Ветрова Ю.В., канд. техн. наук, доц.,
Васюткина Д.И., асс.,
Нестерова Н.В., д-р техн. наук, проф.
Белгородский государственный технологический университет имени В.Г. Шухова

ПУНКТЫ УПРАВЛЕНИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

zchs@intbel.ru

Перспективным направлением повышения безопасности образовательных учреждений высшего профессионального образования является оснащение зданий системами управления, которые осуществляют качественное оперативное управление безопасностью. В статье рассматриваются вопросы размещения и техническому оснащению пунктов управления систем обеспечения безопасности высших учебных заведений.

Ключевые слова: *безопасность, система безопасности, угроза, риск, оперативное управление, пункт управления, автоматизированное рабочее место.*

Введение. Для обеспечения безопасности объекта защиты осуществляется комплекс системных мер и мероприятий по защите от наиболее вероятных угроз, риск проявления которых оценивается как наиболее высокий [1]. Система безопасности представляет собой совокупность технических средств и систем, обеспечивающих безопасность от предполагаемых угроз внешнего и внутреннего характера. Важную роль в формировании системы безопасности играет определение перечня возможных угроз для объекта безопасности, модели нарушителя и тактики его возможных действий [2].

Комплексная система защиты объекта, структура которой в общем случае в равной степени применима для любых объектов, включает в себя [3]:

– систему управления и контроля доступа;
– систему охранной сигнализации;
– систему пожарной сигнализации;
– систему видеонаблюдения;
– систему защиты информации;
– систему жизнеобеспечения;
– персонал службы безопасности;
– спецсредства досмотра, отражения и ликвидации угроз и их последствий;
– процедурные средства;
– систему оперативной громкоговорящей связи;
– элементы строительных конструкций;
– инженерные средства защиты.

Основная часть. Наличие в высших учебных заведениях современных информационных и компьютерных технологий, позволяют осуществлять качественное оперативное управление безопасностью. К оперативному управлению относятся все вопросы управления текущим процессом функционирования системы безопасности ВУЗа [4].

Создание автоматизированных систем управления безопасностью или, другими словами, интегрированных систем безопасности и жизнеобеспечения являются в настоящее время актуальной задачей. Эти системы предназначены для оперативного управления процессами предотвращения пожаров и взрывов, противопожарной защиты; для исключения несанкционированного доступа персонала и посетителей на территорию; для предотвращения злоумышленных нарушений персоналом установленного порядка работы в особо важных зонах; для предотвращения хищений; для обнаружения попыток проникновения на территорию ВУЗа нарушителей; для противодействия несанкционированному получению, искажению или уничтожению злоумышленниками конфиденциальной информации; для контроля и поддержания нормального режима снабжения ВУЗа электроэнергией, освещением, чистым воздухом, а также контроля теплоснабжения, водоснабжения, радиационной, химической обстановки и лифтового оборудования; для реализации мер по снижению вероятности проведения злоумышленниками акций, ведущих к аварийным и чрезвычайным ситуациям; для предупреждения и ликвидации чрезвычайных ситуаций природного и техногенного характера для предупреждения и ликвидации криминальных и террористических акций и других возникающих задач защиты ВУЗа? а также для мониторинга состояния средств обеспечения безопасности [5].

Обычно в состав подобных систем оценки состояния средств обеспечения безопасности и принятия оперативных решений должны входить [6]:

1. Источники информации

К ним относятся:

- информация датчиков пожарной сигнализации;

- информация датчиков охранной сигнализации;
- информация системы видеонаблюдения;
- информация системы жизнеобеспечения;
- информация системы управления и контроля доступа;
- информация состояния системы оповещения, оперативной и громкоговорящей связи;
- информация состояния инженерных средств защиты;
- информация состояния элементов строительных конструкций;
- информация от ЕДДС города (населенного пункта), МВД, ФСБ о криминальных и террористических акциях.

2. Пункты сбора и хранения информации и управляющие центры – пункты управления

Управляющие центры – пункты управления предназначены для сбора, хранения и выдачи информации на центральный пункт управления от систем пожарной сигнализации, видеонаблюдения, технических средств охраны.

Система пожарной сигнализации предназначена для обнаружения возгорания, сопровождающегося повышенной температурой или выделением дыма, сбора, обработки и передачи информации в центральный пункт управления.

Система охранной сигнализации предназначена для обнаружения в период охраны попыток проникновения на объект или совершение краж материальных ценностей, сбора, обработки и передачи информации в центральный пункт управления.

Система видеонаблюдения предназначена для ведения дистанционного визуального контроля за ситуацией на участках охраняемой территории, архивации информации и передачи сигналов на центральный пункт управления в случае обнаружения нарушений.

3. Центральный пункт управления

Центральный пункт управления концентрирует всю полученную информацию, проводит ее оперативный анализ и осуществляет предварительное распределение информации между подчиненными ему управляющими центрами и потребителями информации для принятия экстренных мер по ликвидации возгораний; несанкционированного доступа; аварий в системах жизнеобеспечения; отклонений в состоянии инженерных средств защиты, элементов строительных конструкций зданий и сооружений; предупреждению и ликвидации чрезвычайных и кризисных ситуаций.

4. Потребители информации – комплекс экстренных мер с использованием технических средств, которые ликвидируют чрезвычайную или кризисную ситуацию, возгорания, аварии, поломки, неисправности и т.д.

Пункты управления системами обеспечения безопасности предназначены для вывода оперативной и справочной информации о состоянии всех элементов систем обеспечения безопасности объекта или его автономных комплексов и вводе команд управления, а также документирования циркулирующих сообщений и выполняемых действий.

Места расположения центрального и локальных пунктов управления должны быть определены с учетом структуры и назначения зданий и сооружений ВУЗа, расположения выделяемых зон доступа и деления на пожарные отсеки.

Для обеспечения работоспособности системы в условиях реализации проектной угрозы, а также при выводе из строя центрального пункта управления, целесообразно создавать локальные и резервные пункты управления. Резервные пункты управления предназначены для централизованного управления всеми составными частями системы обеспечения безопасности и используются в составе центров управления в кризисных ситуациях, которые могут размещаться [7]:

– на пункте управления системой противопожарной защиты;

– на центральном пункте диспетчерской службы эксплуатации здания.

Для обеспечения функционирования отдельных зданий, зон доступа, функциональных блоков и т.п. при реализации проектных угроз, а также при выводе из строя каналов связи или нарушении работоспособности устройств управления выше стоящего уровня, в составе системы обеспечения безопасности должны предусматриваться локальные пункты управления.

Вся информация с локальных пунктов управления должна дублироваться на центральном пункте управления.

На пункты управления должна поступать и отображаться необходимая и достаточная информация, позволяющая дежурному оператору однозначно оценить обстановку и принять правильное решение, а также оперативно управлять процессами происходящими в системе обеспечения безопасности объекта.

Пункты управления должны обеспечивать [8]:

– защиту от несанкционированного доступа к оборудованию и предоставляемой информации в соответствии с требованиями нормативных документов по защите информации;

– документирование фактов всех действий оператора (в том числе передача/прием смены);

– возможность тестирования оборудования без нарушения работоспособности комплекса или отдельных его элементов;

– необходимое дублирование и резервирование применяемого оборудования;

– контроль работоспособности и жизнедеятельности оператора.

В случае отсутствия подтверждения жизнедеятельности или работоспособности оператора должны отключаться устройства отображения и пульты управления подсистемами и элементами до момента регистрации нового оператора, имеющего полномочия на выполнение соответствующих функций, а данные события регистрироваться и передаваться ответственному дежурному службы безопасности.

Пункты управления должны размещаться в зонах ограниченного доступа, расположенных в соответствующих охраняемых зонах в специально приспособленных для этого помещениях, имеющих пуленепробиваемые двери и стекла и соответствующую организацию контроля доступа.

Оборудование центрального пункта управления должно обеспечивать:

– представление оператору поступающей информации о несанкционированном проникновении нарушителей в охраняемые зоны (помещения) в реальных буквенно-цифровых координатах объекта;

– контроль состояния средств системы обеспечения безопасности;

– формирование звукового сигнала при изменении состояния контролируемых средств и устройств;

– сигнализацию об отказах и неисправностях аппаратуры системы;

– автоматический и ручной дистанционный контроль работоспособности подключенных средств обнаружения;

– регистрацию действий оператора по обработке сигналов и управлению системами;

– возможность тестирования аппаратуры в автоматическом режиме и по запросам оператора;

– предотвращение несанкционированного доступа к программным средствам и базам данных;

– сохранение вводимых данных параметрирования центральной аппаратуры при отключении напряжения электропитания;

– регистрацию времени поступления сигналов срабатывания средств обнаружения и обработки их оператором.

Помещение центрального пункта управления должно быть оборудовано:

– техническими средствами управления СУЭВ при чрезвычайных ситуациях;

– аппаратурой управления и видеоконтрольными устройствами (мониторами) системы охранного телевидения и контроля доступа;

– коммутатором прямой телефонной связи;

– средствами дублированной связи с ответственным дежурным службы безопасности и МЧС России, телефонной связи - с территориальными органами МВД России.

Автоматизированное рабочее место оперативного дежурного (оператора) должно позволять оператору осуществлять [9]:

– сбор, систематизацию, контроль и анализ всей получаемой от периферийных элементов комплекса информации о состоянии защиты ВУЗа;

– контроль работоспособности (текущего технического состояния) периферийных элементов системы обеспечения безопасности ВУЗа и линий связи;

– формирование и передачу сообщений (команд) подсистемам охраны и реагирования;

– выработку управляющих воздействий на системы безопасности.

Автоматизированное рабочее место администратора безопасности должно позволять ему входить в систему по индивидуальному для каждого администратора паролю (с регистрацией входа и выполненных операций в системном журнале) и обеспечивать выполнение следующих функций:

– проводить инсталляцию и переинсталляцию программного обеспечения комплекса, а также восстановление его работоспособности после сбоев и аварий на основе сохраненной дежурным администратором безопасности информации;

– проводить конфигурирование и переконфигурирование комплекса;

– формировать, устанавливать и изменять сценарии работы комплекса в соответствии с оперативной обстановкой;

– устанавливать и контролировать пароли и уровень доступа пользователей к комплексу, их полномочия по работе в системе;

– устанавливать и контролировать уровень доступа пользователей к информационным базам комплекса с ограниченным уровнем распространения;

– проводить детальную диагностику неисправностей и отказов программной части комплекса;

– проводить анализ работоспособности аппаратной и программной частей комплекса на

основе обобщения информации, получаемой со всех автоматизированных рабочих мест и пультов интегрированного комплекса, а также информации системного журнала;

– просматривать, выбирать и документировать протоколы работы, базы данных системы и системный журнал - печатать на принтер или записывать в файл в формате, доступном для экспорта в стандартные приложения Windows;

– формировать и обмениваться с другими пультами и автоматизированными рабочими местами интегрированного комплекса необходимыми служебными сообщениями.

Вывод. Таким образом, следует принимать во внимание, что в связи с широким использованием современных электронных компонентов и цифровых методов обработки информации в настоящее время происходит существенная "интеллектуализация" систем защиты объектов, объединение технических средств в интегрированные комплексы. Внедрение систем оперативного управления позволяет минимизировать затраты на достижение социального и экономического эффектов при осуществлении планируемых мероприятий по обеспечению безопасности высших учебных заведений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Шаптала В.Г., Радоуцкий В.Ю., Ветрова Ю.В. Система управления рисками чрезвычайных ситуаций: монография. Белгород: ООО "Евро-Полиграф", 2010. 164с.

2. Радоуцкий В.Ю., Шаптала В.Г. Характеристика внутренних опасностей и угроз образовательных учреждений высшего профессионального образования // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2009. №3. С. 124-126.

3. Радоуцкий В.Ю., Ветрова Ю.В., Васюткина Д.И. Обоснование состава системы управления комплексной безопасностью высшего учебного заведения // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2014. №3. С. 210-214.

4. Шаптала В.Г., Радоуцкий В.Ю. Система информационного обеспечения прогнозирования чрезвычайных ситуаций в образовательных учреждениях высшего профессионального образования // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2009. №3. С. 130-131.

5. Радоуцкий В.Ю., Шаптала В.Г., Ветрова Ю.В. Управление комплексной безопасностью высших учебных заведений: монография. Белгород: Изд-во БГТУ, 2013. 125с.

6. Гревцев М.В., Радоуцкий В.Ю. Интегрированные системы безопасности и жизнеобеспечения высших учебных заведений // Инновационный вектор развития науки: Сборник статей Международной научно-практической конференции. Уфа. 2014. С. 13-17.

7. Шаптала В.Г., Радоуцкий В.Ю., Ветрова Ю.В. Мониторинг, прогнозирование, моделирование и оценка рисков чрезвычайных ситуаций в системе высшего профессионального образования: монография. Белгород: ООО "Евро-Полиграф", 2012. 120с.

8. Васюткина Д.И., Радоуцкий В.Ю. Система управления комплексной безопасностью образовательных учреждений высшего профессионального образования // Современные подходы к трансформации концепций государственного регулирования и управления в социально-экономических системах: Материалы 3-й Международной научно-практической конференции. Юго-Западный государственный университет РГП на ПХВ «Северо-Казахстанский государственный университет им. М. Козыбаева», Харьковский автомобильно-дорожный национальный университет, Ставропольский государственный аграрный университет. 2014. С. 76-81.

9. Радоуцкий В.Ю., Шаптала В.Г., Васюткина Д.И. Математические методы анализа эффективности систем обеспечения комплексной безопасности образовательных учреждений // Эволюция научной мысли: Сборник статей Международной научно-практической конференции. Уфа. 2014. С. 183-187.