обследование объектов при поступлении информации о минировании объекта специальными подразделениями;

осуществление осмотра места происшествия следственно-оперативной группой на труднодоступных и небезопасных участках местности;

оказание помощи подразделениям криминальной милиции по поиску исчезнувших лиц;

наблюдение за дорожной обстановкой совместно с экипажами подразделений ГАИ.

УДК 351.75

Л.В. Степанов, А.Ю. Сальникова

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Безопасность – это широко используемое понятие, включающее в себя такие области, как физическая безопасность людей и окружающей среды, информационная безопасность и безопасность в компьютерных сетях. В каждом из этих контекстов безопасность имеет разные аспекты и требует соответствующих мероприятий для обеспечения. Под безопасностью понимают состояние защищенности человека или инженерно-технической и программной инфраструктуры от возможных опасностей и их сочетания путем установления в отношении системы заданных параметров функционирования, а также минимизации опасностей, исходящих от человека и самой системы.

Рассмотрение вопросов безопасности предполагает определение объекта защиты и выявление всех вероятных угроз безопасности его структуре или процессу функционирования. На следующем этапе необходимо определить те или иные направления и средства обеспечения безопасности объекта. При этом существенное влияние имеют особенности данного объекта защиты.

Отличительные особенности предприятий и учреждений позволяют выделить следующие объекты обеспечения безопасности:

безопасность сотрудников и учреждений, включая их жизнь и здоровье;

безопасность посетителей, включая их жизнь и здоровье;

безопасность предприятий и учреждений в целом, а также безопасность производства и порядка функционирования.

Каждый из перечисленных объектов обеспечения безопасности должен находиться под постоянной защитой.

Под обеспечением безопасности следует понимать планирование и осуществление системы правовых, организационных, режимных, оперативных, профилактических, материально-технических, коммунально-бытовых и иных мероприятий, направленных на обеспечение защищенности учреждений и сотрудников от воздействий, понижающих режим безопасности.

Составляющие безопасности включают в себя различные виды мероприятий и действий, направленных на ее обеспечение. Они могут быть предотвращающими, реактивными или непосредственными действиями, а также могут включать использование различных технологий и методов.

Одной из главных составляющих безопасности является физическая безопасность, которая относится к мерам, направленным на предотвращение угроз физических повреждений людей и ущерба материальным ценностям, и включает в себя использование видеонаблюдения, охранной сигнализации, контроля доступа и даже физической охраны.

Еще одной составляющей безопасности является информационная безопасность, которая связана с защитой конфиденциальной, ценной информации от несанкционированного доступа, использования или распространения. Для обеспечения информационной безопасности могут применяться такие меры, как шифрование данных, использование паролей и биометрических идентификаторов, межсетевые экраны и антивирусное программное обеспечение. Злоумышленники в своей деструктивной деятельности руководствуются собственными целями, как правило, ориентированными на дестабилизацию информационного поля и нанесение репутационных потерь.

Для обеспечения безопасности существует широкий спектр технических средств, которые могут быть классифицированы по назначению и области применения.

К средствам физической безопасности относятся:

системы видеонаблюдения (камеры, обеспечивающие мониторинг территорий, как стационарные, так и мобильные) могут быть оснащены функциями ночной съемки и распознавания лиц;

комплексы охранной сигнализации (датчики движения, двери и окна с автоматическим оповещением о несанкционированном доступе) могут быть интегрированы с мобильными приложениями для удаленного контроля;

системы контроля и управления доступом (электронные замки и системы идентификации по отпечаткам пальцев или картам), позволяющие ограничить доступ только авторизованным пользователям;

биометрическая идентификация (отпечатки пальцев, распознавание лиц, радужная оболочка глаза, голос и другие физиологические или по-

веденческие признаки), позволяющая устанавливать и подтверждать личность человека на основе его уникальных биометрических характеристик.

К системам информационной безопасности относятся:

антивирусные программы и межсетевые экраны, способствующие предотвращению несанкционированный доступ к данным и защищающие информацию от киберугроз;

системы обнаружения и предотвращения вторжений (мониторинг сетевого трафика для выявления и блокировки подозрительных действий);

шифрование данных (инструменты для защиты информации при передаче и хранении).

Эти средства в комплексе создают надежную защиту, минимизируя риски и предотвращая инциденты безопасности.

УДК 004.05

Л.В. Степанов, Н.П. Сергеев

АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ И ТЕХНОЛОГИЙ

В настоящее время существует тенденция проникновения современных информационных технологий во все сферы деятельности человека, включая критически важные силовые блоки, такие как уголовно-исполнительная система России (УИС). Вместе с этим появляется проблема обеспечения безопасности функционирования исправительных учреждений и систем контроля, предотвращения утечек конфиденциальных данных и защиты информации особой важности. Постоянно нарастающая угроза реализации злоумышленниками кибератак на критически важные элементы информационного пространства УИС делает вопросы безопасности крайне актуальными и первостепенными. Данная проблема требует от системы постоянного мониторинга, своевременного оперативного реагирования на угрозы и инциденты, а также внедрения современных технологий в сфере защиты информации.

Направление информационной безопасности (далее – ИБ) является важнейшим вектором в обеспечении общей безопасности УИС. Он направлен на защиту конфиденциальной информации, предотвращение несанкционированного доступа злоумышленников к важным секторам и минимизацию рисков, связанных с киберугрозами и инсайдерскими действиями. Методы и технологии, применяемые для защиты инфор-