# УПРАВЛЕНИЕ В СОЦИАЛЬНЫХ И ЭКОНОМИЧЕСКИХ СИСТЕМАХ

УДК 681.3

## ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ СОЦИАЛЬНОЙ ИНФРАСТРУКТУРЫ

***© 2021 Д. Е. Орлова***

*Воронежский институт высоких технологий (Воронеж, Россия)*

*Описывается модель угроз нарушения безопасности критически важных объектов социальной инфраструктуры. Определяются принципы обеспечения комплексной безопасности этих объектов. Выявляются особенности и локальные показатели качества управления комплексной безопасностью критически важных объектов социальной инфраструктуры.*

*Ключевые слова: модель угроз, комплексная безопасность, управление, показатель.*

**Введение.** Важность проблемы обеспечения безопасности критически важных объектов социальной инфраструктуры (КВОСИ) не вызывает сомнений [1]. Однако в настоящее время эта проблема приобретает особую значимость, что обусловлено, происходящим переоснащением КВОСИ средствами обеспечения безопасности. Силовые способы, сохраняя свою роль, уходят на второй план, а ведущее место начинают занимать электронные средства наблюдения, контроля, обеспечения охраны и жизнедеятельности, компьютерные комплексы и инфокоммуникационные сети, автоматизированные средства пожарной сигнализации и пожаротушения. В результате системы безопасности КВОСИ все в большей мере приобретают черты территориально распределенных человеко-машинных объектов, в которых возникают новые точки уязвимости. Этим обстоятельством незамедлительно воспользовались злоумышленники и преступные элементы. Уже сегодня они располагают достаточным арсеналом способов и средств преодоления барьеров безопасности КВОСИ, включая средства электронной и акустической разведки, мобильные средства связи и создания помех, средства взлома защитных ограждений, проникновения в компьютерные сети, огневого поражения систем охраны и жизнеобеспечения. В этом аспекте следует особо подчеркнуть, что преступники постоянно совершенствуют приемы, методы и средства деструктивных воздействий на компоненты системы обеспечения безопасности КВОСИ В результате управление этими системами все в большей мере приобретает форму антагонистического конфликта, для выигрыша в котором необходимо постоянное, комплексное и опережающее совершенствование систем управления безопасностью. Одним из таких направлений является повышение интеллектуального уровня управления путем разработки и внедрения компьютерных комплексов поддержки принятия решений при управлении безопасностью.

**Модель угроз нарушения безопасности критически важных объектов социальной инфраструктуры.** Перечень и содержание типовых угроз, которые должна предотвращать система комплексной безопасности этих объектов является важнейшей составляющей исходных данных для ее моделирования и оптимизации. Анализ источников [3-5] позволил установить, что к наиболее распространенным типам угроз нарушения безопасности КВОСИ следует отнести (рис. 1): 1) угрозы нарушения режима и охраны; 2) угрозы нарушения информационной безопасности; 3) угрозы нарушения пожарной безопасности; 4) угрозы нарушения безопасности жизнедеятельности.

Орлова Дарья Евгеньевна – Воронежский институт высоких технологий, аспирант, dasha_scorobogat@mail.ru.

*Угрозы нарушения режима и охраны* фиксируются в попытках открытого, силового преодоления охранной системы (при этом основными преимуществами являются внезапность и скорость его реализации) и скрытого преодоления охранной системы (максимально скрытая реализация негативного воздействия до момента его обнаружения элементами охранной системы). При этом наиболее распространенными являются: а) угрозы нарушения пропускного режима на подведомственных объектах; б) угрозы нарушения физической защиты от внешних источников опасности, связанных с возможностью совершения преступных актов, нападений, несанкционированных (незаконных) проникновений на территорию; в) угрозы нарушения режима допуска к объектам особой важности.

*Угрозы информационной безопасности* включают возможные действия злоумышленников (как внутри, так и вне охраняемых объектов), которые могут нанести ущерб информационным и компьютерным системам. К ним относятся: а) попытки нарушения работы телекоммуникационного оборудования, а так же работы систем контроля и видеонаблюдения; б) попытки взлома и блокирования компьютерных сетей; в) попытки несанкционированного использования средств мобильной связи. Помимо этого угрозы информационной безопасности связаны с несанкционированным доступом к категорированной информации.


Рисунок 1. Типы угроз нарушения безопасности критически важных объектов социальной инфраструктуры

*Угрозы нарушения пожарной безопасности* включают: а) угрозы поджога зданий и сооружений; б) угрозы поджога хранилищ ГСМ; в) угрозы поджога производственного, отопительного, газосварочного и иного пожароопасного оборудования. Анализ мате-

риалов служебных расследований по фактам зафиксированных в 2016-2020 годах пожаров показывает [3], что основными причинами их возникновения явились: нарушение правил устройства и эксплуатации электрооборудования (45,4 %), неосторожное обращение с огнем (12,1 %), поджоги (9,1 %), нарушение правил эксплуатации печного отопления (9,1 %). Объектами пожаров стали: административно-бытовые здания (24,2 %), жилые здания и помещения (15,1 %), производственные здания и сооружения (18,2 %), сельскохозяйственные объекты (12,1 %), складские и торговые помещения (6,1 %), прочие объекты (21,2 %).

*Угрозы нарушения безопасности жизнедеятельности* связаны, прежде всего, с посягательством на жизнь, здоровье и неприкосновенность личности сотрудников, рабочих и служащих. Эти угрозы можно сгруппировать следующим образом: а) угрозы, направленные на причинение физического вреда персоналу КВОСИ и их родственникам; б) угрозы связанные с экологическим состоянием учреждения (уровни нежелательных воздействий на человека различного рода потоков энергии (механической, электромагнитной, тепловой, ионизирующей), дозы, полученные человеком за время действия на него негативных техногенных факторов (ионизирующих, электромагнитных и др.); концентрации нежелательных для человека токсических и загрязняющих химических веществ; объемы выбросов в атмосферу и сбросов в гидросферу нежелательных для человека токсических и (или) загрязняющих химических веществ); в) угрозы, связанные с нарушениями эксплуатации инженерных сооружений, норм гигиены, питания и оказания медицинской помощи.

**Принципы обеспечения комплексной безопасности критически важных объектов социальной инфраструктуры,** установленные на основе анализа и обобщения, ранее выполненных исследований [6], состоят в следующем:

*Принцип системности,* предусматривающий обеспечение целостности, единства, совместимости и увязки всех компонентов системы обеспечения безопасности, а также возможность ее адаптации к изменениям внешних условий, в том числе к изменениям конфигурации защищаемых объектов и способам преодоления барьеров безопасности, используемыми злоумышленниками.

*Принцип непрерывности* – осуществление мер по обеспечению безопасности должно быть основано на постоянной готовности к отражению как внутренних, так и внешних угроз безопасности. При этом руководители всех уровней должны ясно осознавать: процесс обеспечения безопасности не допускает перерывов, иначе придется все начинать сначала.

*Принцип комплексности* предполагает учет всех факторов, влияющих на безопасность. К числу таких факторов, прежде всего, относят: экономические факторы, связанные с материальной и финансовой обеспеченностью процесса развития системы обеспечения безопасности и ее технического переоснащения; технологические факторы, связанные с соответствием технологий обеспечения безопасности уровню угроз со стороны злоумышленников и преступных элементов; социальные факторы (условия работы сотрудников; качество предоставления социальных гарантий; уровень зарплаты персонала; текучесть кадров и др.).

*Принцип своевременности* предусматривает обеспечение безопасности с использованием упреждающих мер. При этом принцип своевременности предполагает постановку задач по обеспечению безопасности на ранних стадиях формирования системы, а также разработку эффективных мер предупреждения действий злоумышленников и преступных элементов.

*Принцип законности* – обеспечение безопасности на основе законодательства РФ и других нормативных актов, утвержденных органами государственного управления в пределах их компетенции.

*Принцип активности* предполагает обеспечение безопасности с достаточной степенью настойчивости и с широким использованием маневра имеющихся сил и средств.

*Принцип универсальности* предусматривает обеспечение безопасности посредством применения таких мер и проведения таких мероприятий, которые дают положительный эффект независимо от места их конкретного применения.

*Принцип экономической целесообразности* предполагает сопоставление возможного ущерба и затрат на обеспечение безопасности. При этом во всех случаях стоимость системы безопасности не должна превышать размера возможного ущерба от любых видов риска.

*Принцип конкретности и надежности* предусматривает определение конкретных видов ресурсов, выделяемых на обеспечение безопасности. При этом на каждое действие злоумышленников и преступных элементов в системе обеспечения безопасности должны быть предусмотрены меры пресечения этих действий.

*Принцип профессионализма* предполагает реализацию мер безопасности только профессионально подготовленными специалистами. При этом в условиях быстрого развития средств и систем безопасности необходимо постоянное совершенствование мер и средств защиты на базе обучения личного состава.

*Принцип взаимодействия и координации* – предусматривает осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений, служб и ответственных лиц. При этом вопрос о взаимодействии и координации касается не только подразделений и лиц, непосредственно отвечающих за безопасность, но и их связи с остальными подразделениями организации.

*Принцип оптимального сочетания централизации управления и автономности* предполагает обеспечение организационно-функциональной самостоятельности процесса организации защиты всех объектов охраны и централизованное управление обеспечением безопасности в целом.

С целью реализации указанных принципов в составе КВОСИ создаются организационно-технические системы обеспечения безопасности, решающие следующие типовые задачи:

1) организация и проведения профилактических мер по обеспечению безопасности объекта;

2) защита охраняемых объектов от возможных опасностей как внешнего, так и внутреннего характера;

3) обеспечение противопожарной и информационной безопасности объекта, а также безопасности жизнедеятельности персонала, включая устранение явных опасностей в экстренных случаях (например, пресечение вооруженных нападений на персонал объекта);

4) обеспечение контроля работы всех служб, обеспечивающих безопасность объекта;

**Состав, типовая схема и особенности управления комплексной безопасностью критически важных объектов социальной инфраструктуры.** Для реализации своего предназначения перспективная система обеспечения комплексной безопасности КВОСИ должна включать в себя совокупность следующих функциональных подсистем (рис. 2): подсистему обеспечения безопасности охраны и режима; подсистему обеспечения пожарной безопасности; подсистему обеспечения информационной безопасности; подсистему обеспечения безопасности жизнедеятельности (включая безопасность инженерных сооружений, здоровья и жизни людей).

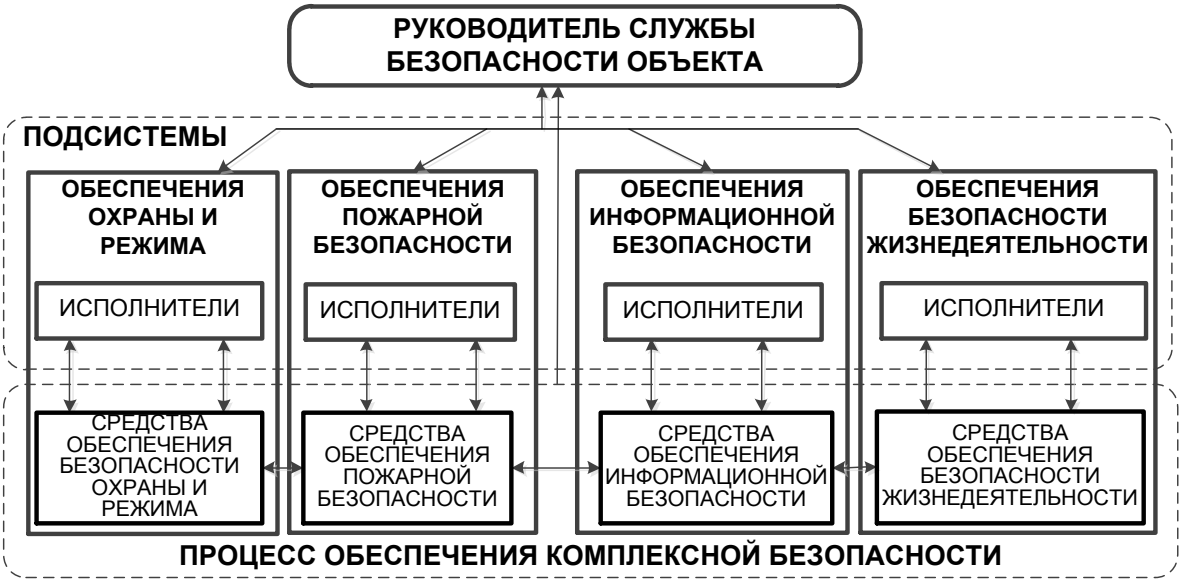


Рисунок 2. Типовая схема управления комплексной безопасностью критически важных объектов социальной инфраструктуры

Каждая подсистема осуществляет управление своими процессами обеспечения безопасности по следующим локальным показателям. *Показатели безопасности режима и охраны:*

- уровень охраны территорий и помещений от несанкционированного проникновения, в том числе с использованием дистанционно-пилотируемых летательных аппаратов;
- уровень личной безопасности сотрудников объекта, включая сотрудников службы безопасности;
- уровень контроля режима секретности и допуска;
- уровень контроля радиочастотного спектра в зоне объекта и возможность пресечения несанкционированной работы мобильных средств связи;
- своевременность реагирования и пресечения нарушений режима и охраны злоумышленниками.

*Показатели пожарной безопасности:*

- уровень защиты от возгорания заранее припасенными средствами и средствами, находившимися на месте поджога;
- уровень защиты от поджогов с помощью дистанционных приспособлений и устройств;
- уровень защищенности от самовозгорающихся средств;
- уровень защиты от распространения пожара на примыкающие территории, здания и сооружения;
- уровень организации и управления пожарной безопасностью;
- уровень подготовки личного состава к действиям на пожаре;
- своевременность выявления и ликвидации пожаров.

*Показатели информационной безопасности:*

- уровень защищенности систем управления базами данных (СУБД);
- уровень защищенности операционных систем (ОС);
- уровень защищенности сетевого программного обеспечения (СПО);
- уровень криптозащиты информации;
- уровень надежности разграничения доступа;
- уровень защищенности объектов от средств криминальной технической разведки;
- своевременность выявления кибератак и ликвидации их последствий.

*Показатели безопасности жизнедеятельности:*

- уровень защищенности личного состава от применения химических отравляющих веществ и средств ошеломляющего действия;
- уровень защищенности инженерных сооружений;
- уровень организации медицинской помощи в случае возникновения критических ситуаций;
- уровень организации мероприятий по эвакуации личного состава;
- своевременность выявления и ликвидации критических ситуаций, связанных с опасностью жизнедеятельности. Функционирование системы обеспечения комплексной безопасности КВОСИ представляется следующим образом. Руководитель службы безопасности, имея информацию о текущем рассогласовании локальных процессов, стремится минимизировать отклонение всего процесса обеспечения безопасности от требуемого уровня. При этом он основывается не на всей информации о состоянии локальных процессов, а только на той его части, которая отражает возникающие рассогласования между ними. Кроме того, руководитель службы безопасности, как правило, не воздействует непосредственно на локальные процессы обеспечения безопасности, а управляет ими опосредованно, путем координирующих и согласующих указаний. Принципиальным качеством такого управления является определенная свобода в выборе подчиненными своего поведения, трактуемая, например, как возможность выработки управлений исходя из собственного видения ситуации. Кроме того, они могут самостоятельно формировать цели своего поведения и выбирать критерии принятия локальных управленческих решений, которые в общем случае могут не совпадать с глобальной целью системы и даже ей противоречить.

Эти конфликты можно ликвидировать, возложив все функции по управлению безопасностью учреждения на себя руководителя, превратив подчиненных в исполнителей, которые беспрекословно выполняют указания начальника и фактически не участвуют в процессах управления безопасностью учреждения. Так обычно и поступают в критических ситуациях, однако типовым является режим, когда в контур управления комплексной безопасностью включаются как и руководитель, выполняющий функции координатора, так и подчиненные, непосред-

ственно управляющие локальными процессами обеспечения безопасности.

Включение подчиненных в общий цикл управления безопасностью учреждения означает расчленение общей задачи управления на два взаимосвязанных класса: задачи, решаемые исполнителями, и задачи, решаемые руководителем. Задачи, решаемые исполнителями, сводятся к тому, чтобы при фиксированных координирующих воздействиях со стороны руководителя, минимизировать отклонения своих локальных процессов от заданных целевых состояний. Задача руководителя будет заключаться в том, чтобы на основании информации о характере рассогласования локальных процессов выработать решение и довести до исполнителей такие координирующие воздействия, которые помогут им вырабатывать локальные управления, отвечающие не только собственным интересам, но и интересам системы.

Субъектами обеспечения безопасности являются: служба охраны объекта, обеспечивая защиту от внешних угроз (нападений на объект, диверсий и т. д.); служба информационной безопасности объекта, обеспечивающая предупреждение и пресечение противоправных действий в сфере IT-технологий;

− служба противопожарной и противохимической безопасности объекта; инженерная служба объекта, обеспечивающая безопасность зданий и сооружений, а также систем водоснабжения, электроснабжения, газоснабжения, теплоснабжения, транспорта и средств производственной деятельности на территории объекта; медицинская служба объекта, обеспечивающая оказание экстренной медицинской помощи в случае критических ситуаций; отряды специального назначения территориальных органов МВД и ФСБ России, а также подразделения МЧС России, службы санэпиднадзора и др.

К наиболее распространенными техническими средствами и комплексами обеспечивающими безопасность охраны и режима, пожарной безопасности и безопасности жизнедеятельности КВОСИ относятся: ИКБ «Пахра» (производитель – ГК «АСБ»); ИКБ «Тобол» (производитель – ФГУП «СНПО «Элерон»); ИКБ «Орион» (производитель – НВП «Болид»); ИСБ «Рубеж-08,09» (производитель – «Сигма»); ИСБ «Микрос» (производитель – АО «Микрос»); ИКБ «Кодос» (производитель – АО «Бауманн»); «Синергет-КСБО» (производитель – «Стилсофт»).

Информационная безопасность КВОСИ обеспечивается встроенными аппаратно-программными средствами защиты и организационно-техническими мероприятиями, реализующими безопасные технологии обработки информации.

Аппаратно-программные средства защиты реализуют следующие функции: защиту информации от несанкционированного доступа (НСД); криптографическую защиту данных, передаваемых по каналам связи; контроль целостности и подлинности электронных документов; безопасность межсетевого взаимодействия; антивирусную защиту.

Функция защиты информации от НСД реализуется системой защиты типа *Secret Net*, обеспечивающей индивидуальную идентификацию и аутентификацию пользователей, и разграничение доступа пользователей к ресурсам. Для обеспечения защиты серверов и рабочих станций от проникновения посторонних пользователей, несанкционированной загрузки операционной системы с дискет и компакт-дисков, а также для организации контроля целостности файлов на накопителях жёстких магнитных дисках применяются программно-аппаратный комплексы типа «Соболь PCI».

Функция криптографической защиты конфиденциальных данных, передаваемых по каналам связи, реализуется путем применения аппаратно-программных комплексов шифрования типа «Континент-К».

Функция безопасности межсетевого взаимодействия реализуется при помощи межсетевых экранов типа *Fortinet FortiGate 100E* или *Dionis DPS*, устанавливаемых в локальной вычислительной сети (ЛВС) для обеспечения защиты и контроля информационных потоков к серверам сертификации и регистрации, серверному оборудованию, АРМ привилегированных пользователей, серверу электронной почты, а также для обеспечения безопасного информационного обмена с взаимодействующими системами.

Для выявления и своевременного предотвращения нежелательных информационных воздействий со стороны хакеров используются системы обнаружения атак типа *Real Secure Network* (*Server*) *Sensor* или *Black ICE Agent*, обеспечивающие обнаружение как внешних атак, так и внутренних злоупотреблений, направленных на серверы приложений, Web-серверы, БД, АРМ, маршрутизаторы.

Функция антивирусной защиты реализуется программными средствами комплексной системы антивирусной защиты типа *McAfee, Norton, Kaspersky*.

Типовой состав технических средств обеспечения безопасности КВОСИ показан на рисунке 3.

Особое место в этой структуре занимает Центр интеграции, обеспечивающий: 1) сбор, обработку и отображение информации о текущем состоянии безопасности объекта; 2) контроль состояния технических средств охраны и надзора; 3) контроль и управление доступом на территорию объекта и локальные участки; 4) оповещение лиц, находящихся на объекте охраны, при помощи речевых, звуковых и световых оповещателей; 5) анализ информации и проведение аналитических расчетов по прогнозированию ситуаций безопасности, оценке рисков нарушения безопасности и возможных последствий; 6) координацию деятельности подчиненных в ходе решения ими функциональных задач по обеспечению безопасности объекта и контроль функционирования локальных подсистем; 7) формирование оперативных донесений в территориальные органы государственной власти; 9) информационное взаимодействие с территориальными органами МВД, МЧС и ФСБ.


Рисунок 3. Типовой состав технических средств обеспечения безопасности критически важных объектов социальной инфраструктуры

В целом можно утверждать, что имеющаяся номенклатура технических средств способна при правильном комплексировании и рациональном управлении обеспечить безопасность КВОСИ от всего спектра угроз со стороны злоумышленников и преступных элементов.

**Заключение.** Безопасность критически важных объектов социальной инфраструктуры представляет собой комплексную категорию, включающую: безопасность режима и охраны, пожарную безопасность, информационную безопасность, безопасность жизнедеятельности (в т. ч. безопасность инженерных сооружений, здоровья и жизни людей). При этом каждый из локальных аспектов безопасности реализуется соответствующей функциональной подсистемой, представляющей собой комплекс разнородных технических, информационных, интеллектуальных, программных и лингвистических средств. Эти подсистемы, обла-

дая определенной автономностью, оказываются связанными между собой, через людские, технические, информационные и иные ресурсы. В результате управление приобретает не только многоаспектный (многокритериальный), но и иерархический характер, вынуждающий учитывать как глобальные интересы всей системы, так и локальные интересы ее функциональных подсистем. Сказанное обусловливает необходимость оснащения критически важных объектов социальной инфраструктуры программно-математическими средствами поддержки принятия управленческих решений с учетом таких аспектов как многослойный иерархический характер объектов управления с наличием как внутренних, так и внешних взаимосвязей зачастую конфликтного характера [7].

**ЛИТЕРАТУРА**

1. Федеральный закон РФ от 26.07.2017 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ, 31.07.2017, N 31 (Часть I).

2. Распоряжение Правительства РФ от 14.10.2010 № 1772-р «О Концепции развития уголовно-исполнительной системы Российской Федерации до 2020 года» // Собрание законодательства РФ, 25.10.2010, № 43, ст. 5544. С изм. и доп. в ред. от 31.05.2012.

3. Измалков А. В. Управление безопасностью социально-экономических систем и оценка его эффективности / А. В. Измалков. – М.: Спутник+, 2003. – 441 с.

4. Вишняков С. М. К вопросу технического регулирования систем безопасности функционально опасных объектов / С. М. Вишняков // Системы безопасности. – 2007. – № 2. – С. 134-136.

5. Ворона В. А. Комплексные (интегрированные) системы обеспечения безопасности / В. А. Ворона, В. А. Тихонов. – М.: Горячая линия-Телеком, 2013. – 160 с.

6. Заключительный отчет по НИР № 13-2015 «Исследование вариантов создания программно-аппаратного комплекса «Интегрированная система безопасности ФСИН России». ФКУ НИИИТ ФСИН России, Тверь, 2015.

7. Орлова Д. Е. Комплекс программ для решения задач моделирования, оптимизации и оценки устойчивости комплексной безопасности объектов критического применения / Д. Е. Орлова // Моделирование, оптимизация и информационные технологии. – Т. 8. – № 1 (28). – 2020.

## PRINCIPLES OF BUILDING ADVANCED SECURITY SYSTEMS FOR CRITICAL SOCIAL INFRASTRUCTURE FACILITIES

***© 2021 D.E. Orlova***

*Voronezh Institute of High Technologies (Voronezh, Russia)*

*The model of threats to the security of critical social infrastructure objects is described. The principles of ensuring the comprehensive security of these objects are defined. The features and local indicators of the quality of integrated security management of critical social infrastructure facilities are identified.*

*Keywords: threat model, integrated security, management, indicator.*