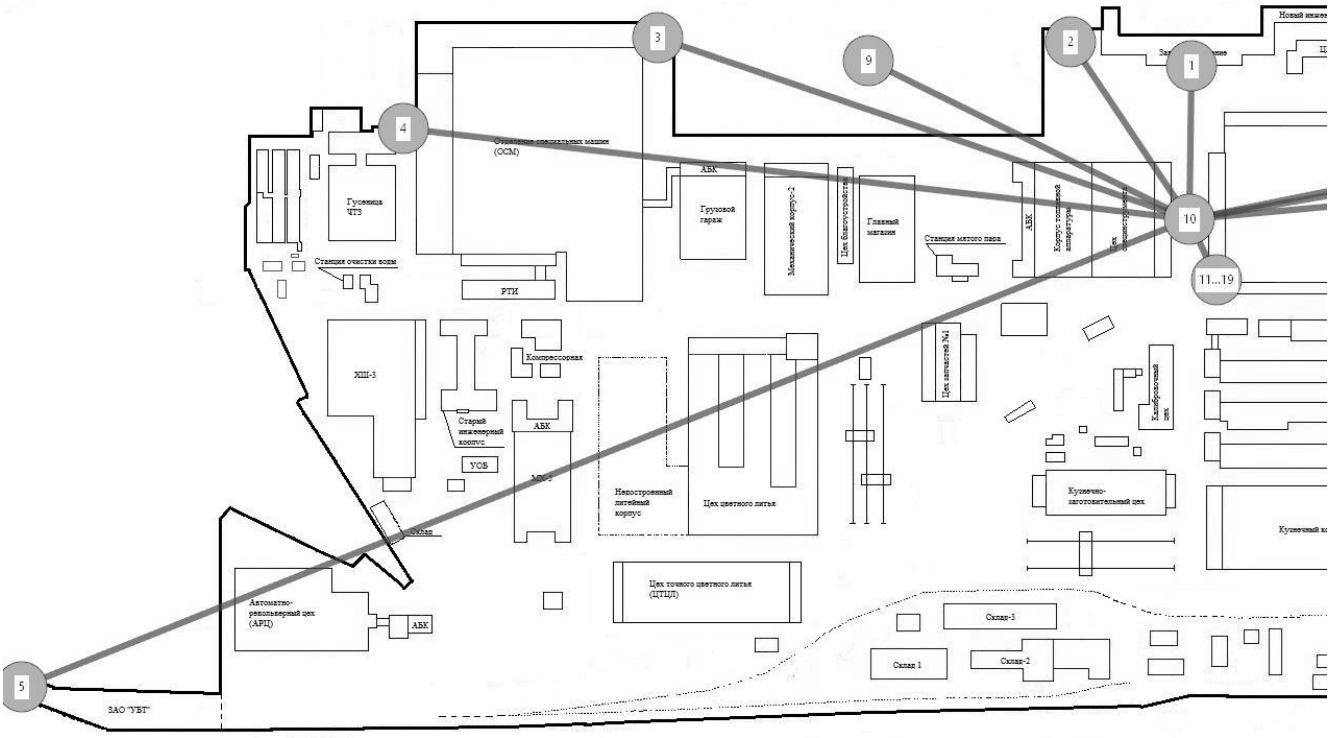


Рисунок Е.1 – Ситуационный план. Часть 1

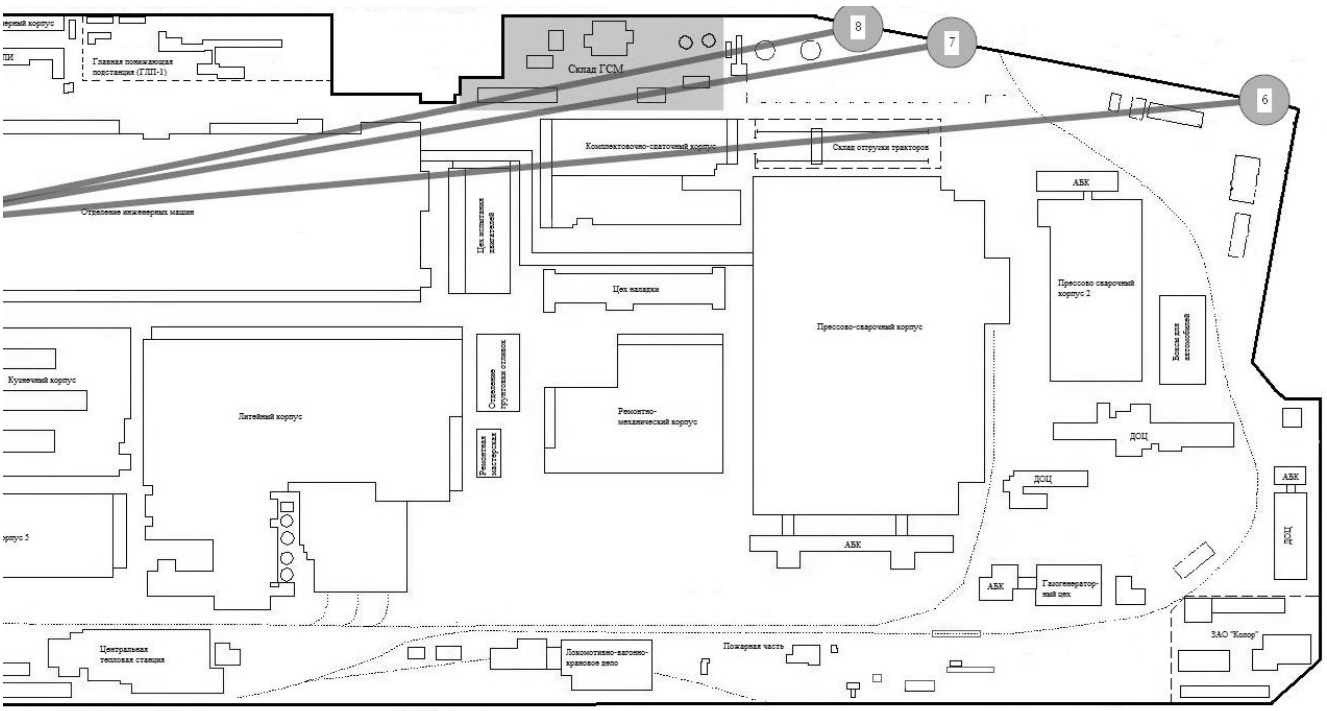


Рисунок Е.2 – Ситуационный план. Часть 2

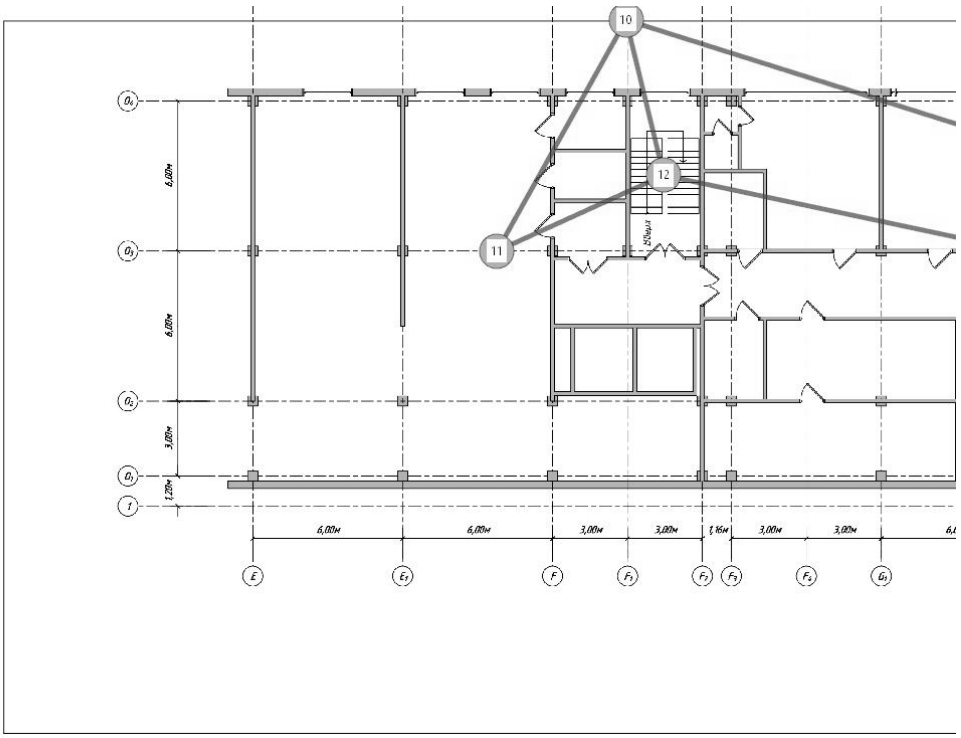


Рисунок Е.3 – Этаж 2. Часть 1

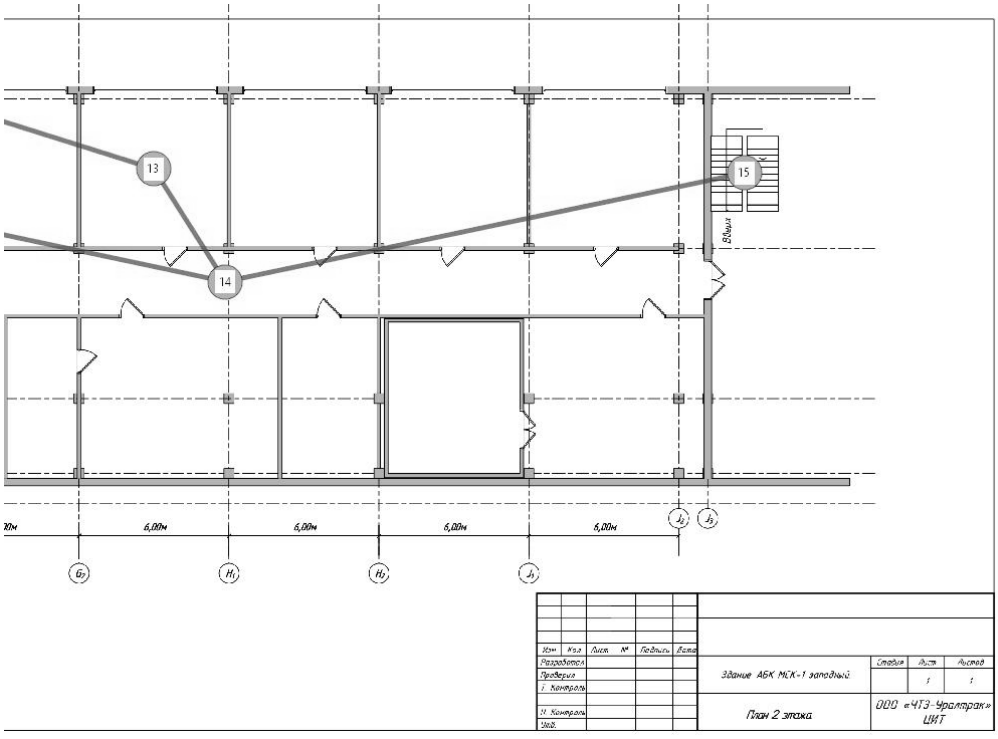


Рисунок Е.4 – Этаж 2. Часть 2

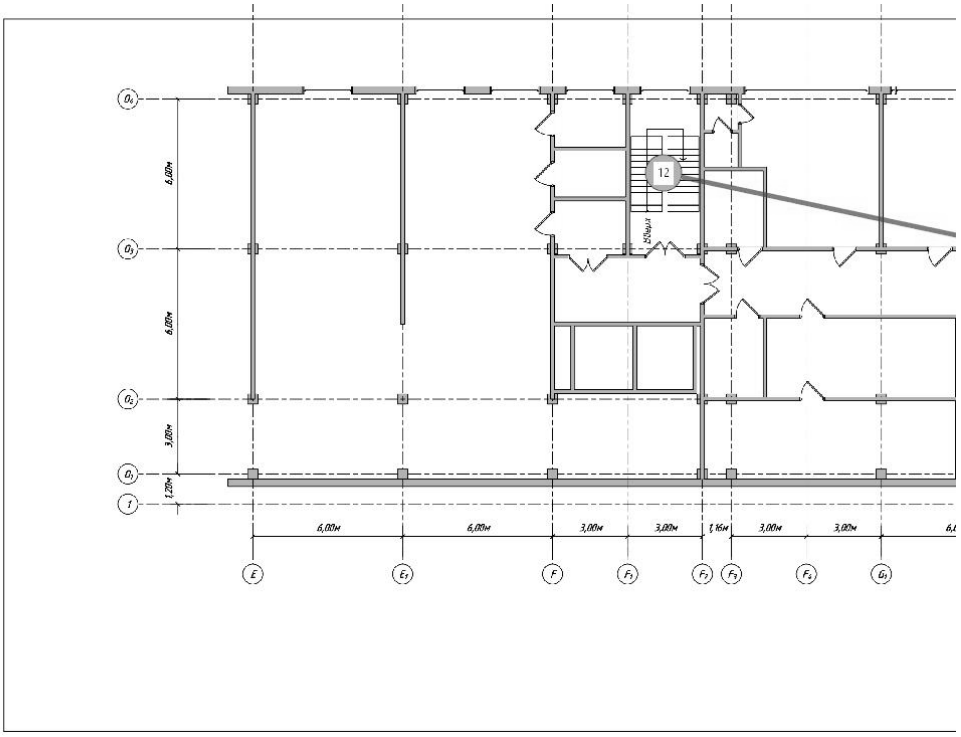


Рисунок Е.5 – Этаж 3. Часть 1

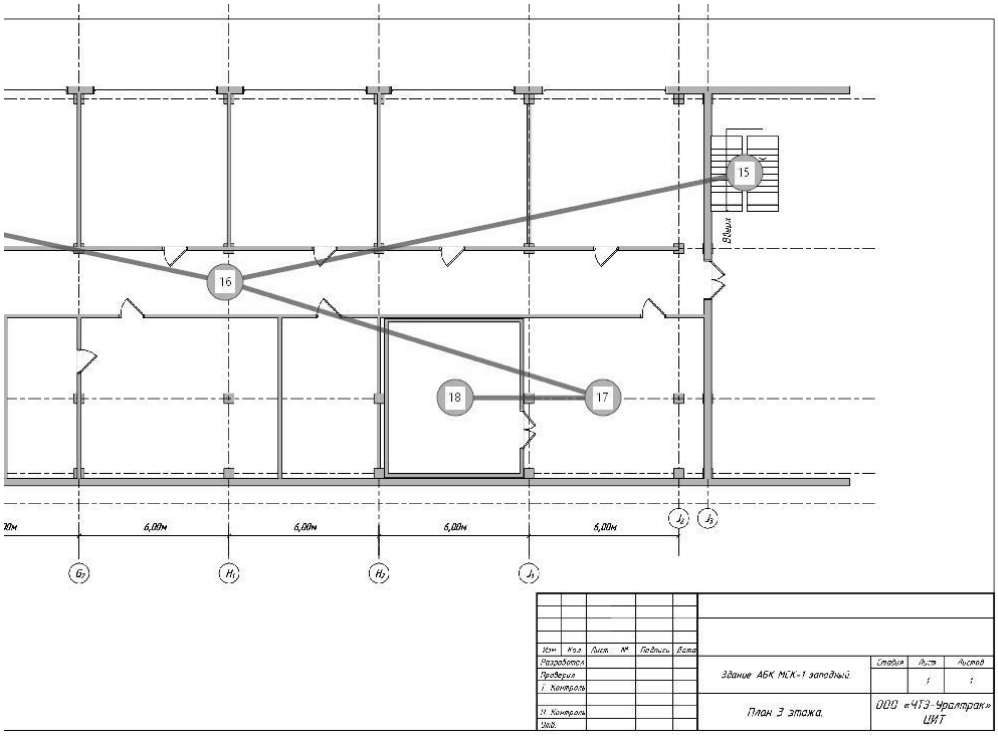


Рисунок Е.6 – Этаж 3. Часть 2

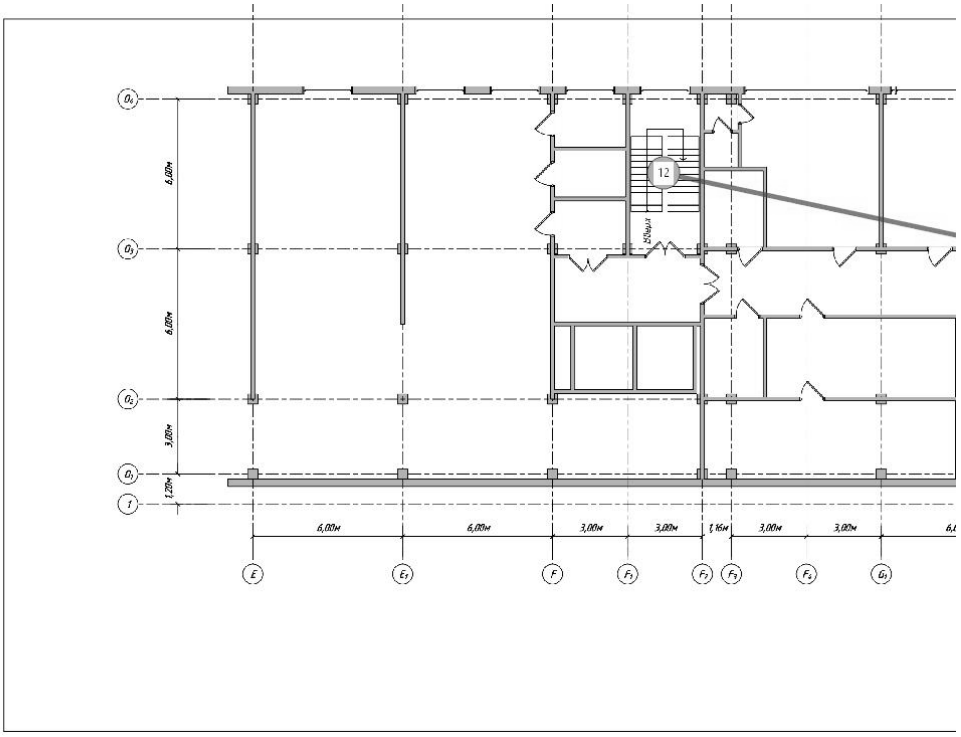


Рисунок Е.7 – Этаж 4. Часть 1

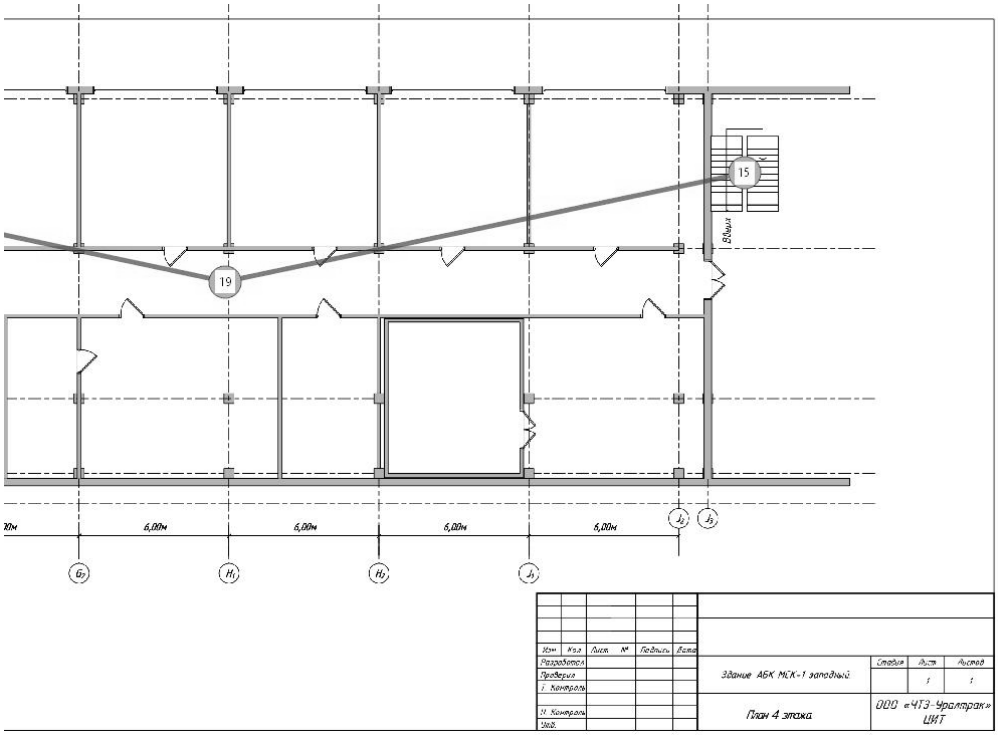


Рисунок Е.8 – Этаж 4. Часть 2

ПРИЛОЖЕНИЕ Ж
Рубежи и зоны объекта. Описание

Номера зон и обозначение рубежей	**Описание зон и рубежей**	**Средства обнаружения**	**Средства задержки**	**Значения вероятностей обнаружения и задержки**
1	**2**	**3**	**4**	**5**
1	КПП	Доступ посторонних ограничен	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
1–10	Вход с территории	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
2	КПП с пропуском автомобильного транспорта	Доступ посторонних ограничен	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
2–10	Вход с территории	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
3	КПП с пропуском автомобильного транспорта	Доступ посторонних ограничен	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
3–10	Вход с территории	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
4	КПП с пропуском автомобильного транспорта	Доступ посторонних ограничен	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
4–10	Вход с территории	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
5	КПП с пропуском автомобильного транспорта	Доступ посторонних ограничен	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
5–10	Вход с территории	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
6	КПП с пропуском автомобильного транспорта	Доступ посторонних ограничен	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
6–10	Вход с территории	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
7	КПП с пропуском железнодорожного транспорта	Доступ посторонних ограничен	СКУД	$P_{обн}$ = низкая $P_{зад}$ = низкая
7–10	Вход с территории	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0

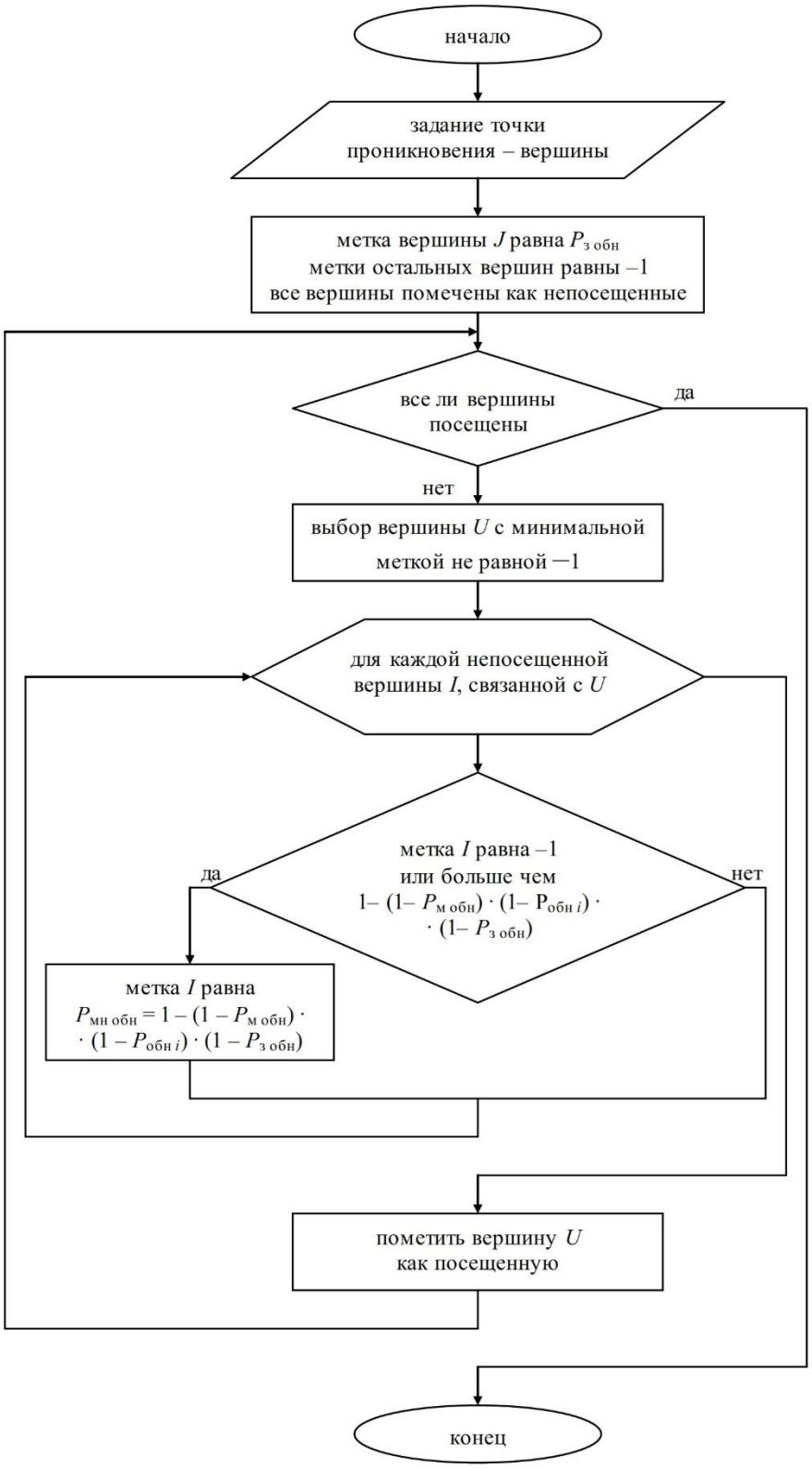
1	2	3	4	5
8	КПП с пропуском автомобильного транспорта	Доступ посторонних ограничен	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
8–10	Вход с территории	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
9	Зона обнаружения и физического сдерживания	Видеонаблюдение	Инженерные укрепления	$P_{обн}$ = средняя $P_{зад}$ = низкая
9–10	Вход с территории	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
10	Территория внутри защитного периметра	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
10–11	«Вход» с территории	Сигнальный рубеж	Окно	$P_{обн}$ = средняя $P_{зад}$ = средняя
10–12	Вход с территории	–	Дверь с замком	$P_{обн}$ =0 $P_{зад}$ = низкая
10–13	«Вход» с территории	Сигнальный рубеж	Окно	$P_{обн}$ = средняя $P_{зад}$ = средняя
11	Помещение	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
11–12	Переход на лестничную площадку	–	Дверь	$P_{обн}$ = 0 $P_{зад}$ = низкая
12	Территория межэтажных пролетов (основная лестница)	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
12–14	Вход на этаж	Сигнальные рубежи	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
12–16	Вход на этаж	Сигнальные рубежи	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
12–19	Вход на этаж	Видеонаблюдение	Дверь с замком	$P_{обн}$ = средняя $P_{зад}$ = низкая
13	Кабинет (2 этаж)	Видеонаблюдение	–	$P_{обн}$ = средняя $P_{зад}$ = 0
13–14	Вход на этаж	Сигнальные рубежи	Дверь с замком (усиленная)	$P_{обн}$ = высокая $P_{зад}$ = средняя
14	Коридор 2 этажа	Видеонаблюдение	–	$P_{обн}$ = средняя $P_{зад}$ = 0

1	2	3	4	5
14–15	Вход на этаж	–	Дверь с замком	$P_{обн}$ = 0 $P_{зад}$ = низкая
15	Территория межэтажных пролетов (внутри здания)	–	–	$P_{обн}$ = 0 $P_{зад}$ = 0
15–16	Вход на этаж	–	Дверь заблокированная	$P_{обн}$ = 0 $P_{зад}$ = низкая
15–19	Вход на этаж	–	Дверь с замком	$P_{обн}$ = 0 $P_{зад}$ = низкая
16	Коридор 3 этажа	Видеонаблюдение	–	$P_{обн}$ = средняя $P_{зад}$ = 0
16–17	Доступ в ЦОД	Доступ посторонних ограничен	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
17	Помещение ЦОД (персонал)	Сигнальные рубежи, видеонаблюдение	–	$P_{обн}$ = высокая $P_{зад}$ = 0
17–18	Доступ в ЦОД	Доступ посторонних ограничен	СКУД	$P_{обн}$ = высокая $P_{зад}$ = высокая
18	Помещение ЦОД (серверная)	Сигнальные рубежи, видеонаблюдение	–	$P_{обн}$ = высокая $P_{зад}$ = 0
19	Коридор 4 этажа	Видеонаблюдение	–	$P_{обн}$ = средняя $P_{зад}$ = 0

Номер зоны	$P_{обн}$	$P_{зад}$
1	0.6	0.6
2	0.6	0.6
3	0.6	0.6
4	0.6	0.6
5	0.6	0.6
6	0.6	0.6
7	0	0
8	0.6	0.6
9	0.3	0
10	0	0
11	0	0
12	0	0
13	0.3	0
14	0.3	0
15	0	0
16	0.3	0
17	0.6	0
18	0.6	0
19	0.3	0

Обозначение рубежа	$P_{обн}$	$P_{зад}$
1–10	0	0
2–10	0	0
3–10	0	0
4–10	0	0
5–10	0	0
6–10	0	0
7–10	0	0
8–10	0	0
9–10	0	0
10–11	0.3	0.3
10–12	0	0
10–13	0.3	0.3
11–12	0	0
12–14	0.6	0.6
12–16	0.6	0.6
12–19	0.3	0
13–14	0.6	0.3
14–15	0	0
15–16	0	0
15–19	0	0
16–17	0.6	0.6
17–18	0.6	0.6

ПРИЛОЖЕНИЕ И
Блок-схема модифицированного алгоритма Дейкстры



ПРИЛОЖЕНИЕ К
Граф объекта. Структурная защищенность

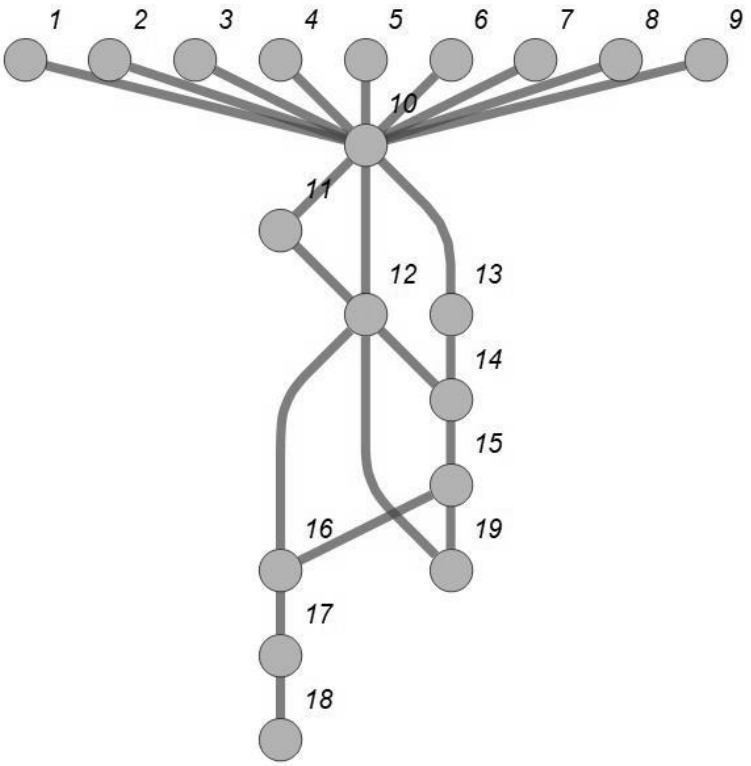


Рисунок К.1 – Граф объекта (абстрактное представление)

Таблица К.1 – Наименее защищенные пути и их мера структурной защищенности

Путь нарушителя	$P_{\text{обн}}$	$P_{\text{зад}}$	$P_{\text{стр}}$
{1, 10, 12, 19, 15, 16, 17, 18}	0.996488	0.936	0.932712
{2, 10, 12, 19, 15, 16, 17, 18}	0.996488	0.936	0.932712
{3, 10, 12, 19, 15, 16, 17, 18}	0.996488	0.936	0.932712
{4, 10, 12, 19, 15, 16, 17, 18}	0.996488	0.936	0.932712
{5, 10, 12, 19, 15, 16, 17, 18}	0.996488	0.936	0.932712
{6, 10, 12, 19, 15, 16, 17, 18}	0.996488	0.936	0.932712
{7, 10, 12, 19, 15, 16, 17, 18}	0.991219	0.84	0.832624
{8, 10, 12, 19, 15, 16, 17, 18}	0.996488	0.936	0.932712
{9, 10, 12, 19, 15, 16, 17, 18}	0.993853	0.84	0.834837

Наименее защищенные пути и их общая составляющая (пунктир)

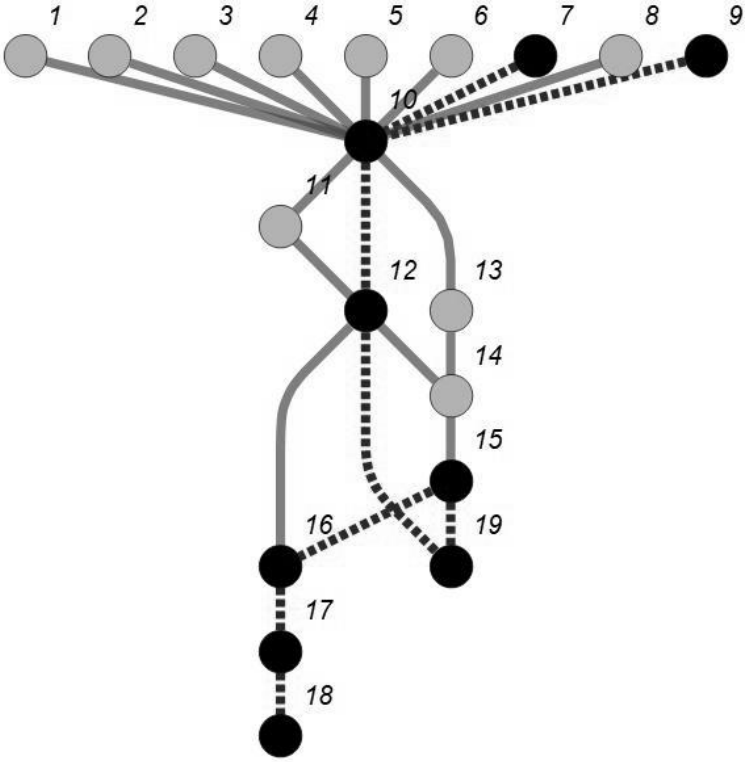


Рисунок К.2 – Наименее защищенные пути (точки проникновения: 7, 9; цель: 18)

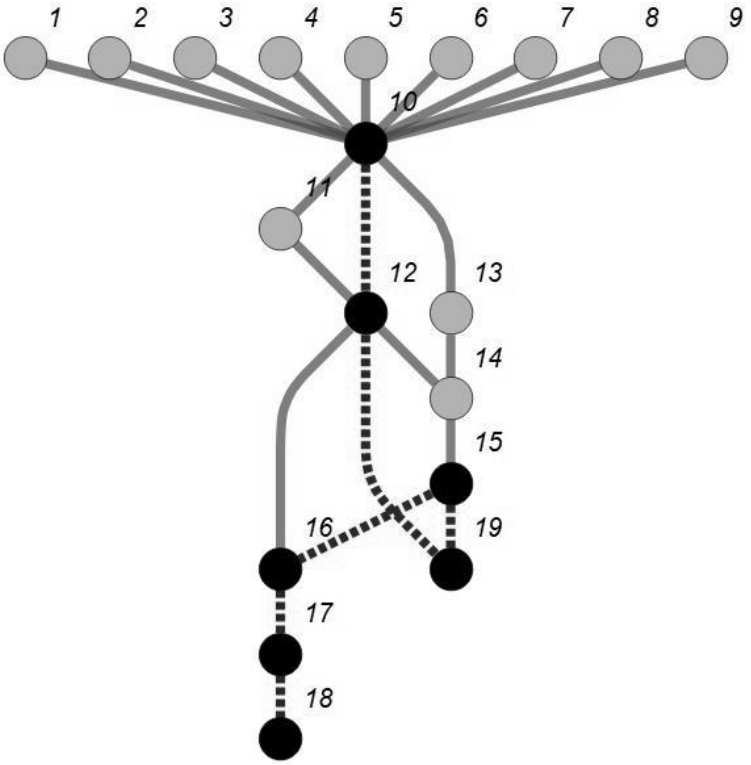


Рисунок К.3 – Общая составляющая наименее защищенных путей