Министерство внутренних дел Российской Федерации
Главное управление вневедомственной охраны

УТВЕРЖДЕНО

на заседании научно-практической секции ГУВО МВД России, протокол №13 от 24 декабря 2013 г.

РЕКОМЕНДАЦИИ по организации комплексной централизованной охраны банковских устройств самообслуживания

Р 78.36.035–2013

Москва, 2014

Методические рекомендации разработаны сотрудниками ФКУ НИЦ «Охрана» МВД России: А.А. Никитиным, Н.В. Малёминым, А.В. Климовым, В.А. Николаевым, В.С. Радченко, В.А. Козловым под руководством. А.Г. Зайцева при участии сотрудников ГУВО МВД России Ю.Н. Зуйкова, М.Н. Жирикова, Д.И. Макарова.

Рекомендации по организации комплексной централизованной охраны банковских устройств самообслуживания (Р 78.36.035–2013) - М.: НИЦ «Охрана», 2012. – 203 с.

В настоящих Рекомендациях отражены основные технические и методические аспекты обеспечения комплексной централизованной охраны банковских устройств самообслуживания, отражены положения законодательства Российской Федерации в данной сфере, нормативных правовых документов МВД России и Банка России, рекомендаций Ассоциации российских банков, а также национальных, европейских и международных стандартов, учтен опыт организации централизованной охраны банкоматов подразделениями вневедомственной охраны МВД России в различных регионах Российской Федерации, использованы данные о новейших разработках в области технических средств охранной сигнализации и противокриминальной защиты.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Как показывает статистика имущественных преступлений в банковской сфере на территории Российской Федерации, наряду с активным и повсеместным развитием системы дистанционного банковского обслуживания, национальной платежной системы, дистанционной оплаты коммунальных и других услуг с помощью банковских устройств самообслуживания, происходит активизация криминальных элементов и сообществ, осуществляющих хищения денежных средств из банкоматов и платежных терминалов посредством их взлома, несанкционированного перемещения, установки самодельных устройств для незаконного доступа к конфиденциальной информации, мошенничества.

Сумма ущерба только от одной кражи наличных денег из нижнего кабинета (сейфа) банкомата после его взлома может исчисляться миллионами рублей, что согласно п.4 примечаний к ст.158 УК РФ [1] квалифицируется как кража в особо крупном размере.

Как показывает статистика, значительную часть банкоматов и платежных терминалов злоумышленники похищают целиком, как правило, с помощью транспортных средств, и взламывают в специально подготовленном и оборудованном помещении. Имеют место и случаи вооруженных нападений на инкассаторов при загрузке банкоматов, а также на охранников организаций, в которых установлены банковские устройства самообслуживания, в том числе вооруженные нападения на сотрудников полиции при задержании

нарушителей. При этом есть основания полагать, что существенная часть похищенных из банкоматов и терминалов денежных средств идет на развитие и расширение преступных сообществ, приобретение ими новых, все более эффективных, средств взлома, автотранспорта, холодного и огнестрельного оружия, средств связи, устройств подавления радиосигналов, используемых для саботажа работы беспроводных систем передачи извещений и охранно-поисковых средств.

Преступники постоянно совершенствуют способы хищения наличных денег из банковских устройств самообслуживания. Все чаще регистрируются хищения отдельно установленных банкоматов с помощью транспортных средств. Для вскрытия сейфов банковских устройств самообслуживания злоумышленники используют специальные электроинструменты, газорежущие аппараты, самодельные взрывные устройства, нейтрализуют и выводят из строя системы видеоконтроля и сигнализации. При этом нарушителей не останавливает даже наличие физической охраны. Проблема с криминальными посягательствами на банкоматы и платежные терминалы приобрела системный характер. Значительный рост числа преступлений в этой области и огромные размеры материального ущерба сдерживают развитие и внедрение современных технологий дистанционного банковского обслуживания населения.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Термины и определения

В настоящих рекомендациях использованы термины по ГОСТ Р 51221-98, ГОСТ Р 52551-2006, а также следующие термины с соответствующими определениями:

Банк: кредитная организация, обладающая исключительным правом осуществлять в совокупности следующие банковские операции: привлечение во вклады денежных средств физических и юридических лиц, размещение указанных средств от своего имени и за свой счет на условиях возвратности, платности, срочности, открытие и ведение банковских счетов физических и юридических лиц.

Банковское устройство самообслуживания[1]**:** банкомат, платежный (информационно-транзакционный) терминал, паркомат, автоматизированный банковский сейф, терминал автоматического обмена валют, автоматизированное хранилище ценностей клиентов (сейфомат), автомат по продаже билетов на общественный транспорт и т.п.

Банкомат: программно-техническое средство, предназначенное для осуществления в автоматическом режиме (без участия уполномоченного лица кредитной организации или банковского платежного

[1] В настоящих Рекомендациях из всей номенклатуры банковских устройств самообслуживания основное внимание уделено банкоматам и платежным терминалам, как наиболее часто подвергаемым криминальным посягательствам.

агента) выдачи и (или) приема средств наличного платежа (банкнот) с использованием идентификационных электронных карт, наличных денежных расчетов и (или) расчетов с использованием идентификационных электронных карт, передачи распоряжений кредитной организации об осуществлении расчетов по поручению клиентов по их банковским счетам и для составления документов, подтверждающих передачу соответствующих распоряжений.

Валидаторная видеокамера: видеокамера, устанавливаемая в банковском устройстве самообслуживания для контроля слота приема наличных денег (валидатора).

Верхний кабинет: составная часть банковского устройства самообслуживания, предназначенная для управления его нижним кабинетом, связи с кредитной организацией (платежным агентом) – владельцем данного устройства, идентификации клиента, выполнения банковских (платежных) операций по распоряжениям клиента и выдачи кассовых чеков.

Виртуальная частная сеть (VPN): обобщённое наименование технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

Внутриобъектовый режим: порядок, обеспечиваемый совокупностью мероприятий и правил, выполняемых лицами, находящимися на охраняемом объектах, в соответствии с установленным порядком функционирования организации (учреждения, предприятия), в которой установлено охраняемое банковское устройство самообслуживания, и требованиями безопасности.

Дистанционное банковское обслуживание: предоставление возможности клиентам кредитных организаций или платежных агентов совершать банковские и платежные операции посредством использования различных каналов телекоммуникации (банкоматов, платежных терминалов, компьютерных, телефонных сетей) без участия уполномоченного работника кредитной организации или платежного агента.

Зона самообслуживания: помещение (выделенная зона, шлюзовая кабина безопасности, участок территории), в котором установлено банковское устройство самообслуживания или расположена его лицевая панель с пользовательским интерфейсом, предназначенное для доступа клиентов к устройству. В зависимости от конструкции и способа установки устройства его зона самообслуживания может быть либо отделена от его зоны загрузки (для устройств, устанавливаемых в проеме стены) либо совпадать с ней (для отдельно устанавливаемых устройств).

Идентификационная электронная карта: пластиковая карта, объединяющая в себе идентификационное и платежное средство, например, банковская, платежная, социальная или универсальная электронная карта, принимаемая банковским устройством самообслуживания для совершения банковских (платежных) операций.

Инженерно-техническая укрепленность: комплекс мероприятий, направленных на упрочнение конструктивных элементов банковских устройств самообслуживания и помещений, в которых они установлены, обеспечивающий необходимое противодей-

ствие несанкционированному проникновению, перемещению, взлому, повреждению и другим криминальным угрозам.

Картридер: устройство, являющееся составной частью банковского устройства самообслуживания, предназначенное для чтения данных идентификационных электронных карт.

Категория места размещения банковского устройства самообслуживания: комплексная оценка места размещения банковского устройства самообслуживания, учитывающая его уязвимость, в зависимости от характера и последствий возможных криминальных угроз, сложности обеспечения охраны и безопасности функционирования.

Кредитная организация (кредитное учреждение): юридическое лицо, которое для извлечения прибыли (как основной цели своей деятельности) на основании специального разрешения (лицензии) Центрального банка Российской Федерации (Банка России) имеет право осуществлять банковские операции, предусмотренные законом [2].

Место размещения банковского устройства самообслуживания: фактическое место, на которое банковское устройство самообслуживания установлено, зарегистрировано (по фактическому адресу), подключено и введено в эксплуатацию.

Модель нарушителя: комплексная характеристика, отражающая психологическое состояние, уровни физической подготовки, технической оснащенности и осведомленности нарушителя.

Нижний кабинет банковского устройства самообслуживания: составная часть банковского устройства самообслуживания, предназначенная для загрузки, хранения и выгрузки наличных денег.

Охранно-дымовая система: техническое средство активной защиты, которое при поступлении управляющего сигнала от технического средства охранной (тревожной) сигнализации или оператора заполняет охраняемое помещение (охраняемую зону) плотным искусственным туманом (дымом) в котором нарушитель теряет возможность зрительного восприятия объектов.

Охранно-поисковое техническое средство: комплект устройств, предназначенных для определения текущего местоположения (позиционирования) банковского устройства самообслуживания и поиска его в случае несанкционированного перемещения (хищения).

Передняя граница зоны самообслуживания: вертикальная плоскость, проходящая через наиболее выступающую лицевую панель банковского устройства самообслуживания (исключая козырьки, навесы, боковые стенки и ширмы).

Персональный идентификационный номер (ПИН-код): индивидуальный код, присваиваемый идентификационной электронной карте клиента и используемый клиентом при совершении операции по карте в качестве электронной подписи (цифрового аналога его личной подписи).

Плата видеозахвата: аппаратно-программное средство охранной телевизионной системы, предназначенное для преобразования аналогового видеосигнала в цифровой видеопоток, состоящее, как правило, из одного или нескольких аналого-цифровых преобра-

зователей, позволяющее обрабатывать сигнал от одного или нескольких аналоговых источников (видеокамер).

Платежный агент: юридическое лицо, за исключением кредитной организации, или индивидуальный предприниматель, осуществляющие деятельность по приему платежей физических лиц [3].

Платежный терминал: программно-техническое средство, предназначенное для приема платежным агентом от плательщика денежных средств, функционирующее в автоматическом режиме без участия уполномоченного лица платежного агента [4].

Позиционирование банковского устройства самообслуживания: определение с заданной точностью координат банковского устройства самообслуживания, основанное на использовании комбинации программных и аппаратных средств, данных глобальных навигационных спутниковых систем, наземных сетей операторов сотовой связи или специально созданных (развернутых) систем позиционирования.

Портретная видеокамера: видеокамера, устанавливаемая в банковском устройстве самообслуживания для регистрации лица клиента.

Презентерная видеокамера: видеокамера, устанавливаемая в банковском устройстве самообслуживания для контроля слота выдачи наличных денег (презентора).

Пропускной режим: порядок, обеспечиваемый совокупностью мероприятий и правил, исключающих возможность бесконтрольного прохода физических лиц, проезда транспортных средств, проноса (провоза) имущества на охраняемый объект или с охраняемого объекта.

Сейф банковского устройства самообслуживания: сейф, обладающий регламентированными защитными свойствами устойчивости к взлому, являющийся составной частью банковского устройства самообслуживания, предназначенный для обеспечения сохранности наличных денег и установленного в нем оборудования, в том числе технических средств безопасности.

Сервисная зона: помещение, в котором установлено банковское устройство самообслуживания и где производится его загрузка наличными деньгами, выгрузка наличных денег и техническое обслуживание. В зависимости от конструкции и способа установки устройства его сервисная зона может быть либо отделена от его зоны самообслуживания (для устройств, размещенных в проеме стены) либо совпадать с ней (для отдельно установленных устройств).

Скиммер: специальная накладка на картридер или тонкая пластина, размещаемая внутри картридера, оснащенная радиоэлектронными компонентами для осуществления скимминга.

Скимминг: неправомерный доступ к персональным данным идентификационной электронной карты при помощи специального считывающего устройства (скиммера).

Сцена видеокамеры (зона видеонаблюдения): часть контролируемой зоны либо прилегающей к ней территории, видеонаблюдение за которой производится одной видеокамерой, входящей в состав охранной телевизионной системы.

Техническое средство активной защиты банковского устройства самообслуживания: техниче-

ское средство, предназначенное для психологического и (или) физического воздействия на нарушителя, создания в окружающем пространстве условий, препятствующих осуществлению противоправных действий и привлечения внимания к охраняемому банковскому устройству самообслуживания.

Функция "день-ночь": функция видеокамеры охранной телевизионной системы, обеспечивающая улучшение качества полученного изображения путем отключения передачи цвета и повышения чувствительности видеокамеры в инфракрасном диапазоне при ухудшении условий освещенности зоны видеонаблюдения.

Функция компенсации и подавления засветки (HSBLC): функция видеокамеры, обеспечивающая улучшение качества изображения видеокамеры, полученного в условиях присутствия в сцене яркого источника света (солнце, фонарь, фары транспортных средств) путем применения алгоритмов цифровой обработки видеосигнала на встроенном процессоре, маскирующих наиболее яркие области в кадре.

Функция назначения зон конфиденциальности: функция видеокамеры, установленной в банковском устройстве самообслуживания или в зоне его размещения, позволяющая накладывать на части передаваемого видеокамерой изображения, наблюдение за которыми нежелательно или незаконно, специального маскирующего изображения, как правило, в форме одноцветных многоугольников или фигур сложной формы.

Функции трехмерного цифрового шумоподавления (3DNR): функция видеокамеры, обеспечивающая улучшение качества изображения, полученного в условиях низкой освещенности путем применения алгоритмов цифровой обработки видеосигнала на встроенном процессоре, учитывающих при определении шума временную (состояние того же пикселя в следующем кадре) и пространственную (обнаружение движения) информацию.

Функция цифрового расширения динамического диапазона (D-WDR): функция видеокамеры, позволяющая сохранять детализацию изображения, как в темных, так и в светлых участках в условиях больших перепадов освещенностей в сцене видеокамеры путем применения специальных алгоритмов цифровой обработки на встроенном процессоре.

1.2. Сокращения

АРМ – автоматизированное рабочее место

БУС – банковское устройство самообслуживания

ВК – верхний кабинет

ВСП – внутреннее структурное подразделение (кредитной организации)

ГЗ – группа задержания

ДПС – дорожно-патрульная служба полиции

ИК – инфракрасный (инфракрасная)

ИТУ – инженерно-техническая укрепленность

ИЭК – идентификационная электронная карта

КТС – кнопка тревожной сигнализации

НК – нижний кабинет

ППКОП – прибор приемно-контрольный охранно-пожарный (охранный)

ППС – патрульно-постовая служба полиции

ПЦО – пункт централизованной охраны

ПЦН – пульт централизованного наблюдения

РСПИ – радиоканальная система передачи извещений

ТСАЗ – техническое средство активной защиты

СКУД – система контроля и управления доступом

СОТ – система охранная телевизионная

СПВО – строевое подразделение вневедомственной охраны

СПИ – система передачи извещений

ТВЛ – телевизионные линии

ТСО – технические средства охраны

ТСОС – технические средства охранной сигнализации

УОО – устройство объектовое оконечное

2. КЛАССИФИКАЦИЯ БАНКОВСКИХ УСТРОЙСТВ САМООБСЛУЖИВАНИЯ

На территории Российской Федерации кредитными организациями и платежными агентами в основном используются банкоматы и платежные (информационно-транзакционные) терминалы производства компаний NSR (серии SelfServ и Personas), Diebold Incorporated (серии Opteva), Nautilus Hyosung (серии Monimax), Wincor Nixdorf (серии ProCash, CINEO), ЗАО "Новый Город" (серии Discovery DSV), ООО "ДОРС" (серии DORS) и др., которые отличаются конструктивными и дизайнерскими решениями, способами установки и крепления к строительным или специальным конструкциям, областью применения (размещения), максимальным объемом загружаемых и принимаемых наличных денежных средств, функциональными возможностями и уровнем механической защиты нижнего кабинета (сейфа).

2.1. Классификация БУС по конструкции, области применения и способу установки

2.1.2. В зависимости от конструкции и области применения БУС подразделяются на две основные категории:

- предназначенные для отдельной (обособленной) установки внутри или снаружи помещений;
- предназначенные для монтажа в специальном проеме капитальной строительной конструкции (стене) помещения.

При этом в зависимости от способа установки, особенностей эксплуатации и обслуживания, в каждой категории можно выделить по три группы БУС.

2.1.1. БУС, предназначенные для отдельной (обособленной) установки внутри или снаружи помещений подразделяются на следующие группы:

- группа ОП – БУС, отдельно устанавливаемые во внутренних или специально выделенных помещениях кредитных или иных организаций (учреждений, предприятий). Доступ клиентов к таким БУС, как правило, ограничен режимом работы организации (объектовым режимом). Загрузка (выгрузка) денежных средств и техническое обслуживание БУС производятся либо со стороны его лицевой панели, либо с задней стороны;

- группа ОВ – БУС, отдельно устанавливаемые в вестибюлях зданий, помещениях зон круглосуточного самообслуживания ("зонах 24"), павильонах банковского самообслуживания или специальных шлюзовых кабинах безопасности БУС (п.7.10). Доступ клиентов к таким БУС осуществляется без непосредственного входа в здание (офисные помещения) организации. Загрузка (выгрузка) денежных средств и техническое обслуживание БУС производятся либо со стороны его лицевой панели, либо с задней стороны;

- группа ОУ – БУС, отдельно устанавливаемые на открытой или огороженной территории. Загрузка (выгрузка) денежных средств и техническое обслуживание БУС производятся либо со стороны его лицевой панели, либо с задней стороны.

2.1.2. БУС, предназначенные для монтажа в специальном проеме капитальной строительной (несущей, защитной) конструкции здания, подразделяются на следующие группы:

- группа СП – БУС, устанавливаемые в проеме внутренней стены здания таким образом, что лицевая панель выходит во внутреннее помещение организации (учреждения, предприятия). Доступ клиентов к таким БУС возможен только из внутренних помещений организации. Загрузка (выгрузка) денежных средств и техническое обслуживание БУС производят с задней стороны;

- группа СВ – БУС, устанавливаемые в проеме внутренней стены помещения так, что лицевая панель выходит в вестибюль здания, помещение зоны круглосуточного самообслуживания ("зоны 24"), павильон или специальную шлюзовую кабину безопасности БУС (п.7.10). Доступ клиентов к БУС осуществляется без непосредственного входа в здание (офисные помещения) организации. Загрузка (выгрузка) денежных средств и техническое обслуживание таких БУС производят с задней стороны;

- группа СУ – БУС, устанавливаемые в проеме наружной стены здания или строения так, что лицевая панель выходит на открытую или огороженную территорию. Загрузка (выгрузка) денежных средств и техническое обслуживание БУС производят с задней стороны.

Основные варианты размещения БУС групп ОП, ОВ, ОУ, СП, СВ, СУ приведены в приложении А.

2.2. Классификация БУС по материальной ценности

2.2.1. В зависимости от максимального объема загружаемых в банкомат наличных денег[2] или макси-

[2] Определяется кредитной или иной организацией, являющейся владельцем БУС, с учетом конкретного типа БУС,

мальной наполняемости устройства для хранения денежных купюр в платежном терминале, БУС подразделяют на следующие категории материальной ценности[3]:

- категория ценности М1 – максимальная сумма загружаемых (хранящихся) в БУС наличных денег составляет более 1 миллиона рублей (хищение такой суммы квалифицируется[4] как кража в особо крупном размере);

- категория ценности М2 – максимальная сумма загружаемых (хранящихся) в БУС наличных денег составляет от 250 тысяч до 1 миллиона рублей (хищение такой суммы квалифицируется как кража в крупном размере);

- категория ценности М3 – максимальная сумма загружаемых (хранящихся) в БУС наличных денег составляет менее 250 тысяч рублей.

2.2.2. Если в одном помещении (зоне) установлено несколько БУС, то категорию ценности БУС по п.2.2.1 рекомендуется определять, исходя из суммарной стоимости наличных денег, хранящихся (загружаемых) в БУС, расположенных в данном охраняемом помещении (охраняемой зоне).

категории места его размещения (см. раздел 3) и должно быть указано в договоре на охрану БУС.

[3] Банкоматы, как правило, относятся к БУС категорий ценности М1 или М2, платежные терминалы, в зависимости от конструкции и функциональных возможностей – к категории ценности М2 или М3.

[4] По п.4 примечаний к статье 158 УК РФ [1]. В случае внесения изменений в УК РФ в части увеличения стоимости имущества, определяющего размер кражи, следует руководствоваться положениями действующей редакции закона.

2.2.3. Максимальный объем наличных денег, *S*, загружаемых в банкомат можно определить по формуле:

$$S = \sum_{i=1}^{N} K_i \cdot C_i, \qquad (2.1)$$

где S – общая стоимость загружаемых в банкомат денежных купюр, рублей или иностранной валюты (USD, EUR);

N – максимальное число кассет, предназначенных для выдачи денежных купюр (без учета reject/retract-кассет, предназначенных для хранения отбракованных или забытых купюр);

i – порядковый номер кассеты;

K_i – максимальное число денежных купюр, помещающихся в i-ю кассету;

C_i – номинал купюр, помещаемых в i-ю кассету;

В различных моделях банкоматов используется от 2 до 6 кассет, в которых помещается до трех тысяч купюр.

Например, если в банкомате для выдачи наличных используется четыре кассеты, в которые загружаются банкноты номиналом 5000, 1000, 500, 100 рублей по 1000 купюр в каждую, то максимальный объем наличных денег (при такой средней загрузке банкомата) составит 6 600 000 рублей.

2.3. Классификация БУС по функциональным возможностям

2.3.1. Банкоматы по своим функциональным возможностям и назначению можно разделить на следующие виды:

а) банкоматы с функцией выдачи наличных денег;

б) банкоматы с функциями выдачи и приема наличных денег;

в) банкоматы с функциями полного (замкнутого) оборота наличных, выполняющие функции выдачи и приема наличных денег, использующие получаемые от клиентов купюры для выдачи другим клиентам без процедуры инкассации;

г) многофункциональные банкоматы, выполняющие кроме функций выдачи и приема наличных денег дополнительные функции, например, управления банковскими депозитами, проведения наличных платежных операций[5], приема (сканирования), обработки, печати и выдачи банковских документов и т.п.

2.3.2. Платежные терминалы по своим функциональным возможностям и назначению можно разделить на следующие виды:

- платежные терминалы, предназначенные для проведения наличных платежных операций, осуществляющие прием и хранение наличных денег;

- универсальные платежные терминалы, предназначенные для проведения наличных и безналичных платежных операций, осуществляющие прием наличных денег и чтение идентификационных электронных карт;

- многофункциональные информационно-транзакционные терминалы, предназначенные для проведения наличных и безналичных платежных операций, осуществляющие прием и выдачу наличных денег, обмен валюты, прием и сканирование документов, другие

[5] Оплат услуг, налогов, штрафов, приобретение билетов на общественный транспорт, погашение кредитов, пополнения счетов, "электронных кошельков" и т.п.

операции. Такие терминалы в контексте обеспечения безопасности могут быть отнесены к банкоматам с присвоением соответствующей категории материальной значимости.

2.4. Классификация БУС по устойчивости к взлому

По устойчивости к взлому БУС подразделяют на классы в соответствии с типами их сейфов, которые в зависимости от величины сопротивления к разрушающим воздействиям различными инструментами подразделяются на классы устойчивости к взлому, приведенные в приложении Б.

3. КАТЕГОРИРОВАНИЕ МЕСТ РАЗМЕЩЕНИЯ БАНКОВСКИХ УСТРОЙСТВ САМООБСЛУЖИВАНИЯ

В соответствии с рекомендациями Банка России [5] с целью повышения безопасности БУС необходимо классифицировать места их размещения по степени риска быть подвергнутыми преступным посягательствам (попыткам физического взлома, кражи, установки скимминговых устройств, вредоносного программного обеспечения, совершения несанкционированных операций). Впоследствии, по мере развития технологий, появления новых средств и методов совершения криминальных посягательств на БУС рекомендуется обновлять классификацию мест размещения БУС.

С учетом рекомендаций Банка России и Экспертно-методического центра банковской безопасности при Ассоциации российских банков, в зависимости от степени риска возникновения криминальных угроз, места размещения БУС могут быть условно разделены на четыре категории[6].

3.1. Места размещения категории Р1

Места размещения БУС, относящиеся к категории Р1, отличаются низкой (минимальной) степенью риска криминальных посягательств на БУС, обусловленной высоким постоянным уровнем противокриминальной защищенности, которая характеризуется ограниченным (по времени работы организации) доступом к БУС, высоким уровнем инженерно-технической укрепленности помещений, наличием необходимых средств охранной, тревожной сигнализации и видеонаблюдения, профессиональной физической охраны, имеющей специальную подготовку и оснащение.

К таким местам размещения БУС могут быть отнесены, например:

- помещения для совершения операций с ценностями кредитных организаций (банков), оборудованные средствами ИТУ, ТСОС, СОТ и имеющие круглосуточный пост физической охраны (дежурства), доступ в которые (в зону размещения БУС) ограничен установленным режимом работы организации;

---

[6] Места размещения БУС, которые не были перечислены в пп.3.1–3.4, классифицируются по ближайшему аналогу с учетом возможного риска совершения преступных посягательств на БУС.

- внутренние помещения (не имеющие непосредственных выходов на открытую территорию) органов власти, учреждений и организаций, в том числе подлежащих обязательной охране полицией в соответствии с Перечнем, утвержденным Правительством Российской Федерации [6], на которых предусмотрены внутриобъектовый и пропускной режимы, круглосуточный пост физической охраны (дежурства), в том числе возможно наличие электронной СКУД, оборудованные средствами ИТУ, ТСОС, СОТ.

3.2. Места размещения категории Р2

Места размещения БУС, относящиеся к категории Р2, отличаются средней степенью риска криминальных посягательств на БУС, обусловленной средним уровнем противокриминальной защищенности, которая характеризуется ограниченным (по времени работы организации) доступом к БУС, при этом уровень инженерно-технической укрепленности помещения или участка территории, состав используемых на объекте средств охранной, тревожной сигнализации и видеонаблюдения, а также уровень подготовки и оснащения физической охраны могут быть различными (в зависимости от конкретного вида объекта).

К таким местам размещения БУС могут быть отнесены, например:

- контрольно-пропускные пункты организаций (учреждений, предприятий, органов власти), оборудованные средствами тревожной сигнализации, видеонаблюдения, а также (при необходимости) СКУД, на которых предусмотрены посты физической охраны

(полиции, ведомственной охраны, частной охранной организации, внутренней сторожевой охраны);

- вестибюли, холлы, клиентские зоны офисных центров, учреждений культуры и искусства, доступ в которые ограничен режимом работы организации (учреждения), оборудованные средствами ИТУ, ТСОС, системами видеонаблюдения, на которых возможно наличие круглосуточной физической охраны (дежурного персонала);

- внутренние участки огражденной и оборудованной ТСОС, СКУД и СОТ территории предприятий, организаций или учреждений с круглосуточной физической охраной, имеющей специальную подготовку и оснащение.

3.3. Места размещения категории Р3

Места размещения БУС, относящиеся к категории Р3, отличаются повышенной степенью риска криминальных посягательств на БУС, обусловленной невысоким, неравномерным или непостоянным (в течение времени работы БУС) уровнем противокриминальной защищенности, которая характеризуется тем, что режим доступа к БУС, уровень инженерно-технической укрепленности помещения или участка территории, состав используемых на объекте средств охранной, тревожной сигнализации, видеонаблюдения и средств активной защиты, уровень подготовки и оснащения физической охраны (при ее наличии) могут быть различными (в зависимости от конкретного вида объекта и установленного в данный период времени порядка его функционирования, определяемого собственником объекта).

К таким местам размещения БУС могут быть отнесены, например:

- вестибюли, холлы, клиентские зоны, зоны самообслуживания предприятий мелкооптовой и розничной торговли (торгово-развлекательных центров, гипермаркетов), спортивно-развлекательных комплексов, гостиниц и иных объектов потребительского рынка, функционирующих либо в ограниченном по времени, либо в круглосуточном режиме с постоянным присутствием обслуживающего персонала и (или) сотрудника службы безопасности данного предприятия, на которых также возможно наличие системы видеонаблюдения;

- объекты транспортной инфраструктуры (вокзалы), автозаправочные станции, автосервисы, функционирующие в круглосуточном режиме с постоянным присутствием обслуживающего персонала и (или) дежурного охранника, оборудованные системами видеонаблюдения и средствами тревожной сигнализации (КТС у персонала объекта);

- муниципальные учреждения здравоохранения (стационары), функционирующие в круглосуточном режиме с постоянным присутствием обслуживающего персонала и (или) дежурного охранника, оборудованные средствами тревожной сигнализации, например, стационарной и (или) переносной КТС у дежурной медсестры и охранника медучреждения;

- круглосуточные зоны дистанционного банковского обслуживания ("зоны 24"), в том числе специальные павильоны для банкоматов, оборудованные системой постоянного видеонаблюдения;

- подъезды многоквартирных жилых домов (комплексов), оборудованные домофонами и системами видеонаблюдения, на которых предусмотрено наличие консьержа с круглосуточным графиком работы;

- внутренние участки огражденной территории предприятия, организации или учреждения, жилого, спортивного или торгового комплекса с ограниченным контролируемым доступом на территорию, оборудованные СКУД и системой видеонаблюдения.

3.4. Места размещения категории Р4

Места размещения БУС, относящиеся к категории Р4, отличаются высокой (максимальной) степенью риска криминальных посягательств на БУС. Это объекты с низким уровнем противокриминальной защищенности, который характеризуется неограниченным (круглосуточным) доступом к БУС, отсутствием средств инженерно-технической укрепленности, охранной сигнализации (кроме тех, что установлены в самом БУС), постоянно присутствующей физической охраны.

К таким местам размещения БУС могут быть отнесены, например, открытые участки территории городских поселений (площади, улицы, тротуары), подземные или надземные переходы, открытые платформы железнодорожных станций или вокзалов, на которых предусмотрено постоянное видеонаблюдение и патрулирование полицией (ППС, ДПС).

4. МОДЕЛЬ НАРУШИТЕЛЯ, ОСНОВНЫЕ ВИДЫ КРИМИНАЛЬНЫХ УГРОЗ БАНКОВСКИМ УСТРОЙСТВАМ САМООБСЛУЖИВАНИЯ, СПОСОБЫ ЗАЩИТЫ

4.1. Модель нарушителя, совершающего криминальные посягательства на БУС

4.1.1. Общие критерии формирования модели нарушителя

Основная задача нарушителя, целью которого является тайное хищение (кража) наличных денег из сейфа БУС, заключается в скрытном преодолении средств инженерно-технической укрепленности БУС и помещения, в котором оно установлено, "обходе" ТСОС, СКУД и СОТ (при их наличии) для получения неправомерного доступа к наличным деньгам, размещенным в сейфе БУС, электронным компонентам (компьютеру) БУС, каналам связи или персональным данным ИЭК клиентов, использующих БУС для осуществления дистанционного банковского обслуживания или платежных операций.

Основная цель создания системы комплексной централизованной охраны БУС – противостоять угрозе незаконного проникновения нарушителя в зону размещения БУС и совершения противоправных действий по отношению к БУС и средствам обеспечения его безопасности (охранной сигнализации, видеонаблюдения).

Поэтому в процессе концептуального проектирования такой системы важно создать модель нарушителя и создаваемых им угроз для определения впоследствии оптимального состава системы, отвечающего

требованиям по надежности охраны и ее технико-экономической эффективности.

Модель угроз представляет собой перечень возможных способов достижения нарушителем своей цели, а также сценария наиболее вероятных его действий при несанкционированном проникновении в зону размещения БУС и совершении криминальных воздействий на БУС.

Такой подход дает возможность сформировать требования к ИТУ, ТСОС, СКУД, СОТ, ТСАЗ и другим средствам противокриминальной защиты БУС, при реализации которых возможно обеспечить эффективную защиту БУС от преступных посягательств.

Исходя из многообразия характеристик нарушителей, можно выделить следующие критерии их классификации.

1. По мотивации:

- случайный нарушитель (попал на объект случайно);

- преднамеренный нарушитель (действует с определённым умыслом).

2. По уровню подготовки:

- квалифицированный (профессионал) – основной деятельностью такого нарушителя (организованной преступной группы) являются криминальные посягательства на БУС, преодоление систем обеспечения их безопасности, он имеет большой опыт такой деятельности и, как правило, хорошо оснащён;

- подготовленный – имеющий общие знания об устройстве БУС и системах обеспечения их безопасности, системах сигнализации, методах обхода, ин-

формацию о конкретном объекте, на котором установлено БУС, и (возможно) опыт проникновения;

- неподготовленный – не имеющий знаний об устройстве БУС и системах обеспечения их безопасности, системах сигнализации, причем как общих, так и специальных – применительно к конкретному объекту, а также опыта проникновения (взлома или кражи БУС).

3. По численности:

- одиночный;

- организованная преступная группа.

4. По отношению к охраняемому объекту (организации, в которой установлено БУС):

- внешний нарушитель (в настоящее время, не имеет прямого отношения к кредитной, обслуживающей организациям, арендодателю);

- внутренний нарушитель (является сотрудником кредитной, платежной или обслуживающей БУС организаций, либо арендодателя, использует служебное положение и знания для осуществления преступления, либо подготовки к нему.

- группа лиц, имеющих различное отношение к охраняемому объекту, действующих по предварительному сговору.

5. По степени осведомлённости о функционировании и структуре охраняемого объекта (о самом БУС, а также об организации, в которой установлено и функционирует БУС), о его системе охраны:

- неосведомлённый;

- имеющий общую информацию;

- имеющий детальную информацию.

6. По степени технической оснащённости:

- не оснащён;

- оснащён бытовыми средствами (стандартными инструментами);

- оснащён специальными средствами и оборудованием.

7. По физическому состоянию:

- находящийся в хорошей физической форме;

- имеющий слабую физическую подготовку или травмы (заболевания).

8. По преследуемым целям:

- для взлома нижнего кабинета (сейфа) БУС с целью хищения хранящихся в нем кассет с наличными деньгами;

- для несанкционированного перемещения (хищения) БУС целиком с целью последующего взлома в удаленном скрытом месте;

- для установки устройств на БУС и (или) в зоне его размещения, предназначенных для неправомерного доступа к персональным данным ИЭК (скиммера, скрытой видеокамеры, накладки на клавиатуру и т.п.) или для механической блокировки (кражи) ИЭК ("ливанская петля") и др.

9. По способу незаконного проникновения:

- контактный (непосредственное проникновение на территорию и/или в помещение охраняемого объекта и выполнение необходимых действий);

- бесконтактный (использование различных дистанционных технологий неправомерного доступа к конфиденциальным данным ИЭК и кражи денежных средств со счетов граждан).

Обычно, прежде чем действовать, опытные нарушители производят "разведку" – сбор информации

об объекте и его системе охраны. Исключение могут составлять случаи, требующие немедленного принятия решения и действий. Возможно также появление их самих на объекте охраны под благовидным предлогом, например, в качестве посетителя, покупателя, рекламного агента, случайного лица и т.п. Следовательно, важно не допустить утечки информации и принять комплекс мер, препятствующих этому.

Возможен также сговор с работниками кредитной или иной организации, в которой установлено БУС, или сотрудниками подразделением безопасности этой организации, причём побуждения могут быть различными, начиная с элементарного подкупа и заканчивая шантажом.

В любом случае нарушителю необходимо достичь цели, минуя элементы ИТУ, ТСОС, СОТ и СКУД (если она установлена).

При этом нарушителю важно получить доступ в интересующее место и не "засветиться" (не обнаружить себя). Для преодоления охранных рубежей нарушителями могут применяться следующие приёмы:

- проход по сговору;
- обман СКУД;
- обход зон обнаружения ТСОС и зон видеонаблюдения СОТ;
- саботаж работы ТСОС, СКУД, СОТ, ТСАЗ.

4.1.2. Типология нарушителей по подготовленности к преодолению системы охраны

В целом личность нарушителя можно определить как личность человека, который способен на преступ-

ления вследствие присущих ему психологических особенностей, антиобщественных взглядов, отрицательного отношения к нравственным ценностям и вследствие выбора общественно опасного пути для добровольного удовлетворения своих потребностей, под принуждением или в силу сложившихся обстоятельств.

Специфическая сущность личности нарушителя заключается в особенностях его психического склада, которые выражают собой внутренние предпосылки антиобщественного поведения. Общественную опасность представляет потенциальная предрасположенность личности к преступному поведению, которая понимается как внутренняя возможность совершения при определенных условиях преступных действий.

Можно выделить две группы нарушителей, отличающихся характером поведения при совершении противоправных действий на объекте, – осторожные и неосторожные.

Осторожные нарушители характеризуются, как правило, низким уровнем тревожности, проявляют общительность, стремятся к установлению межличностных контактов, социально адаптированы, в наименьшей степени упрекают себя за совершение преступления.

Неосторожные нарушители характеризуются высоким уровнем тревожности, проявляют неуверенность в себе, склонность к волнениям при стрессе, избыточный самоконтроль, непродуманное поведение, реализуют эмоциональные, а не рациональные, спокойные реакции на угрозы в экстремальной ситуации.

Дерзкие нарушители характеризуются высоким уровнем тревожности, при этом самоуверенны, резки в общении и реагировании на угрозы в экстремальной ситуации.

Психологические аспекты поведения нарушителей, совершающих криминальные действия в отношении БУС, необходимо учитывать, в частности, при выборе тактики действия сотрудников полиции (ГЗ СПВО), осуществляющих оперативное реагирование по сигналу тревоги, проступившему с объекта, на котором установлено активное средство защиты БУС (п.7.5.3), оказывающее отпугивающее или дезориентирующее воздействие на нарушителей.

Физическая подготовленность нарушителя характеризуется развитостью его физических возможностей по перемещению на объекте, преодолению средств ИТУ БУС и зоны его размещения.

Объединяя психологические особенности и физическое состояние, можно охарактеризовать высокоподготовленного нарушителя как осторожного, решительного, физически развитого человека. Слабый уровень психофизической подготовленности характеризуется плохим физическим развитием, высоким уровнем тревожности нарушителя, неуверенностью в себе. Промежуточное положение между ними занимает средний уровень психофизической подготовленности.

Уровень технической подготовленности нарушителя характеризуется наличием у него специальных технических средств для проникновения и навыков в обращении с ними. Высокая степень технической подготовленности подразумевает наличие специальных

наборов инструментов, оборудования и высокую квалификация нарушителя по их применению. Для внешнего или внутреннего нарушителя среднего уровня подготовленности это может быть подобранный под конкретную задачу набор самодельных или усовершенствованных технических средств. Нарушитель с низким уровнем технической подготовленности использует, как правило, подручные, бытовые легкодоступные средства или не использует их вовсе.

Осведомленность нарушителя об охраняемом объекте (как самих БУС, так и зон их размещения) и системе охраны существенно влияет на уровень его подготовленности. Можно выделить три типичных уровня осведомленности нарушителя:

- высокая – нарушитель знает практически все об устройстве БУС, об организации зон его размещения (зоны самообслуживания, сервисной зоны), о системе охраны и их уязвимых местах;

- средняя – нарушитель знает сравнительно много об устройстве БУС, об организации зон его размещения (зоны самообслуживания, сервисной зоны), но не знает уязвимых мест БУС и зон их размещения, имеет недостаточно знаний о системе охраны, значимости критических элементов защиты и точных местах их нахождения;

- низкая – нарушитель имеет общее представление об устройстве БУС и системе его охраны, но практически ничего не знает об уязвимых местах БУС и зон его размещения, значимости и местах нахождения критических элементов защиты.

Рассмотрим обобщенную модель возможных действий нарушителей в зависимости от уровня их подготовленности.

1. Квалифицированный нарушитель при планировании и подготовке к совершению криминальных посягательств на БУС, как правило, проводит внешний осмотр здания, в котором установлено БУС, выбранное им в качестве объекта криминального посягательства, изучает прилегающую территорию и пути подъезда к зданию, а также пути "отхода" в случае прибытия ГЗ СПВО или внутренней службы охраны кредитной или иной организации.

Он визуально изучает внутри этого здания конкретное помещение, в котором установлено БУС, где расположены зона самообслуживания и сервисная зона данного БУС, визуально определяет уровень ИТУ помещения, наличие СКУД, ТСАЗ, типы и места расположения ТСОС, видеокамер СОТ, с целью выбора такого способа проникновения внутрь здания и помещения, где установлено БУС, при котором он сможет остаться незамеченным для указанных средств охраны. Его квалификация позволяет ему применять любой способ проникновения. Однако особое внимание он уделяет возможности заблаговременного выведения из строя ТСО на объекте (в том числе и путем сговора с персоналом объекта) или выбору объектов, на которых ТСО (ТСОС, видеокамеры СОТ, элементы СКУД) временно находятся в неисправном состоянии или выключены. Как правило, он предварительно оценивает время оперативного реагирования ГЗ СПВО

путем инициирования ложного сигнала тревоги (удары в дверь, окна, отключение электропитания и др.).

Квалифицированного нарушителя интересуют в первую очередь БУС высокой категории материальной значимости (чаще всего М1, реже М2), количество которых в регионе (округе, поселении) ограничено. Такие нарушители являются наиболее опасными, так как чаще всего успешно совершают кражи с большим ущербом. Однако в течение года большую серию краж они не реализуют из-за малого числа интересующих их объектов в одном регионе с допустимым для них риском неудачной кражи.

2. Подготовленный нарушитель на этапе планирования и подготовки преступления проводит, как правило, внешний осмотр здания и прилегающей территории объекта так же, как и квалифицированный нарушитель. Степень подготовленности позволяет ему реализовать "квалифицированные" способы проникновения в зону размещения БУС, связанные с проломом стен, пола, потолка, подбором ключей (специальных отмычек), проникновением в здание до его сдачи под охрану, и осуществить взлом сейфа БУС или кражу БУС целиком с помощью стандартных (по ГОСТ Р 50862-2012) средств взлома, имеющихся в свободной продаже. Только часть таких нарушителей удается задержать по горячим следам, остальные в течение года могут совершить серию из нескольких краж.

3. Неподготовленный нарушитель при подготовке к совершению кражи ограничивается внешним осмотром здания, оценивает в основном техническую укрепленность окон и дверей и качество охранного

освещения. Попытки проникновения он совершает, например, путем разрушения стекол или выбивания дверей слабо укрепленных объектов в надежде совершить кражу "на рывок". Нарушителей этого типа в большинстве случаев удается задержать при совершении первой кражи на охраняемом объекте. При срабатывании ТСАЗ на объекте (звукового или комбинированного охранного оповещателя, охранно-дымовой, газовой системы или системы активной защиты помещения туманом) такой нарушитель чаще всего прекращает дальнейшее проникновение и покидает объект.

Модель наиболее вероятного нарушителя для конкретного объекта выбирается из типовых (или создается специально) в результате анализа статистики нарушений на защищаемом и аналогичных объектах, а также криминогенной обстановки в регионе и ее прогноза.

4.1.3. Классификация нарушителей, совершающих преступные посягательства на БУС

Основные категории нарушителей и виды совершаемых ими преступлений, связанных с незаконным проникновением в зону размещения БУС, криминальными посягательствами на БУС и конфиденциальную информацию ИЭК, а также на пользователей БУС, инкассаторов и обслуживающий персонал, приведены в таблице 4.1.

Таблица 4.1 – Категории нарушителей и виды совершаемых преступлений

Категория нарушителя	*Виды совершаемых преступлений*	*Квалификация преступления*
Н1В	Незаконное проникновение в зону размещения БУС (сервисную зону). Саботаж работы ТСОС. Взлом сейфа БУС с помощью высокопроизводительных средств взлома, в том числе – взрывных устройств. Изъятие наличных денег из БУС.	Статья 158 УК РФ (кража)
Н2В	Незаконное проникновение в зону размещения БУС (сервисную зону). Саботаж работы ТСОС. Несанкционированное перемещение БУС с использованием автотранспортного или специального средства перемещения. Взлом БУС в удаленном скрытом специально оборудованном месте. Изъятие наличных денег из БУС.	Статья 158 УК РФ (кража)
Н3В	Незаконное проникновение в зону размещения БУС (сервисную зону). Взлом сейфа БУС с использованием простейших механических средств взлома. Изъятие наличных денег из БУС.	Статья 158 УК РФ (кража)

Н4В	Незаконное проникновение в зону размещения БУС (сервисную зону). Несанкционированное перемещение БУС ручным способом или с помощью подручных средств. Взлом БУС в удаленном скрытом месте. Изъятие наличных денег из БУС.	Ст.158 УК РФ (кража)
Н5В	Разрушение или повреждение лицевой панели (экрана, клавиатуры) верхнего кабинета БУС, совершаемое из хулиганских побуждений или из-за низкой осведомленности о месте хранения наличных денег в БУС	Ст. 167 УК РФ (умышленные уничтожение или повреждение имущества)
Н1Р	Разбойное нападение на работников кредитной или иной организации, осуществляющих инкассацию, обслуживание (ремонт) и охрану БУС с целью получения доступа к наличным деньгам, хранящимся в сейфе БУС.	Ст. 162 УК РФ (разбой), ст. 317, 318 (в случае нападения на сотрудника вневедомственной охраны)

Н2Р	Ограбление пользователя БУС (клиента банка) при получении им наличных денег из БУС или получение пользователем БУС наличных денег под принуждением.	Ст. 161 УК РФ (грабеж) или ст. 162 УК РФ (разбой)
Н3Р	Кража наличных денег, ИЭК или другого имущества у пользователя БУС при осуществлении им дистанционного банковского обслуживания.	Ст. 158 УК РФ (кража)
Н1К	Незаконное проникновение в зону размещения БУС (сервисную зону), кроме БУС, установленных на улице или в "зоне 24". Вскрытие верхнего кабинета БУС. Незаконное подключение к компьютеру БУС, переустановка ПО БУС, измененного под криминальные цели, инсталляция вредоносных компьютерных программ в ПО БУС	Ст. 272 УК РФ (неправомерный доступ к компьютерной информации), ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ)

Н2К	Установка скимминговогообо-рудования с целью кражи кон-фиденциальных данных ИЭК клиентов. Другие различные виды мошенничества в сфере дистанционного банковского обслуживания.	Ст. 272 УК РФ (непра-вомерный доступ к компью-терной информа-ции)[7], ст. 159 УК РФ (мо-шенниче-ство)

4.2. Основные виды криминальных угроз в отношении БУС и рекомендуемые способы защиты

4.2.1. Основные виды криминальных угроз в отношении БУС и рекомендуемые способы противодействия таким угрозам приведены в таблице 4.2.

Таблица 4.2 – Криминальные угрозы БУС и способы противодействия угрозам

№ п/п	*Основные виды криминальных угроз в отношении БУС*	*Способы противодействия указанным угрозам*
1	Несанкционированное проникновение на	Выполнение требований по ИТУ дверей,

[7] С учетом положений ст.30, ч.3 и ч.4 ст.159, ст.159.3 УК РФ, ч.1 ст.3 Федерального закона 27 июля 2006 г. № 152-ФЗ "О персональных данных" [7] и п.3.3 Положения Банка России от 19 августа 2004 г. №262-П [8].

	территорию, в здание, помещение, в котором установлено БУС, посредством механического повреждения входных дверей, оконных или других строительных (защитных) конструкций	окон и строительных (защитных) конструкций помещения Установка ТСОС для контроля: - открывания дверей и окон помещения; - разрушения дверей, окон, строительных и защитных конструкций помещения; - проникновения через дверной или оконный проем; - перемещения в охраняемой зоне. Установка СОТ, ТСАЗ.
2	Вскрытие НК БУС путем сквозного повреждения (разрушения) оболочки сейфа с помощью ручных, электрических и термических инструментов	Выполнение требований по классу защиты сейфа БУС. Установка средства раннего обнаружения попытки повреждения защитной оболочки сейфа БУС. Установка СОТ (с соответствующей видеоаналитической функцией).

3	Вскрытие НК БУС путем механического повреждения (взлома) запирающих устройств декоративной двери НК и основной двери сейфа	Выполнение требований по классу защиты сейфа БУС, количеству замков и их классам защиты. Установка ТСОС для контроля: - несанкционированного открывания декоративной двери НК БУС; - открывания и взлома основной двери сейфа БУС; - разрушения запирающих устройств сейфа БУС. Установка СОТ (с соответствующей видеоаналитической целевой функцией), ТСАЗ.
4	Вскрытие НК БУС путем подбора ключей или кодов к запирающему устройству сейфа	Выполнение требований по классу устойчивости сейфа БУС к взлому и криминальному открытию, в том числе требований по количеству замков сейфа БУС и их классам защиты. Установка ТСОС для контроля:

		- несанкционированного открывания декоративной двери НК БУС; - открывания или взлома двери сейфа БУС; - открывания запирающих устройств сейфа БУС. Установка СОТ (с соответствующей видеоаналитической функцией), ТСАЗ.
5	Вскрытие НК БУС путем создания внутри сейфа взрывной волны при помощи взрывоопасной газовой смеси.	Выполнение требований по классу устойчивости сейфа БУС к взлому. Установка ТСОС для определения наличия горючих газов, а также (при значительном объеме загружаемых денежных средств и сложной криминогенной обстановке) введение нейтрализатора взрывоопасной смеси. Установка СОТ (с соответствующей видеоаналитической функцией), ТСАЗ.

6	Вскрытие НК БУС путем мощного силового воздействия на оболочку сейфа (изменение формы конструкции), при помощи строительной техники, гидравлического или другого специального оборудования.	Установка специализированного ТСОС, обеспечивающего обнаружение повреждения и разрушения сейфа различными методами. Установка видеокамер СОТ в зоне размещения БУС и вокруг нее.
7	Несанкционированное перемещение (хищение) БУС с места размещения ручным способом (при помощи монтажных инструментов или без них) с целью последующего вскрытия сейфа БУС в удаленном месте.	Выполнение требований по классу устойчивости сейфа БУС к взлому, в том числе требований устойчивости его элементов крепления к разрушению и силе отрыва от пола (основания). Установка ТСОС для контроля положения БУС. Установка СОТ (с соответствующей видеоаналитической функцией), ТСАЗ Оснащение БУС системой позиционирования и поиска.
8	Срыв (хищение "на рывок") БУС с места установки при по-	Выполнение требований по классу устойчивости сейфа БУС к взлому, в

	мощи автотранспорта или строительной техники (бульдозера, автокара, эвакуатора, экскаватора, самоходного гидравлического домкрата, подъемного автокрана и т.п.)	том числе требований устойчивости его элементов крепления к разрушению и силе отрыва от пола (основания). Установка ТСОС для контроля положения БУС. Установка видеокамер СОТ в зоне размещения БУС и вокруг нее. Оснащение БУС системой позиционирования и поиска.
9	Вскрытие НК БУС путем взлома запорных устройств сейфа при помощи автотранспорта или строительной техники	Выполнение требований по классу устойчивости сейфа БУС к взлому. Установка ТСОС для контроля несанкционированного открывания декоративной двери НК БУС и основной двери сейфа БУС.
10	Вскрытие ВК (блока электронного управления) БУС с целью незаконного вторжения в операционную систему и прикладные программы БУС (установка вредоносных программ или подмена ПО БУС	Установка ТСОС для контроля несанкционированного открывания (доступа) ВК БУС и вскрытия (повреждения) оболочки ВК БУС. Установка СОТ, ТСАЗ. Применение защищенного ПО и средств аутентификации подключений к компьютеру ВК БУС.

11	Умышленное нарушение связи БУС с кредитной организацией (банком) путем повреждения электрических линий связи или внешней антенны, использования средств подавления радиосигнала	Контроль линий связи, установка антенны в защищенном месте или использование внешней антенны с датчиком положения.
12	Умышленное нарушение работы проводной или оптоволоконной СПИ путем обрыва или замыкания линий связи, подключения несанкционированных устройств	Использование проводных или оптоволоконных СПИ, обеспечивающих постоянный контроль состояния линий связи, защищенных от криминальных воздействий.
13	Умышленное нарушение работы РСПИ, использующих каналы сотовой связи (GSM, 3G, 4G, LTE), путем механического повреждения внешней антенны или подавления радиосигналов	Использование специализированных РСПИ с антеннами, устанавливаемыми внутри БУС, устойчивых к умышленному подавлению радиосигналов
14	Умышленное нарушение работы системы позиционирования и поиска БУС (GPS,	Использование систем позиционирования и поиска БУС устойчивых к подавлению ра-

	ГЛОНАСС), путем механического повреждения внешних антенн или подавления радиосигналов	диосигналов, со скрытыми (внутренними) антеннами и специальными маяками.
15	Умышленное нарушение работы видеокамер, установленных в БУС или зоне самообслуживания (повреждение, заклеивание объектива, нарушение линий связи видеокамер с видеорегистратором, кража видеорегистратора)	Выбор и применение СОТ, защищенных от указанных видов угроз. Установка в зоне самообслуживания не менее двух камер: на стене (камера общего обзора) и на потолке (портретная купольная камера) на высоте не менее 2,5 м.
16	Организация аварии или умышленного отключения электроснабжения (сети 220 В) в зоне размещения БУС или во всем здании (на всем объекте)	Применение средств, обеспечивающих бесперебойное электропитание БУС и ТСОС
17	Отключение освещения в помещении или на территории, где установлено БУС	Организация аварийного освещения. Использование видеокамер СОТ с ИК подсветкой

18	Вооруженное нападение на физическую охрану объекта или помещения, в котором установлено БУС (сторожа, работника ведомственной охраны или частной охранной организации)	Установка стационарной КТС и обеспечение работника охраны переносной КТС с датчиком падения. Применение СОТ, ТСАЗ, СКУД
19	Вооруженное нападение на работников кредитной или другой уполномоченной организации, осуществляющих техническое обслуживание БУС, загрузку, выгрузку и перевозку наличных денежных средств (инкассацию)	Установка стационарной КТС. Обеспечение инкассаторов переносной КТС с датчиком падения. Установка СОТ. Применение специальных кодов открытия БУС под принуждением.
20	Кража наличных денег из кассет, устанавливаемых в БУС (при инкассации, обслуживании или ремонте БУС)	Применение автономных счетчиков регистрации открывания шторки кассет БУС с наличными деньгами
21	Неправомерный доступ к персональным данным пользователей БУС, хранящимся на	Установка активного антискиммингового средства. Установка видеока-

	магнитной полосе ИЭК, путем установки скиммингового оборудования	меры СОТ, контролирующей картридер БУС
22	Неправомерный доступ к персональным данным пользователей ИЭК (ПИН-кодам) путем установки считывающей накладки на клавиатуру БУС или скрытой видеокамеры	Установка датчиков, обнаруживающих установку несанкционированных устройств на БУС. Установка видеокамер СОТ, контролирующих БУС
23	Кража ИЭК путем ее механической блокировки в картридере БУС (траппинг или "ливанская петля")	Использование модифицированного картридера или датчика на картридер Установка видеокамеры СОТ, следящей за картридером БУС
24	Захват и извлечение банкнот после банковской операции (мошенничество со шторкой презентера БУС)	Установка датчика движения шторки презентера и специальной конструкции шторки, затрудняющая установку устройств незаконного захвата банкнот

4.2.2. Средства защиты составных частей БУС от криминальных угроз, указанных в пп.21 – 24 таблицы 4.1, в том числе различные датчики (сенсоры), как

правило, устанавливаются опционально предприятиями-изготовителями или организациями-поставщиками БУС на этапе производства или предпродажной подготовки банкоматов и платежных терминалов по заказу кредитной организации или платежного агента.

4.2.3. Не указанные в таблице 4.1 криминальные угрозы, такие, например, как ложная отмена банковской или платежной операции на БУС, установка подложных БУС ("банкоматов-клонов"), создание "сайтов-клонов" кредитных организаций или платежных агентов (фишинг) или рассылка на сотовые телефоны держателей банковских карт SMS-сообщений от имени банка о якобы блокировке банковской карты (вишинг), относятся к сфере деятельности подразделений безопасности Банка России и кредитных организаций (платежных агентов), являющихся владельцами БУС, а также требуют от пользователей БУС соблюдения общепринятых мер безопасности обращения с БУС и ИЭК.

Для организации эффективной противокриминальной защиты БУС, в особенности отдельно устанавливаемых банкоматов высокой материальной значимости, находящихся в группе особого риска, наряду с указанными в пп.4.2.1, 4.2.3 потенциальными криминальными угрозами в отношении БУС, как таковых, необходимо проанализировать и рассчитать возможные типы потенциальных нарушителей применительно к конкретной организации (учреждению, предприятию), в которой установлено БУС, с учетом категории места размещения БУС, статистики аналогичных преступлений, криминогенной ситуации в конкретном Федеральном округе, субъекте Российской Федерации, муниципальном образовании (районе, населенном пункте, микрорайоне).

5. РЕКОМЕНДАЦИИ ПО ВЫБОРУ МЕСТ РАЗМЕЩЕНИЯ БАНКОВСКИХ УСТРОЙСТВ САМООБСЛУЖИВАНИЯ

5.1. Общие требования к выбору мест размещения БУС

5.1.1 Банкоматы и платежные терминалы должны быть установлены в наиболее безопасных местах, обеспечивающих выполнение рекомендаций Банка России "О мерах безопасного использования банковских карт" [9].

При выборе места размещения БУС необходимо предусмотреть возможность его безопасного использования маломобильными группами населения, людьми с ограниченными возможностями (инвалидами).

Рекомендуется размещать на экране БУС либо в пределах прямой видимости от него предупреждающие сообщения о необходимости соблюдения мер предосторожности при наборе персонального идентификационного номера (ПИН-кода) при использовании БУС.

5.1.2. При выборе места размещения БУС необходимо также учитывать:

- группу БУС по классификации, приведенной в разделе 2;

- категорию места размещения БУС в соответствии с данными, приведенными в разделе 3;

- потенциально возможные для данного класса БУС и категории его размещения криминальные угрозы, а также имеющиеся на данном объекте средства противодействия указанным угрозам, в том числе видеокамеры СОТ, наличие физической охраны, средств

тревожной сигнализации или оперативной связи с полицией, в соответствии с данными, приведенными в разделе 4;

- общую криминогенную обстановку на территории расположения БУС.

5.1.3. Место размещения БУС должно обеспечивать удобство обслуживания и безопасность держателей ИЭК при эксплуатации БУС, а также безопасность работников, осуществляющих инкассацию и техническое обслуживание БУС.

5.1.4. Пространство перед БУС, установленным в помещении, должно быть освещено в соответствии с требованиями СанПиН 2.2.1/2.1.1.1278-03 (п.30 таблицы 2) [10], предъявляемыми к искусственному освещению помещений для обслуживания физических лиц в банковских учреждениях.

Для БУС, установленных вне помещений (на открытой или огороженной территории), должно быть предусмотрено постоянное и охранное освещение в соответствии с РД 78.36.003-2002 МВД России [11].

5.1.5. Не рекомендуется установка БУС рядом с зеркальными поверхностями, в том числе под зеркальными потолками, позволяющими со стороны увидеть процесс ввода ПИН-кода.

5.1.6. Место размещения БУС должно быть выбрано таким образом, чтобы был обеспечен подъезд автомобиля службы инкассации на максимально близкое расстояние к входу в помещение, где расположена зона загрузки БУС.

5.2. Дополнительные требования к выбору мест размещения БУС в зависимости от установленной категории

5.2.1. Требования к местам размещения категории Р1

Место и способ размещения БУС в помещении должны быть выбраны и реализованы таким образом, чтобы не было препятствий для входа и выхода клиентам (пользователям БУС), посетителям и работникам организации (учреждения, предприятия), в которой установлено БУС, работникам службы инкассации и других обслуживающих организаций, сотрудникам полиции (ГЗ СПВО).

Свободная площадь перед БУС должна быть достаточной для размещения на ней нескольких человек (очереди к БУС) на безопасном расстоянии друг от друга, исключающем возможность подглядывания ПИН-кода при обслуживании БУС впереди стоящего клиента и обеспечивающем свободное расположение группы инкассации при загрузке и выгрузке наличных денег.

В нерабочее время БУС должно находиться в сфере действия системы охраны здания и (или) помещения, в котором оно установлено (в зоне действия ТСО, СОТ, физической охраны).

5.2.2. Требования к местам размещения категории Р2

Место размещения БУС должно хорошо просматриваться службой внутренней физической охраны объекта, персоналом организации (учреждения, пред-

приятия), в которой установлено БУС, либо находиться под постоянным дистанционным контролем при помощи видеокамер СОТ.

В месте размещения БУС должна быть предусмотрена так называемая "зона безопасности" необходимая для того, чтобы держатель ИЭК мог без опасений считывания посторонними лицами ввести ПИН-код и забрать наличные денежные средства.

Помещение, где установлено БУС, должно быть оборудовано охранной сигнализацией с передачей извещений на ПЦО вневедомственной охраны и дополнительно – в подразделение безопасности кредитной организации, собственную службу безопасности объекта.

Помещение или участок территории, где установлено БУС, должно быть достаточно освещено (п.5.1.4) и оборудовано видеокамерами СОТ (п.7.3).

5.2.3. Требования к местам размещения категории Р3

Место установки БУС должно находиться:

- в зоне видимости работников охраны, персонала организации и камер видеонаблюдения;
- на максимально возможном удалении от остекленных конструкции внешнего периметра зданий (например, витрин магазинов, окон, стеклянных дверей и т.п.).

Зоны круглосуточного банковского обслуживания ("зоны 24", павильоны для банкоматов) рекомендуется размещать по возможности на оживленных и освещенных территориях поселений, как можно ближе к подразделениям полиции, желательно в пределах видимости телевизионных камер, контролирующих

данную территорию, например, в рамках системы "Безопасный город" и (или) систем видеонаблюдения ближайших организаций (учреждений, предприятий), жилых комплексов.

Снаружи здания (помещения), в котором установлено БУС, рекомендуется применение специальных инженерных сооружений, препятствующих возможности свободного приближения автотранспорта к месту установки БУС, дверным и оконным конструкциям.

Место размещения БУС должно обеспечивать свободный доступ к БУС бригадам инкассации и технических специалистов, в том числе при нештатных ситуациях (пожар, инженерно-технические аварии и т.п.) в нерабочее время.

Договор на установку, эксплуатацию и обслуживание БУС должен предусматривать обязательное согласование с кредитной или платежной организацией, являющейся владельцем БУС, а также подразделением вневедомственной охраны, организующем централизованную охрану БУС, любых его перемещений, в том числе порядок вывоза на техническое обслуживание или утилизацию.

Помещение (участок территории), где установлено БУС, должно быть освещено (п.5.1.4) и оборудовано видеокамерами СОТ (п.7.3).

5.2.4. Требования к местам размещения категории Р4

Место размещения БУС должно быть оборудовано системой охранного освещения в соответствии с требованиями РД 78.36.003-2002 МВД России [11].

Информация о точном местонахождении БУС, включая наименование объекта (железнодорожной платформы, остановки автотранспорта, вокзала), точный адрес объекта, фотографии БУС и места его размещения, координаты местоположения БУС по системе глобальной навигации (GPS, ГЛОНАСС), должна храниться на ПЦО с возможностью ее оперативной выдачи ГЗ СПВО.

Помимо точного указания места нахождения БУС на ПЦО должна быть информация с описанием (картой) прилегающей территории и указанием мест подхода (подъезда) к БУС и имеющихся ближайших средств видеонаблюдения.

Помещение или участок территории, где установлено БУС, должно быть освещено (п.5.1.4) и оборудовано видеокамерами СОТ (п.7.3) и (или) системы "Безопасный город".

Банкоматы или платежные терминалы, относящиеся к группе ОУ или СУ, устанавливаемые на открытой территории городских поселений или выходящие лицевой панелью на улицу, рекомендуется размещать как можно ближе к терминалам городских систем экстренной связи с полицией "Гражданин – Полиция" (п.7.2.10).

6. РЕКОМЕНДАЦИИ ПО ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ УКРЕПЛЕННОСТИ И ОБОРУДОВАНИЮ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ОХРАНЫ БАНКОВСКИХ УСТРОЙСТВ САМООБСЛУЖИВАНИЯ И МЕСТ ИХ РАЗМЕЩЕНИЯ

6.1. Общие положения по защите БУС и мест их размещения от преступных посягательств

6.1.1. В соответствии с рекомендациями Банка России [5] кредитным организациям, в том числе при привлечении специализированных организаций (вневедомственной охраны, мониторинговых компаний), рекомендуется:

- оснащать БУС защитным оборудованием[8] и специальным программным обеспечением[9], при этом их тип, комплектацию и функциональные возможности рекомендуется выбирать с учетом классификации места размещения БУС (раздел 3);

- на регулярной основе, в зависимости от места размещения БУС, контролировать их внешний вид и отсутствие несанкционированного оборудования, а также контролировать порядок действий работников обслуживающих организаций[10];

---

[8] Антискиммингговое оборудование, охранная сигнализация и иное оборудование, предназначенное для предотвращения криминальных посягательств (атак) на БУС.

[9] Программное обеспечение, предназначенное для обнаружения вредоносных компьютерных программ или несанкционированных подключений к БУС.

[10] Организации, осуществляющие операции по загрузке (изъятию) наличных денег, наличной иностранной валюты из

- использовать системы удаленного мониторинга состояния БУС, обеспечивающие контроль надлежащего функционирования защитного оборудования и специального программного обеспечения;

- обеспечивать обнаружение, фиксацию фактов криминальных посягательств на БУС, в том числе попыток их совершения, и информирование о них подразделений обеспечения безопасности кредитных и платежных организаций, соответствующих подразделений МВД России и Банка России;

- проводить анализ и устранять выявленные уязвимости[11] в случаях, когда БУС подверглось атакам или попыткам их совершения;

- совершенствовать применяемые решения и процедуры, направленные на обнаружение, фиксацию, идентификацию и предотвращение криминальных посягательств на БУС или попыток их совершения;

- осуществлять сотрудничество с иными кредитными и специализированными (охранными) организациями, а также осуществлять на регулярной основе обмен информацией в целях развития и совершенствования мер обеспечения безопасности БУС;

- осуществлять крепление БУС к стене или к полу в помещениях и к фундаменту вне помещений (см. пп.6.2.4–6.2.6);

БУС, а также организации, предоставляющие услуги ремонта и (или) профилактики, включая программное обеспечение.

[11] Слабые места в БУС, а также защитном оборудовании и специальном программном обеспечении БУС, которые могут привести к нарушению его работы или безопасности.

- устанавливать БУС с антивандальным исполнением корпуса и панелей.

- оборудовать БУС системами видеонаблюдения (как минимум, двумя видеокамерами) со сроком хранения записей видеосъемки не менее 60 календарных дней. Выбираемые для этих целей видеокамеры и средства видеорегистрации, а также места установки видеокамер (внутри БУС или в зоне его размещения) должны соответствовать требованиям, изложенным в п.7.3.

6.1.2. Вместе с тем, в соответствии с требованиями Банка России [12] помещения для совершения операций с ценностями должны располагаться таким образом, чтобы исключить возможность нахождения в них посторонних лиц, не связанных с осуществлением операций с наличными деньгами, а также визуального наблюдения указанными лицами за транспортировкой наличных денег между помещениями для совершения операций с ценностями.

При размещении кредитной организации (ВСП) в помещениях здания, в котором расположены другие организации, должен быть оборудован отдельный выход из помещений для совершения операций с ценностями, контролируемый службой охраны (сотрудниками службы безопасности) кредитной организации (ВСП) и (или) ТСО.

Площади помещений для совершения операций с ценностями определяются, исходя из необходимости размещения планируемых объемов наличных денег, с условием соблюдения правил пожарной безопасности, противокриминальной защиты и санитарных норм.

Техническая укрепленность помещений для совершения операций с ценностями должна обеспечивать защиту жизни и здоровья работников кредитной и охранной организации (ВСП), сохранность имущества организации, денежных и иных ценностей и достигается применением комплекса необходимых средств противокриминальной защиты, в соответствии с требованиями законодательства Российской Федерации, нормативными правовыми документами Банка России, МВД России, внутренними нормативными документами (инструкциями) кредитной организации (ВСП) и настоящими Рекомендациями.

Помещения для совершения операций с ценностями и БУС должны быть оснащены охранной и тревожной сигнализациями с выводом сигналов на пост охраны кредитной организации (ВСП) и ПЦО СПВО.

Выбор конкретного типа и класса БУС, порядок его установки и оборудование средствами охранной и тревожной сигнализациями, организация охраны БУС и помещений, в которых они установлены, определяются кредитной организацией совместно с подразделением вневедомственной охраны, руководствуясь настоящими Рекомендациями.

Уровень ИТУ помещений для совершения операций с ценностями, конструктивное исполнение и регламентированные защитные свойства, в том числе сейфов БУС, структура охранной и тревожной сигнализаций определяются кредитной организацией (ВСП) совместно с подразделением вневедомственной охраны, в соответствии с настоящими Рекомендациями.

6.2. Требования к инженерно-технической укрепленности БУС

6.2.1. Минимальные требования по устойчивости к взлому сейфов (приложение Б) БУС различных групп (п.2.1), принимаемых под охрану, в зависимости от категории их материальной ценности (п.2.2) и категории мест их размещения (раздел 3), приведены в пп.6.3–6.8.

6.2.2. Для БУС, принимаемых под централизованную охрану, в дополнение к минимальным требованиям, установленным в пп.6.3–6.8, необходимо учитывать следующие положения.

Класс устойчивости сейфа БУС к взлому (подтвержденный сертификатом соответствия) характеризуется определенным минимальным интервалом времени, которое нарушитель вынужден затрачивать для получения доступа к наличным деньгам, размещенным в сейфе. Это время зависит от инструментов и приспособлений по ГОСТ Р 50862-2012, которые чаще всего применяют нарушители для взлома сейфов БУС, а также подготовленности и осведомленности нарушителя о конструкции сейфа БУС и его запирающих механизмов, наличия в месте размещения БУС открытого доступа к электросети (220 В) и других обстоятельств.

Минимальные (согласно экспертной оценке) значения времени (T_1, мин), необходимого квалифицированному нарушителю для взлома сейфа БУС с целью получения доступа к наличным деньгам приведены в таблице 6.1.

Таблица 6.1 – Минимальные оценочные значения времени взлома сейфа БУС

Класс устойчивости сейфа БУС ко взлому по ГОСТ Р 50862-2012	Минимальное оценочное значение времени взлома сейфа БУС (полный доступ), T_1, мин
L	1
I	2
III	5
IV	7

6.2.3. При решении вопроса о принятии БУС, объекта или помещения с установленными БУС под централизованную охрану СПВО необходимо (в дополнение к минимальным требованиям по п.6.2.1) сопоставить значение времени (T_y, мин), определяемое по формуле (6.1), со значением времени (T_p, мин), определяемым по формуле (6.2):

$$T_y = T_1 + T_2 \ , \quad (6.1)$$

$$T_p = T_3 + T_4 + T_5 \quad (6.2)$$

где T_1, – минимальное оценочное значение времени взлома сейфа БУС, соответствующее его классу устойчивости к взлому (таблица 6.1), мин;

T_2, – минимальное оценочное значение времени проникновения нарушителя в охраняемое помещение

с установленным БУС (считается со времени срабатывания первого рубежа сигнализации), мин;

T_3, – максимальное суммарное значение времени срабатывания ТСОС (охранных извещателей, используемых для обнаружения вскрытия БУС), указанное в эксплуатационных документах на ТСОС, мин;

T_4, – максимальное значение времени передачи извещения о тревоге на ПЦН, указанное в эксплуатационных документах на СПИ, мин;

T_5, – максимальное расчетное значение времени прибытия ГЗ СПВО (патрульной группы) на охраняемый объект (к охраняемому БУС), мин.

Если значение время $T_у$ превышает (с тактическим запасом) значение времени $T_р$, то данный БУС и (или) объект с установленными БУС может быть принят под централизованную охрану СПВО. В противном случае необходимо принять меры по усилению ИТУ БУС и (или) места его размещения.

6.2.4. Независимо от места размещения отдельно устанавливаемых БУС групп ОП, ОВ, ОУ необходимо обязательное прочное крепление БУС к полу помещения или специально подготовленному основанию через существующие штатные отверстия в основании БУС, а также дополнительно к стене помещения (если такое крепление предусмотрено конструкцией БУС), в соответствии с требованиями эксплуатационных документов БУС.

6.2.5. Строительная конструкция (пол помещения или специально подготовленное основание), предназначенная для установки БУС, должна быть не ниже 3 класса защиты (см. приложение В).

6.2.6. Крепление БУС к полу, фундаменту или специальному основанию рекомендуется производить четырьмя монтажными анкерными болтами диаметром не менее 18 мм и глубиной закладки не менее 220 мм, с анкерными шайбами толщиной не менее 3 мм.

Конкретные виды и типоразмеры крепежных анкерных болтов должны соответствовать классу устойчивости сейфа БУС по ГОСТ Р 50862-2012, указанному в сертификате соответствия, и требованиям соответствующих эксплуатационных документов на конкретные типы БУС.

Пол или специальное основание под БУС должны выдерживать нагрузку, возникающую в точках установки крепежных анкерных болтов, при силе отрыва по ГОСТ Р 52862-2012.

НЕ ДОПУСКАЕТСЯ принимать под централизованную охрану БУС, не прикрепленные к строительным конструкциям в установленном порядке.

6.2.7. Лицевая панель БУС: монитор, клавиатура для ввода ПИН-кода и другие внешние органы пользовательского интерфейса должны быть устойчивы к криминальным воздействиям, в том числе вандализму или умышленному повреждению (см. приложение Г).

6.2.8. В пп.6.3 – 6.8 приведены рекомендуемые меры по обеспечению необходимого уровня инженерно-технической укрепленности БУС и зон их размещений, оборудованию их ТСОС, ТСАЗ и СОТ, в зависимости от классификации БУС по материальной значимости, конструкции, способу установки, режиму функционирования (раздел 2), а также категории мест размещения БУС (раздел 3).

Примечания

1. Знаком "+" в таблицах 6.2 – 6.7 обозначены рекомендуемые к применению меры (средства) противокриминальной защиты БУС и помещений (зон), в которых они установлены. Знаком "–" обозначены меры (средства) противокриминальной защиты, которые не предназначены для данной категории БУС и (или) мест их размещения.

2. В графах, относящихся к вопросам установки видеокамер СОТ в зонах размещения БУС, число знаков "+" соответствует минимальному числу видеокамер.

3. Выбор конкретных мер (средств) противокриминальной защиты БУС, обозначенных знаком "+/–", производится на этапе комиссионного обследования БУС и места его размещения, с учетом тактических, технических и экономических аспектов организации охраны данного БУС, наличия физической охраны на объекте, удаленности БУС от СПВО, требований противопожарной безопасности для данного помещения и других определяющих факторов.

6.3. Рекомендации по обеспечению противокриминальной защиты БУС группы ОП

6.3.1. Если объект, в помещении которого расположено БУС группы ОП, сдается на охрану СПВО, то уровень ИТУ зоны самообслуживания БУС должен соответствовать требованиям РД.78.36.003-2002 МВД России [9] с учетом настоящих Рекомендаций.

6.3.2. В случае заключения договора на охрану только самого БУС, рекомендуется, чтобы БУС было установлено в отдельном (закрываемом для доступа посетителей в нерабочее время) помещении, оборудованном ТСО и сдаваемом под централизованную охрану СПВО. При этом должен быть обеспечен беспрепятственный доступ ГЗ СПВО в помещение, в котором установлено охраняемое БУС, при поступлении на ПЦО извещения о тревоге.

6.3.3. Рекомендуемые меры противокриминальной защиты БУС группы ОП и помещений, в которых они установлены, приведены в таблице 6.2.

Таблица 6.2 – Рекомендуемые меры защиты БУС группы ОП

Наименование мер защиты БУС		Применение мер защиты БУС в зависимости от категории их ценности и места размещения		
		Р1	Р2	Р3
1. Инженерно-техническая укрепленность БУС				
1.1. Минимальный класс устойчивости сейфа БУС к взлому (приложение Б), подтвержденный сертификатом соответствия	М1	I	III	III
	М2	I	I	III
	М3	L	I	I
1.2. Минимальный класс антивандальной защиты лицевой панели, (экрана) БУС (приложение Г)	М1	IK08	IK08	IK08
	М2	IK08	IK08	IK08
	М3	IK08	IK08	IK08
1.3. Крепление БУС к строительной конструкции (полу и дополнительно к стене[12] помещения), в соответствии с требованиями	М1	+	+	+
	М2	+	+	+
	М3	+	+	+

[12] Если такое дополнительное крепление предусмотрено конструкцией БУС.

эксплуатационных документов БУС				
1.4. Минимальный класс защиты строительной конструкции (приложение В), к которой осуществляется крепление БУС	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
2. Инженерно-техническая укрепленность помещения, в котором установлено БУС				
2.1. Минимальный класс защиты ограждающих строительных конструкций помещения, в котором установлено БУС (приложение В)	М1	3	3	3
	М2	3	3	3
	М3	2	2	2
2.2. Минимальный класс защиты дверной конструкции помещения, в котором установлено БУС (приложение Д)	М1	3	3	3
	М2	3	3	3
	М3	2	2	2
2.3. Минимальный класс защиты остекленных строительных (оконных, витринных) конструкций помещения, в котором установлено БУС (приложение Е)	М1	4	4	4
	М2	4	3	3
	М3	4	3	3
2.4. Оборудование помещения, в котором установлено БУС, СКУД по ИЭК (п.7.9)	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–
	М3	–	–	–

3. Оборудование БУС средствами обнаружения криминальных угроз				
3.1. Блокировка "на открывание" декоративной двери нижнего кабинета банкомата или двери корпуса платежного терминала (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.2. Блокировка "на открывание" основной двери сейфа БУС (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.3. Блокировка (защита от взлома) сейфа БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.4. Блокировка (защита от несанкционированного перемещения) БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.5. Блокировка "на открывание" верхнего кабинета банкомата (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	–	–	–
3.6. Блокировка (защита от взлома) верхнего кабинета банкомата или корпуса платежного терминала (пп.7.1.3, 7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
3.7. Блокировка (защита от взлома и вандализма) лицевой панели БУС (пп.7.1.3, 7.1.6)	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–
	М3	–	–	–

3.8. Оборудование БУС средством защиты от скимминга[13] (п.7.7).	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.9. Оборудование БУС охранно-поисковым средством (п.7.4)	М1	+/–	+	+
	М2	+/–	+/–	+
	М3	–	+/–	+/–
3.10. Установка КТС внутри БУС для защиты обслуживающего персонала и инкассаторов от угрозы разбойного нападения при работе с денежными средствами (п.7.2)	М1	+/–	+	+
	М2	+/–	+	+
	М3	–	–	–
4. Оборудование зоны размещения БУС средствами обнаружения криминальных угроз				
4.1. Блокировка "на открывание" дверной конструкции помещения, в котором установлено БУС (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4.2. Блокировка "на открывание" оконной конструкции помещения, в котором установлено БУС (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4.3. Блокировка "на разрушение" остекленных конструкций (окна, двери)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+

[13] Кроме платежных терминалов, не имеющих считывателя ИЭК

помещения, в котором установлено БУС (п.7.1.2)				
4.4. Блокировка "на разрушение" ограждающих и защитных конструкций помещения, в котором установлено БУС (п.7.1.3)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
4.5. Блокировка "на проникновение" дверных и оконных проемов помещения, в котором установлено БУС (п.7.1.4)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
4.6. Блокировка "на проникновение" внутреннего пространства помещения, в котором установлено БУС (п.7.1.5)	М1	+	+	+/–
	М2	+	+	+/–
	М3	+/–	+/–	+/–
4.7. Блокировка локальной зоны вокруг БУС, вместо блокировки всего помещения по п.4.6 данной таблицы (если такая блокировка нецелесообразна) или в дополнение к ней (п.7.1.5)	М1	+	+	+
	М2	+/–	+/–	+
	М3	+/–	+/–	+
4.8. Установка КТС в зоне размещения БУС для защиты клиентов, персонала организации, инкассаторов от угрозы разбойного нападения при работе с денежными средствами (п.7.2)	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–
	М3	–	–	–

5. Оборудование БУС и зоны его размещения видеокамерами СОТ				
5.1. Установка портретной видеокамеры СОТ внутри БУС или в отдельном антивандальном блоке, замаскированном под составную часть БУС (п.7.3)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
5.2. Установка обзорных видеокамер СОТ в зоне размещения БУС (п.7.3)	М1	++	++	+++
	М2	++	++	++
	М3	+/–	+	+
6. Оборудование БУС средствами активной защиты и оповещения				
6.1. Установка в верхнем кабинете банкомата или внутри корпуса платежного терминала звукового оповещателя с автономным электропитанием (п.7.5.1), включающегося при срабатывании средств обнаружения, установленных по пп.3.1 – 3.9 данной таблицы	М1	+/–	+	+
	М2	+/–	+/–	+
	М3	+/–	+/–	+/–
6.2. Установка в нижнем кабинете банкомата средств зашиты кассет с наличными деньгами (п.7.7)	М1	–	+/–	+/–
	М2	–	–	+/–
	М3	–	–	–
7. Оборудование зоны размещения БУС, средствами активной защиты и оповещения				

7.1. Установка в зоне размещения БУС охранно-дымовой системы, заполняющей помещение туманом, при срабатывании средств обнаружения, установленных по пп.3.1 – 3.9, 4.1, 4.2, 4.5 – 4.7 данной таблицы (п.7.5.3)	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–
7.2. Установка в зоне размещения БУС стробоскопа в дополнение к охранно-дымовой системе, установленной по п.7.1 данной таблицы (п.7.5.2)	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–
7.3. Установка внутри или снаружи помещения, в котором установлено БУС, звукового оповещателя, включающегося при срабатывании средств обнаружения, установленных по пп.3.1 – 3.9, 4.1 – 4.7 данной таблицы (п.7.5.1)	М1	+	+	+
	М2	+/–	+/–	+/–
	М3	–	–	–

6.4. Рекомендации по обеспечению противокриминальной защиты БУС группы ОВ

6.4.1. К помещениям, в которых возможно размещение БУС группы ОВ или СВ, могут быть отнесены:

- специально выделенные помещения банков для дистанционного банковского самообслуживания в круглосуточном режиме ("зона 24");

- проходные организаций, предприятий, учреждений, входные зоны жилых зданий, предприятий торговли, функционирующих в круглосуточном режиме;

- тамбуры основных входов или вестибюли зданий организаций, учреждений или отдельные помещения с выходом на фасадную сторону здания;

- залы ожиданий железнодорожных вокзалов, автовокзалов, терминалов аэропортов;

- вестибюли или переходы метрополитена.

6.4.2. При размещении лицевых панелей БУС напротив остекленной (оконной или дверной) конструкции, через которую возможна их засветка, в том числе засветка портретной видеокамеры, установленной в БУС, рекомендуется применять защитное остекление с солнцезащитным (декоративным) мягким или твердым покрытием по ГОСТ Р 54178-2010 или ГОСТ Р 54179-2010, соответственно.

6.4.3. В зоне самообслуживания должно быть установлено не отключаемое из этой зоны освещение. Устройства (светильники), применяемые для освещения зоны самообслуживания, должны иметь антивандальное исполнение (см. приложение Б), быть вне досягаемости для посторонних лиц, обеспечивать удобство обслуживания клиентов и нормальную работу видеокамер СОТ.

6.4.4. Рекомендуемые меры по обеспечению противокриминальной защиты БУС группы ОВ приведены в таблице 6.3.

Таблица 6.3 – Рекомендуемые меры защиты БУС группы ОВ

Наименование мер защиты БУС	Применение мер защиты БУС в зависимости от категории их ценности и места размещения			
		Р1	Р2	Р3
1. Инженерно-техническая укрепленность БУС				
1.1. Минимальный класс устойчивости сейфа БУС к взлому (приложение Б), подтвержденный сертификатом соответствия	М1	III	IV	IV
	М2	III	III	III
	М3	I	I	I
1.2. Минимальный класс антивандальной защиты лицевой панели БУС (приложение Г)	М1	IK 10	IK1 0	IK1 0
	М2	IK 10	IK1 0	IK1 0
	М3	IK08	IK08	IK08
1.3. Крепление БУС к строительной конструкции (полу и дополнительно к стене[14] помещения)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
1.4. Минимальный класс защиты строительных конструкций (приложение В), к которым осуществляется крепление БУС	М1	3	3	3
	М2	3	3	3
	М3	3	3	3

[14] Если такое дополнительное крепление предусмотрено конструкцией БУС.

2. Инженерно-техническая укрепленность отдельного помещения "зоны 24", оборудованного СКУД по ИЭК				
2.1. Оборудование помещения "зоны 24" СКУД по ИЭК (п.7.9)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
2.2. Минимальный класс защиты ограждающих строительных конструкций помещения "зоны 24" (приложение В)	М1	3	3	3
	М2	3	3	3
	М3	2	2	2
2.3. Минимальный класс защиты внешней дверной конструкции помещения "зоны 24" (приложение Д)	М1	3	3	3
	М2	3	3	3
	М3	2	2	2
2.4. Минимальный класс защиты остекленных строительных конструкций помещения "зоны 24" (приложение Е)	М1	3	3	3
	М2	3	3	3
	М3	2	2	2
3. Оборудование БУС средствами обнаружения криминальных угроз				
3.1. Блокировка "на открывание" декоративной двери нижнего кабинета банкомата или двери корпуса платежного терминала (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.2. Блокировка "на открывание" основной двери сейфа БУС (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+

3.3. Блокировка (защита от взлома) сейфа БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.4. Блокировка (защита от несанкционированного перемещения) БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.6. Блокировка (защита от взлома) верхнего кабинета банкомата или корпуса платежного терминала (пп.7.1.3, 7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	–	–	–
3.7. Блокировка (защита от взлома и вандализма) лицевой панели БУС (пп.7.1.3, 7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
3.8. Оборудование БУС средством защиты от скимминга (п.7.7) [15]	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.9. Оборудование БУС охранно-поисковым средством (п.7.4)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
3.10. Установка КТС внутри БУС для защиты инкассаторов от угрозы разбойного нападения при работе с денежными средствами (п.7.2)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–

[15] Кроме платежных терминалов, не имеющих считывателя ИЭК

4. Оборудование отдельного помещения "зоны 24", оборудованного СКУД по ИЭК, средствами обнаружения криминальных угроз				
4.1. Блокировка "на открывание" дверных конструкций помещения "зоны 24" для защиты от попытки обхода СКУД (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
4.2. Блокировка "на открывание" оконных конструкций помещения "зоны 24" для защиты от проникновения в помещение в обход СКУД (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
4.3. Блокировка "на разрушение" остекленных конструкций (окна, двери) помещения "зоны 24" для защиты от проникновения в помещение в обход СКУД (п.7.1.2)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
4.4. Установка КТС в помещении "зоны 24" для защиты клиентов, обслуживающего персонала и инкассаторов от угрозы разбойного нападения при работе с денежными средствами (п.7.2)	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–
	М3	+/–	+/–	+/–
5. Оборудование БУС и помещения "зоны 24" видеокамерами СОТ				

5.1. Установка портретной видеокамеры СОТ внутри БУС или в отдельном антивандальном блоке, замаскированном под часть БУС (п.7.3)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
5.2. Установка обзорных видеокамер СОТ в зоне размещения БУС (п.7.3)	М1	++	++	+++
	М2	++	++	++
	М3	+	++	++
6. Оборудование БУС средствами активной защиты				
6.1. Установка в верхнем кабинете банкомата или внутри корпуса платежного терминала звукового оповещателя с автономным электропитанием (п.7.5.1), включающегося при срабатывании средств обнаружения, установленных по пп.3.1 – 3.9 данной таблицы	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
6.2. Установка внутри или снаружи БУС средства активной защиты (п.7.5.3.1), активизирующегося при срабатывании средств обнаружения, установленных по пп.3.1 – 3.9 данной таблицы	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–
6.3. Установка в нижнем кабинете банкомата средств защиты кассет с наличными деньгами (п.7.7)	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–
	М3	–	–	–

7. Оборудование помещения "зоны 24" средствами активной защиты и оповещения				
7.1. Установка в зоне размещения БУС охранно-дымовой системы, заполняющей помещение туманом при срабатывании средств обнаружения, установленных по пп.3.1 – 3.9, 4.1, 4.2 данной таблицы (п.7.5.3)	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–
7.2. Установка в зоне размещения БУС стробоскопа в дополнение к охранно-дымовой системе, установленной по п.7.1 данной таблицы (п.7.5.2)	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–
7.3. Установка внутри или снаружи помещения "зоны 24" звукового оповещателя, включающегося при срабатывании средств обнаружения, установленных по пп.3.1 – 3.9, 4.1 – 4.3 данной таблицы (п.7.5.1)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–

6.5. Рекомендации по обеспечению противокриминальной защиты БУС группы ОУ

6.5.1. При обеспечении противокриминальной защиты БУС группы ОУ необходимо учитывать следующие их эксплуатационные особенности.

К банкоматам и платежным терминалам группы ОУ может быть предусмотрен, как круглосуточный, так и регламентированный режимом работы организации (учреждения, предприятия) доступ клиентов для осуществления банковских (платежных) операций.

Банкоматы и платежные терминалы группы ОУ могут быть установлены на огражденных охраняемых территориях организаций, учреждений, предприятий, жилых комплексов (категории размещения Р2, Р3), в том числе с использованием специальных шлюзовых кабин безопасности (см. п.7.10).

Платежные терминалы (в том числе паркоматы, инфокиоски) могут быть установлены также на открытых территориях поселений (площадях, тротуарах, подземных или надземных переходах), платформах железнодорожных станций, остановках общественного транспорта (категория размещения Р4).

6.5.2. Конструктивное исполнение БУС группы ОУ должно соответствовать условиям эксплуатации БУС, учитывать возможные для данной местности перепады температуры и влажности воздуха, обеспечивать необходимую защиту от воздействия внешних факторов (дождя, града, снега, ветра, грозовых разрядов, пыли, грязи, различных химических реагентов, используемых для обработки дорог, платформ, тротуаров и т.п.).

6.5.3. Банкоматы, относящиеся к категории материальной ценности М1, не рекомендуется устанавливать на открытых участках объектов, относящихся к категории размещения Р4, по причине высокого риска воз-

никновения криминальных угроз в отношении большого объема материальных ценностей (наличных денег).

6.5.4. При необходимости, банкоматы, относящиеся к категориям материальной ценности М1, М2, могут быть установлены на огражденных охраняемых участках территорий объектов, относящихся к категории размещения Р2 – Р4 при условии размещения их в специальных шлюзовых кабинах безопасности (см. п.7.10), оборудованных КТС, СОТ, СКУД, ТСАЗ.

6.5.5. В зоне самообслуживания БУС группы ОУ должно быть предусмотрено охранное освещения по РД 78.36.003-2002 МВД России [10]. При этом устройства (светильники), применяемые для освещения зоны самообслуживания БУС, должны иметь антивандальное исполнение (приложение Б), быть вне досягаемости для посторонних лиц, обеспечивать удобство обслуживания клиентов и нормальную работу видеокамер СОТ, установленных в БУС и зонах их размещения.

6.5.6. Если БУС группы ОУ установлено на огороженной охраняемой территории, то ИТУ ограждения зоны самообслуживания в этом случае должна соответствовать требованиям РД 78.36.003-2002 МВД России [11] (быть не ниже 3 класса защиты).

6.5.7. Если к зоне самообслуживания БУС группы ОУ имеется возможность подъезда автотранспорта, то пути подъезда рекомендуется оборудовать СКУД с автоматическими дорожными барьерами, блокирующими свободный проезд автотранспорта, кроме автомобилей службы инкассации и ГЗ СПВО.

6.5.8. Рекомендуемые меры по обеспечению противокриминальной защиты БУС группы ОУ приведены в таблице 6.4.

Таблица 6.4 – Рекомендуемые меры защиты БУС группы ОУ

Наименование мер защиты БУС	Применение мер защиты БУС в зависимости от категории их ценности и места размещения			
		Р2	Р3	Р4
1. Инженерно-техническая укрепленность БУС				
1.1. Минимальный класс устойчивости сейфа БУС к взлому (приложение Б), подтвержденный сертификатом соответствия	М1	III	IV	IV
	М2	III	III	III
	М3	I	I	III
1.2. Минимальный класс антивандальной защиты лицевой панели БУС (приложение Г)	М1	IK10	IK10	IK10
	М2	IK10	IK10	IK10
	М3	IK10	IK10	IK10
1.3. Крепление БУС к строительной конструкции (полу), специальному основанию, дополнительно[16] к капитальной стене здания или ограждающей конструкции зоны размещения БУС (п.6.5.3)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+

[16] Если такое дополнительное крепление предусмотрено конструкцией БУС.

1.4. Минимальный класс защиты строительной конструкции (приложение В), к которой осуществляется крепление БУС	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
1.5. Установка БУС в специальную шлюзовую кабину безопасности (п.7.10), оборудованную СКУД по ИЭК с функцией "вход по одному", КТС и СОТ	М1	+	+	+
	М2	+	+	+
	М3	–	–	–
2. Инженерно-техническая укрепленность зоны размещения БУС				
2.1. Минимальный класс защиты строительной конструкции (приложение В), к которой осуществляется крепление БУС	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
2.2. Минимальный класс защиты ограждающих конструкций (п.6.5.3) зоны размещения БУС, установленного на огражденной территории	М1	3	3	3
	М2	3	3	3
	М3	2	2	2
3. Оборудование БУС средствами обнаружения криминальных угроз				
3.1. Блокировка "на открывание" декоративной двери нижнего кабинета банкомата или двери корпуса платежного терминала (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+

3.2. Блокировка "на открывание" основной двери сейфа БУС (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.3. Блокировка (защита от взлома) сейфа БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.4. Блокировка (защита от несанкционированного перемещения) БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.5. Блокировка "на открывание" верхнего кабинета банкомата (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	–	–	–
3.6. Блокировка (защита от взлома) верхнего кабинета банкомата или корпуса платежного терминала (пп.7.1.3, 7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.7. Блокировка (защита от взлома и вандализма) лицевой панели БУС (пп.7.1.3, 7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.8. Оборудование БУС средством защиты от скимминга (п.7.7) [17]	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.9. Оборудование БУС системой позиционирования и поиска БУС в случае	М1	+	+	+
	М2	+	+	+
	М3	+	+	+

[17] Кроме платежных терминалов, не имеющих считывателя ИЭК

его несанкционированного перемещения (п.7.4)				
3.10. Установка КТС внутри БУС для защиты инкассаторов от угрозы разбойного нападения при работе с денежными средствами (п.7.2)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4. Оборудование БУС и зоны его размещения видеокамерами СОТ				
4.1. Установка портретной видеокамеры СОТ в БУС или в отдельном антивандальном блоке, замаскированном под часть БУС (п.7.3)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
4.2. Установка обзорных видеокамер СОТ в зоне размещения БУС (п.7.3)	М1	+++	+++	+++
	М2	++	+++	+++
	М3	++	++	++
5. Оборудование БУС средствами активной защиты				
5.1. Установка в верхнем кабинете банкомата или платежном терминале звукового оповещателя с автономным электропитанием (п.7.5.1), включающегося при срабатывании средств обнаружения, установленных по пп.3.1 – 3.9 данной таблицы.	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
6.3. Установка в нижнем кабинете банкомата средств защиты кассет с наличными деньгами (п.7.7)	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–
	М3	–	–	–

6.6. Рекомендации по обеспечению противокриминальной защиты БУС группы СП

6.6.1. В большинстве случаев БУС группы СП (встроенные во внутреннюю стену помещения) устанавливаются в операционных залах кредитных, платежных или иных организаций, где проводится дистанционное банковское обслуживания граждан (клиентов, посетителей, покупателей).

6.6.2. Место установки БУС должно обеспечивать возможность визуального контроля (со стороны персонала организации или работников охраны) действий клиентов при осуществлении банковских (платежных) операций с помощью БУС.

6.6.3. Режим функционирования БУС группы СП, как правило, определяется режимом работы организации (учреждения, предприятия), в которой они установлены.

6.6.4. Уровень ИТУ помещений, отведенных для зоны самообслуживания и сервисной зоны БУС, оборудование их ТСОС, СОТ и СКУД должны соответствовать требованиями РД 78.36.003-2002 МВД России [10] для соответствующей категории объектов с учетом рекомендаций, приведенных в таблице 6.5.

6.6.5. Указанные в п.6.6.4 помещения должны иметь не менее двух рубежей охранной сигнализации, а установленные в них БУС должны быть защищены отдельным (третьим или выше) рубежом охранной сигнализации.

6.6.6. В помещении сервисной зоны БУС категорий М1, М2 для обнаружения перемещения нарушителя в охраняемой зоне рекомендуется устанавливать не менее двух охранных извещателей, основанных

на различных физических принципах обнаружения или комбинированный извещатель.

Рекомендуемые меры по обеспечению противокриминальной защиты БУС группы СП приведены в таблице 6.5.

Таблица 6.5 – Рекомендуемые меры защиты БУС группы СП

Наименование мер защиты БУС		Применение мер защиты БУС в зависимости от категории их ценности и места размещения		
		Р1	Р2	Р3
1. Инженерно-техническая укрепленность БУС				
1.1. Минимальный класс устойчивости сейфа БУС к взлому (приложение Б), подтвержденный сертификатом соответствия	М1	I	I/II I	III
	М2	I	I	III
	М3	L	I	I
1.2. Минимальный класс антивандальной защиты лицевой панели БУС (приложение Г)	М1	IK08	IK 10	IK 10
	М2	IK08	IK 08	IK 10
	М3	IK08	IK08	IK08
1.3. Минимальный класс защиты строительной конструкции (приложение В), в которую встроено БУС	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
2. Инженерно-техническая укрепленность зоны самообслуживания				

2.1. Минимальный класс защиты ограждающих строительных конструкций зоны самообслуживания[18] (приложение В)	М1	2	3	3
	М2	2	2	3
	М3	2	2	2
2.2. Минимальный класс защиты дверной конструкции[19] зоны самообслуживания (приложение Д)	М1	2	2	2
	М2	2	2	2
	М3	2	2	2
2.3. Минимальный класс защиты остекленных строительных конструкций зоны самообслуживания (приложение Е)	М1	4	3	3
	М2	4	3	3
	М3	4	3	3
3. Инженерно-техническая укрепленность сервисной зоны				
3.1. Минимальный класс защиты ограждающих строительных конструкций сервисной зоны (приложение В)	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
3.2. Минимальный класс защиты дверной конструкции сервисной зоны (приложение Д)	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
3.3. Минимальный класс защиты остекленных строи-	М1	4	4	4
	М2	4	4	4

[18] Кроме строительной конструкции, в которую встроено БУС (см. п.1.3 данной таблицы).

[19] Кроме дверной конструкции, ведущей из зоны самообслуживания в сервисную зону (см. п.3.2 данной таблицы).

тельных конструкций сервисной зоны (приложение Е)	М3	4	3	3
4. Оборудование БУС средствами обнаружения криминальных угроз				
4.1. Блокировка "на открывание" основной двери сейфа БУС (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4.2. Блокировка (защита от взлома) сейфа БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4.3. Блокировка "на открывание" верхнего кабинета банкомата (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	–	–	–
4.4. Блокировка (защита от взлома) корпуса верхнего кабинета банкомата или корпуса платежного терминала (п.7.1.6)	М1	+/–	+	+
	М2	+/–	+/–	+
	М3	+/–	+/–	+/–
4.5. Блокировка (защита от взлома и вандализма) лицевой панели БУС (п.7.1.6)	М1	+/–	+	+
	М2	+/–	+/–	+
	М3	+/–	+/–	+/–
4.6. Оборудование БУС средством защиты от скимминга (п.7.7) [20]	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
5. Оборудование зоны самообслуживания средствами обнаружения криминальных угроз				

[20] Кроме платежных терминалов, не имеющих считывателя ИЭК

5.1. Блокировка "на открывание" дверных конструкций помещения зоны самообслуживания (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
5.2. Блокировка "на открывание" оконных конструкций помещения зоны самообслуживания (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
5.3. Блокировка "на разрушение" остекленных конструкций (окна, двери) помещения зоны самообслуживания (п.7.1.2)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
5.4. Блокировка "на разрушение" ограждающих и защитных конструкций помещения зоны самообслуживания (пп.7.1.3, 7.1.6)	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–
	М3	+/–	+/–	+/–
5.5. Блокировка "на проникновение" дверных и оконных проемов помещения зоны самообслуживания (п.7.1.4)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
5.6. Блокировка "на проникновение" внутреннего пространства помещения (п.7.1.5)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
5.7. Оборудование помещения зоны самообслуживания СКУД по ИЭК (п.7.9)	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–
	М3	+/–	+/–	+/–
5.8. Установка КТС в помещении зоны самообслу-	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–

живания для защиты клиентов от угрозы разбойного нападения при работе с денежными средствами (п.7.2)	М3	+/–	+/–	+/–
6. Оборудование сервисной зоны средствами обнаружения криминальных угроз				
6.1. Блокировка "на открывание" дверной конструкции помещения сервисной зоны (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
6.2. Блокировка "на открывание" оконной конструкции помещения сервисной зоны (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
6.3. Блокировка "на разрушение" стекол в оконной конструкции помещения сервисной зоны (п.7.1.2)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
6.4. Блокировка "на разрушение" ограждающих и защитных конструкций помещения сервисной зоны (пп.7.1.3, 7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
6.5. Блокировка "на проникновение" дверных и оконных проемов помещения сервисной зоны (п.7.1.4)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
6.6. Блокировка "на проникновение" внутреннего пространства помещения сервисной зоны (п.7.1.5)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+

7. Оборудование БУС, зоны самообслуживания и сервисной зоны видеокамерами СОТ				
7.1. Установка портретной видеокамеры СОТ внутри БУС или в отдельном антивандальном блоке, замаскированном под составную часть БУС (п.7.3)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
7.2. Установка обзорных видеокамер СОТ в зоне самообслуживания (п.7.3)	М1	+	+	++
	М2	+/–	+	+
	М3	+/–	+/–	+/–
7.3. Установка обзорных видеокамер СОТ в сервисной зоне (п.7.3)	М1	++	++	++
	М2	+	+	++
	М3	+/–	+/–	+/–
7. Оборудование сервисной зоны средствами оповещения и активной защиты				
7.1.Установка в помещении сервисной зоны охранно-дымовой системы, заполняющей помещение туманом при срабатывании средств обнаружения, установленных по пп.6.1, 6.2, 6.6 данной таблицы (п.7.5.3)	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–
7.2. Установка в помещении сервисной зоны стробоскопа в дополнение к охранно-дымовой системе, установленной по п.7.1 данной таблицы (п.7.5.2)	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–
7.3. Установка внутри или	М1	+	+	+

снаружи помещения сервисной зоны звукового оповещателя, включающегося при срабатывании средств обнаружения, установленных по пп.5.1 – 5.7, 6.1 – 6.6 данной таблицы (п.7.5.3)	М2	+/–	+/–	+/–
	М3	–	–	–

6.7. Рекомендации по обеспечению противокриминальной защиты БУС группы СВ

6.7.1. Рекомендуемые меры по обеспечению противокриминальной защиты БУС группы СВ приведены в пп.6.4.1–6.4.3, а также в таблице 6.6 (с учетом конструктивных особенностей БУС группы СВ).

Таблица 6.6 – Рекомендуемые меры защиты БУС группы СВ

Наименование мер защиты БУС	Применение мер защиты БУС в зависимости от категории их ценности и места размещения			
		Р1	Р2	Р3
1. Инженерно-техническая укрепленность БУС				
1.1. Минимальный класс устойчивости сейфа БУС к взлому (приложение Б), подтвержденный сертификатом соответствия	М1	I	I/II I	III
	М2	I	I	III
	М3	L	I	I
1.2. Минимальный класс ан-	М1	IK1	IK	IK

тивандальной защиты лицевой панели БУС (приложение Г)		0	10	10
	М2	IK10	IK 10	IK 10
	М3	IK08	IK 08	IK 08
1.3. Минимальный класс защиты строительной конструкции (приложение В), в которую встроено БУС	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
2. Инженерно-техническая укрепленность помещения зоны самообслуживания ("зоны 24"), оборудованного СКУД по ИЭК				
2.1. Оборудование помещения зоны самообслуживания ("зоны 24") СКУД по ИЭК (п.7.9)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
2.2. Минимальный класс защиты ограждающих строительных конструкций помещения зоны самообслуживания ("зоны 24")[21] (приложение В)	М1	2	3	3
	М2	2	2	3
	М3	2	2	2
2.3. Минимальный класс защиты дверной конструкции[22] зоны самообслуживания ("зоны 24") (приложение Г)	М1	2	3	3
	М2	2	2	3
	М3	2	2	2

[21] Кроме строительной конструкции, в которую встроено БУС (см. п.1.3 данной таблицы).

[22] Кроме дверной конструкции, ведущей из зоны самообслуживания ("зоны 24") в сервисную зону (см. п.3.2 данной таблицы).

2.4. Минимальный класс защиты остекленных строительных конструкций зоны самообслуживания ("зоны 24") (приложение Д)	М1	3	3	3
	М2	3	3	3
	М3	2	2	2
3. Инженерно-техническая укрепленность помещения сервисной зоны				
3.1. Минимальный класс защиты ограждающих строительных конструкций сервисной зоны (приложение В)	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
3.2. Минимальный класс защиты дверной конструкции сервисной зоны (приложение Г)	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
3.3. Минимальный класс защиты остекленных строительных конструкций сервисной зоны (приложение Д)	М1	4	4	4
	М2	4	4	4
	М3	4	3	3
4. Оборудование БУС средствами обнаружения криминальных угроз				
4.1. Блокировка "на открывание" основной двери сейфа БУС (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4.2. Блокировка (защита от взлома) сейфа БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4.3. Блокировка "на открывание" верхнего кабинета банкомата (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	–	–	–

4.4. Блокировка (защита от взлома) корпуса верхнего кабинета банкомата или корпуса платежного терминала (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
4.5. Блокировка (защита от взлома и вандализма) лицевой панели БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
4.6. Оборудование БУС средством защиты от скимминга (п.7.7) [23]	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
5. Оборудование зоны самообслуживания средствами обнаружения криминальных угроз				
5.1. Оборудование помещения зоны самообслуживания ("зоны 24") СКУД по ИЭК (п.7.9)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
5.2. Блокировка "на открывание" дверной конструкции помещения зоны самообслуживания ("зоны 24") для защиты от попытки обхода СКУД (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
5.3. Блокировка "на открывание" оконных конструкций помещения зоны самообслуживания ("зоны 24") для защиты от проникнове-	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–

[23] Кроме платежных терминалов, не имеющих считывателя ИЭК

ния в обход СКУД (п.7.1.1)				
5.4. Блокировка "на разрушение" остекленных конструкций (окна, двери) помещения зоны самообслуживания ("зоны 24") для защиты от проникновения в обход СКУД (п.7.1.2)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
5.5. Установка КТС в помещении зоны самообслуживания ("зоны 24") для защиты клиентов от угрозы разбойного нападения при работе с денежными средствами (п.7.2)	М1	+/–	+/–	+/–
	М2	+/–	+/–	+/–
	М3	+/–	+/–	+/–
6. Оборудование сервисной зоны средствами обнаружения криминальных угроз				
6.1. Блокировка "на открывание" дверной конструкции помещения сервисной зоны (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
6.2. Блокировка "на открывание" оконной конструкции помещения сервисной зоны (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
6.3. Блокировка "на разрушение" остекленных конструкций помещения сервисной зоны (п.7.1.2)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
6.4. Блокировка "на разрушение" ограждающих и за-	М1	+	+	+
	М2	+	+	+

щитных конструкций помещения сервисной зоны (пп.7.1.3, 7.1.6)	М3	+	+	+
6.5. Блокировка "на проникновение" дверных и оконных проемов помещения сервисной зоны (п.7.1.4)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
6.6. Блокировка "на проникновение" внутреннего пространства помещения сервисной зоны (п.7.1.5)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
7. Оборудование БУС, зоны самообслуживания и сервисной зоны видеокамерами СОТ				
7.1. Установка портретной видеокамеры СОТ внутри БУС или в отдельном антивандальном блоке, замаскированном под составную часть БУС (п.7.3)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
7.2. Установка обзорных видеокамер СОТ в зоне самообслуживания (п.7.3)	М1	+	++	++
	М2	+	+	++
	М3	+/–	+/–	+/–
7.3. Установка обзорных видеокамер СОТ в сервисной зоне (п.7.3)	М1	++	++	++
	М2	+	+	++
	М3	+/–	+/–	+/–
8. Оборудование сервисной зоны средствами оповещения и активной защиты				
8.1. Установка в помещении сервисной зоны охранно-дымовой системы, заполняющей помещение тума-	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–

ном при срабатывании средств обнаружения, установленных по пп.6.1 – 6.6 данной таблицы (п.7.5.3)				
8.2. Установка в помещении сервисной зоны стробоскопа в дополнение к охранно-дымовой системе, установленной по п.8.1 данной таблицы (п.7.5.2)	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–
8.3. Установка внутри или снаружи помещения сервисной зоны звукового оповещателя, включающегося при срабатывании средств обнаружения, установленных по пп.6.1 – 6.6 данной таблицы (п.7.5.1)	М1	+	+	+
	М2	+/–	+/–	+/–
	М3	–	–	–

6.8. Рекомендации по обеспечению противокриминальной защиты БУС группы СУ

6.8.1. В зоне самообслуживания БУС, относящихся к группе СУ, должно быть предусмотрено охранное освещение по РД 78.36.003-2002 МВД России [11]. При этом устройства (светильники), применяемые для освещения зоны самообслуживания, должны иметь антивандальное исполнение (приложение Б), располагаться вне пределов досягаемости для посторонних лиц, обеспечивать удобство обслуживания клиентов и нормальную работу видеокамер СОТ.

6.8.2. Если лицевая панель с пользовательским интерфейсом БУС выходит на открытую территорию городского поселения, то желательно, чтобы этот участок территории находился в пределах видимости телевизионных камер, контролирующих данную территорию, например, в рамках системы "Безопасный город" и (или) систем видеонаблюдения ближайших государственных или муниципальных учреждений, коммерческих организаций или предприятий.

Рекомендуемые меры по обеспечению противокриминальной защиты БУС группы СУ приведены в таблице 6.7.

Таблица 6.7 – Рекомендуемые меры защиты БУС группы СУ

Наименование мер защиты БУС	Применение мер защиты БУС в зависимости от категории их ценности и места размещения			
		Р2	Р3	Р4
1. Инженерно-техническая укрепленность БУС				
1.1. Минимальный класс устойчивости сейфа БУС к взлому (приложение Б), подтвержденный сертификатом соответствия	М1	I	I/II I	III
	М2	I	I	III
	М3	L	I	I
1.2. Минимальный класс антивандальной защиты лицевой панели БУС (приложение Г)	М1	IK 10	IK 10	IK 10
	М2	IK10	IK1 0	IK 10
	М3	IK	IK	IK

		08	08	08
1.3. Минимальный класс защиты строительной конструкции (приложение В), в которую встроено БУС	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
1.4. Размещение лицевой панели БУС в специальной шлюзовой кабине безопасности (п.7.10), оборудованной СКУД по ИЭК с функцией "вход по одному", КТС и СОТ	М1	+/–	+	+
	М2	+/–	+/–	+
	М3	–	–	–
2. Инженерно-техническая укрепленность помещения сервисной зоны				
2.1. Минимальный класс защиты ограждающих строительных конструкций сервисной зоны (приложение В)	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
2.2. Минимальный класс защиты дверной конструкции сервисной зоны (приложение Д)	М1	3	3	3
	М2	3	3	3
	М3	3	3	3
2.3. Минимальный класс защиты остекленных строительных конструкций сервисной зоны (приложение Е)	М1	4	4	4
	М2	4	4	4
	М3	4	3	3
3. Оборудование БУС средствами обнаружения криминальных угроз				
3.1. Блокировка "на открывание" основной двери сейфа БУС (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
3.2. Блокировка (защита от	М1	+	+	+

взлома) сейфа БУС (п.7.1.6)	М2	+	+	+
	М3	+	+	+
3.3. Блокировка "на открывание" верхнего кабинета банкомата (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	–	–	–
3.4. Блокировка (защита от взлома) корпуса верхнего кабинета банкомата или корпуса платежного терминала (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
3.5. Блокировка (защита от взлома и вандализма) лицевой панели БУС (п.7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
3.6. Оборудование БУС средством защиты от скимминга (п.7.7) [24]	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4. Оборудование сервисной зоны средствами обнаружения криминальных угроз				
4.1. Блокировка "на открывание" дверной конструкции помещения сервисной зоны (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4.2. Блокировка "на открывание" оконной конструкции помещения сервисной зоны (п.7.1.1)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4.3. Блокировка "на разрушение" стекол оконной конструк-	М1	+	+	+
	М2	+	+	+

[24] Кроме платежных терминалов, не имеющих считывателя ИЭК

ции помещения сервисной зоны (п.7.1.2)	М3	+	+	+
4.4. Блокировка "на разрушение" ограждающих и защитных конструкций помещения сервисной зоны (пп.7.1.3, 7.1.6)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
4.5. Блокировка "на проникновение" дверных и оконных проемов помещения сервисной зоны (п.7.1.4)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
4.6. Блокировка "на проникновение" внутреннего пространства помещения сервисной зоны (п.7.1.5)	М1	+	+	+
	М2	+	+	+
	М3	+	+	+
5. Оборудование БУС, зоны самообслуживания и сервисной зоны видеокамерами СОТ				
5.1. Установка портретной видеокамеры СОТ внутри БУС или отдельном антивандальном блоке, замаскированном под составную часть БУС (п.7.3)	М1	+	+	+
	М2	+	+	+
	М3	+/–	+/–	+/–
5.2. Установка обзорных видеокамер СОТ в зоне самообслуживания (п.7.3)	М1	++	++	++
	М2	+	++	++
	М3	+/–	+	+
5.3. Установка обзорных видеокамер СОТ в сервисной зоне (п.7.3)	М1	++	++	++
	М2	+	++	++
	М3	+/–	+/–	+/–
6. Оборудование сервисной зоны средствами оповещения и активной защиты				
6.1. Установка в помещении сервисной зоны охранно-дымовой системы, заполняю-	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–

щей помещение туманом при срабатывании средств обнаружения, установленных по пп.4.1 – 4.6 данной таблицы (п.7.5.3)				
6.2. Установка в помещении сервисной зоны стробоскопа в дополнение к охранно-дымовой системе, установленной по п.6.1 данной таблицы (п.7.5.2)	М1	+/–	+/–	+/–
	М2	–	–	–
	М3	–	–	–
6.3. Установка внутри или снаружи помещения сервисной зоны звукового оповещателя, включающегося при срабатывании средств обнаружения, установленных по пп.4.1 – 4.6 данной таблицы (п.7.5.1)	М1	+	+	+
	М2	+/–	+/–	+/–
	М3	–	–	–

7. РЕКОМЕНДАЦИИ ПО ВЫБОРУ ОБОРУДОВАНИЯ ДЛЯ ОРГАНИЗАЦИИ КОМПЛЕКСНОЙ ОХРАНЫ БАНКОВСКИХ УСТРОЙСТВ САМООБСЛУЖИВАНИЯ

Эффективность мер, принимаемых для обеспечения защиты БУС от преступных посягательств, во многом зависит от правильности выбора и применения технических средств охраны, в первую очередь – средств обнаружения криминальных посягательств на БУС (охранных извещателей), а также средств тревожной сигнализации, систем охранного телевидения, охранно-поисковых устройств, средств активной защиты и оповещения, специальных кассет, антискимминговых устройств, систем передачи извещений, систем контроля и управления доступом, других средств обеспечения безопасности БУС, при условии соблюдения требований к инженерно-технической укрепленности (раздел 6), причем, как самих БУС, так и зон их размещения (зон самообслуживания, сервисных зон).

Для организации комплексной централизованной охраны БУС и зон их размещения рекомендуется прежде всего использовать технические средства охраны, приведенные в "Списке технических средств безопасности, удовлетворяющих "Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны" и "Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подраз-

делениях вневедомственной охраны" [13] (далее – "Список ТСО"). В дополнение к ним могут быть установлены технические средства охранной сигнализации и противокриминальной защиты БУС, указанные в пп.7.1 – 7.8, выбираемые в соответствии с возможными криминальными угрозами БУС, описанными в разделе 4, с учетом рекомендаций, приведенных в разделе 6 для различных групп БУС, в зависимости от категории их материальной значимости (М1 – М3) и места размещения (Р1 – Р4).

7.1. Средства обнаружения проникновения

В качестве средств обнаружения незаконного проникновения на охраняемый объект или в охраняемую зону (см. раздел 4) в составе комплекса ТСО, как правило, используются охранные извещатели различного назначения и принципа действия, применяемые для защиты, как самих БУС от преступных посягательств (взлома, повреждения, вандализма, несанкционированного перемещения), так и помещений, в которых они установлены (зоны самообслуживания, сервисной зоны) от незаконного проникновения в охраняемое помещение (зону).

Общие организационно-технические вопросы, отражающие особенности выбора, установки и эксплуатации средств обнаружения проникновения и угроз различных видов (охранных извещателей) в зависимости от степени важности и опасности объектов приведены в Р 78.36.028-2012 МВД России [13].

7.1.1. Средства обнаружения криминального открывания БУС и помещений, в которых они установлены

Для блокировки "на открывание" дверных, оконных и иных подвижных строительных (защитных) конструкций помещений, в которых установлены БУС, а также открываемых или перемещаемых конструкций самих БУС, обеспечивающих доступ к их составным частям, в том числе к нижнему и верхнему кабинетам БУС, рекомендуется использовать извещатели охранные точечные магнитоконтактные по ГОСТ Р 54832-2011, которые должны выбираться в соответствии с видами, размерами и материалами охраняемых конструкций.

При выборе конкретных типов магнитоконтактных извещателей, устанавливаемых внутри банкомата, в частности, для блокировки "на открывание" основной двери нижнего кабинета (сейфа) необходимо учитывать ограничения по размерам свободного пространства, связанные с высокой плотностью расположения внутренних механизмов (кассет с наличными деньгами), периодически перемещаемых и извлекаемых при инкассации, а также при обслуживании и ремонте.

Для блокировки "на открывание" пластиковой декоративной двери нижнего кабинета (сейфа) банкомата группы ОП, ОВ или ОУ целесообразно использовать малогабаритные магнитоконтактные извещатели, предназначенные для установки на поверхности стальных конструкций и обладающие функцией защиты от саботажа внешним магнитным полем, поскольку в этом случае исполнительный блок извещателя устанавливается на поверхность стального сейфа, а задающий блок – на поверхность декоративной пластиковой двери банкомата, через которую нарушитель

может оказать умышленное воздействие на извещатель мощным магнитом с целью саботажа его функционирования. Необходимо также иметь в виду, что свободное пространство для установки указанных блоков извещателей на многих моделях банкоматов очень ограничено, поэтому необходимо выбирать извещатели, имеющие соответствующие габаритные размеры.

7.1.2. Средства обнаружения разрушения остекленных конструкций помещений

7.1.2.1. На территории Российской Федерации для остекления строительных конструкций помещений (окон, витрин, дверей, перегородок, стеклянных крыш и фасадов зданий) используют, как правило, листовые стекла по ГОСТ Р 54170-2010, ГОСТ Р 54169-2010, стекла с различными видами низкоэмиссионных, солнцезащитных, декоративных мягких и твердых покрытий по ГОСТ Р 54176-2010, ГОСТ Р 54177-2010, ГОСТ Р 54178-2010, ГОСТ Р 54179 - 2010, закаленные стекла по ГОСТ Р 54162-2010, термоупрочненные стекла по ГОСТ Р 54180-2010, многослойные, обладающие регламентированными защитными свойствами стекла по ГОСТ Р 54171-2010, а также стеклопакеты по ГОСТ Р 54175-2010, выполненные с использованием указанных видов стекол.

7.1.2.2. В охраняемых или принимаемых под охрану помещениях, в которых установлены БУС, необходимо проконтролировать (визуально и по документам), чтобы в остекленных (оконных, дверных) конструкциях были использованы стекла (стеклопакеты), имеющие соответствующий класс защиты, указанный в пп.6.3 – 6.8, соответствующий категории ма-

териальной ценности для данной категории БУС и места его размещения. При этом защитные стекла (стеклопакеты) должны быть установлены в оконные защитные блоки по ГОСТ 31462-2011, имеющие соответствующий класс устойчивости к взлому.

7.1.2.3. Для обнаружения разрушения обычных листовых и защитных стекол, стеклопакетов, а также стекол со специальными свойствами и стеклоблоков различных видов, применяемых в строительных конструкциях помещений, в которых установлены БУС, рекомендуется использовать извещатели охранные поверхностные звуковые по ГОСТ Р 51186-98, обладающие функцией активной защиты от маскирования и автоматического контроля работоспособности, например, извещатель ИО329-10 "Стекло-4".

7.1.3. Средства обнаружения разрушения ограждающих и защитных конструкций помещения

Для обнаружения попытки умышленного разрушения, повреждения или взлома ограждающих строительных и защитных конструкций помещения, в котором установлено БУС, других хранилищ материальных ценностей, рекомендуется использовать извещатели охранные поверхностные вибрационные по ГОСТ Р 53702-2009, способные обнаруживать любые известные средства взлома по ГОСТ Р 50862-2012, выбираемые в соответствии с видами, размерами и материалами охраняемых конструкций, например, извещатель ИО313-5/1 "Шорох-2", контролирующий одну зону (конструкцию), или извещатель ИО313-5/2 "Шорох-2-10", контролирующий от 2 до 10 зон (конструкций).

7.1.4. Средства обнаружения проникновения нарушителя через дверной или оконный проем помещения, в котором установлено БУС

Для обнаружения проникновения нарушителя через дверной или оконный проем помещения, в котором установлено БУС, рекомендуется использовать извещатели охранные поверхностные оптико-электронные (инфракрасные) по ГОСТ Р 50777-95, имеющие поверхностную зону обнаружения типа "ИК штора" и обладающие функцией активной защиты от маскирования, например, извещатель ИО309-14 "Фотон-16Б".

7.1.5. Средства обнаружения перемещения нарушителя в помещении, в котором установлено БУС

Для обнаружения перемещения нарушителя в помещении, в котором установлено БУС (в сервисной зоне), рекомендуется использовать не менее двух извещателей с объемной зоной обнаружения и защитой от маскирования, принцип действия которых (одного из них) должен отличаться от принципа действия извещателя, используемого для блокировки "на проникновение" оконного и дверного проемов (см п.7.1.4).

Для этих целей могут быть использованы оптико-электронные объемные ИК извещатели по ГОСТ Р50777-95 с функцией антимаскирования, например, извещатель ИО409-30 "Фотон-16" совместно с охранным объемным радиоволновым извещателем по ГОСТ Р 50659-2012, например, ИО407-5/4 "Аргус-2" или охранным объемным ультразвуковым извещателем по ГОСТ Р 50658-94, например, ИО408-5 "Эхо-5".

В качестве альтернативы вышеуказанным извещателям, для блокировки внутреннего пространства помещения, в котором установлено БУС, могут быть использованы комбинированные извещатели по ГОСТ Р 52650-2006 или ГОСТ Р 55150-2012, например, ИО414-1 "Сокол-2" (для размещения на стене) или ИО414-3 "Сокол-3" (для размещения на потолке).

7.1.6. Специализированные средства обнаружения взлома и несанкционированного перемещения (хищения) БУС

Для обнаружения взлома нижнего кабинета (сейфа) банкомата или вскрытия корпуса платежного терминала, встроенного в капитальную строительную конструкцию (БУС группы СП, СВ или СУ) могут быть использованы вибрационные извещатели, указанные в п.7.1.3.

Вместе с тем, БУС групп ОП, ОВ, ОУ должны быть защищены не только от взлома (повреждения, вандализма), но и от несанкционированного перемещения (кражи целиком) с целью последующего взлома в удаленном скрытом месте. Для защиты таких БУС рекомендуется использовать совмещенные извещатели, в состав которых входят соответствующие каналы обнаружения на основе датчиков вибрации и перемещения (наклона), например, извещатель ИО315-10 "Шорох-3", специально предназначенный для комплексной защиты банкоматов и платежных терминалов от преступных посягательств.

При организации охраны БУС, к которым предусмотрен круглосуточный доступ клиентов и которые при этом должны находиться под охраной, а также

при сложной помеховой обстановке на объекте (станции метрополитена, вокзалы, аэропорты, помещения с работающим промышленным оборудованием) целесообразно осуществлять раздельную регулировку чувствительности извещателя "Шорох-3" к различным видам воздействий.

Для этих целей в извещателе "Шорох-3" предусмотрена возможность конфигурирования его параметров обнаружения отдельно для каждого вида воздействий (инструментов) с помощью персонального компьютера (ноутбука) и устройство согласования последовательного интерфейса ("УС-ПИ"), поставляемого вместе с извещателем или по отдельному заказу.

Необходимое для этого программное обеспечение можно скачать на официальном сайте предприятия-изготовителя извещателя (http://rielta.ru/). Порядок подключения и конфигурирования параметров извещателя "Шорох-3" с помощью персонального компьютера приведен в эксплуатационных документах извещателя.

7.1.7. Средства обнаружения и защиты от попытки взлома сейфа БУС при помощи взрывных устройств

Одним из наиболее опасных и разрушительных криминальных посягательств на БУС является вскрытие (попытка вскрытия) его нижнего кабинета (сейфа) при помощи взрыва, организуемого злоумышленниками, например, путем наполнения внутренней полости сейфа взрывоопасной смесью[25] и последующего ини-

[25] Смесь горючих газов или паров с воздухом при нормальных атмосферных условиях, у которой при воспламенении горение распространяется на весь объем несгоревшей смеси.

циирования взрыв управляемым электрическим или электростатическим разрядом.

Для противодействия данному виду криминальных угроз в отношении БУС рекомендуется применение следующих мер безопасности.

Сейф БУС (особенно это касается БУС категории ценности М1) должен быть высокого класса устойчивости к взлому (не ниже III класса по ГОСТ Р 50862-2012), в том числе после взрыва, т.е. иметь специальную маркировку "EX" (см. приложение А).

Для защиты нижнего кабинета БУС от попытки проникновения во внутреннее пространство сейфа, предназначенное для хранения наличных денег, должен быть установлен вибрационный извещатель "Шорох-2" (для БУС групп СП, СВ, СУ, см. п.7.1.3) или совмещенный извещатель "Шорох-3" (для БУС групп ОП, ОВ, ОУ, см. п.7.1.6).

По данным специализированных информационных изданий для обнаружения и сигнализации о появлении в сейфе БУС горючего газа на ранней (безопасной) стадии, как правило, на уровне 10–20% НКПР (LEL)[26], могут быть использованы датчики (детекторы) утечки горючих газов, например, природного газа, метана, пропана, бутана, ацетилена, водорода, сжиженного углеводородного газа и др., соответствующие требованиям ГОСТ Р ЕН 50194-2008.

При необходимости обеспечения повышенного уровня безопасности БУС, относящихся к категории

[26] НКПР – нижний концентрационный предел распространения пламени (LEL – lower explosive limit).

ценности М1 и (или) БУС, установленных на критически важных, социально значимых или опасных объектах, где взрыв сейфа БУС может привести к тяжелым последствиям, целесообразно рассматривать вопрос о применении в дополнении к указанным датчикам систем активного подавления взрыва, которые при срабатывании датчиков обеспечивают быстрое введение в защищаемый сейф БУС ингибитора (взрывоподавляющего состава), приостанавливающего дальнейший процесс развития взрыва. Используя такие системы, можно подавлять взрыв настолько эффективно, что в защищаемом пространстве практически не произойдет сколько-нибудь заметного повышения давления, и, следовательно, разрушения оболочки сейфа БУС, а также выброса в атмосферу токсичных и пожаровзрывоопасных продуктов, горячих газов и открытого огня.

Для нейтрализации взрывоопасной смеси такие системы используют флегматизаторы (инертные добавки, которые, изменяя общий химический состав смеси, выводят его за пределы взрываемости) и ингибиторы (вещества, выполняющие роль "отрицательных катализаторов" химической реакции горения).

7.2. Средства тревожной сигнализации

7.2.1. Средства тревожной сигнализации предназначены для передачи сообщений на ПЦО и (или) в дежурную часть органов внутренних дел о противоправных действиях (разбойных нападениях, хулиганских действиях, угрозах) в отношении граждан при осуществлении ими с помощью БУС дистанционного банковского обслуживания (получения наличных денег), а также в отношении персонала организации

(учреждения, предприятия), в которой установлено и функционирует БУС, работников инкассации при работе с денежными средствами.

7.2.2. В качестве средств тревожной сигнализации для обеспечения безопасности при эксплуатации, обслуживании и ремонте БУС могут быть использованы:

- стационарные средства тревожной сигнализации – извещатели охранные ручные точечные электроконтактные (КТС), устанавливаемые внутри БУС, в зоне самообслуживания, в сервисной зоне БУС;

- мобильные средства радиосистем тревожной сигнализации, которыми должны быть оснащены инкассаторы и работники, осуществляющие регламентное обслуживание и (или) экстренный ремонт действующих БУС на местах их постоянного размещения.

7.2.3. В соответствии с требованиями РД 78.36.003-2002 МВД России [11] все помещения для совершения операций с ценностями должны быть оснащены средствами охранной и тревожной сигнализации.

7.2.4. Средства тревожной сигнализации (КТС), в зависимости от группы БУС, категории ценности БУС и места его размещения, с учетом рекомендаций по пп.6.3 – 6.8, устанавливаются в следующих местах:

- внутри нижнего кабинета (сейфа) БУС групп ОП, ОВ, ОУ – для защиты от разбойного нападения на инкассаторов при загрузке (изъятии) наличных денег, на работников кредитной или обслуживающей БУС организации при регламентном обслуживании БУС или его экстренном ремонте на месте постоянного размещения;

- в зоне самообслуживания (в помещении или на участке территории, где установлено БУС) – для защиты от разбойного нападения на клиентов, посетителей или персонал организации при осуществлении ими дистанционного банковского обслуживания или работе с наличными денежными средствами;

- в сервисной зоне (сейфовой комнате) БУС группы СП, СВ или СУ – для защиты от разбойного (вооруженного) нападения на инкассаторов при загрузке (изъятии) наличных денег, на работников кредитной или обслуживающей организации, например, при ремонте БУС на месте постоянного размещения.

7.2.5. В соответствии с требованиями РД 78.36.003-2002 МВД России [11] система тревожной сигнализации организуется "без права отключения".

7.2.6. Средства тревожной сигнализации, используемые для защиты клиентов и персонала от противоправных действий при работе с денежными средствами должны соответствовать требованиям ГОСТ Р 52435-2005, ГОСТ Р 50009-2000, ГОСТ 31817.1.1-2012, ГОСТ IEC 60065-2011.

7.2.7. Стационарные средства тревожной сигнализации (КТС) следует размещать в скрытых местах, определяемых представителем кредитной или платежной организации (подразделения безопасности банка), являющейся собственником охраняемого БУС, представителем организации (учреждения, предприятия), в помещении которой установлено БУС, совместно с представителем подразделения полиции (вневедомственной охраны), осуществляющем оперативное реагирование на извещение о нападении, формируемое КТС.

7.2.8. Банкоматы или платежные терминалы, относящиеся к группе ОУ или СУ, устанавливаемые на открытой территории городских поселений или выходящие лицевой панелью на улицу, рекомендуется размещать как можно ближе к терминалам городских систем экстренной связи с полицией "Гражданин – Полиция".

Такие системы позволяют без набора телефонного номера быстро связаться с органами внутренних дел и попросить помощь в экстренной ситуации или проинформировать о совершаемых (совершенных) преступлениях и правонарушениях. Терминалы таких систем, как правило, снабжены видеокамерой, кнопкой вызова и коммуникационным устройством.

Системы экстренной связи с полицией "Гражданин – Полиция" обычно интегрируют в общегородскую сеть "Безопасный город", к которой, помимо камер уличного видеонаблюдения, подключены системы безопасности торговых комплексов, платформ железнодорожного транспорта, метрополитена (в городах федерального значения) и других общественных мест, устройства дистанционного контроля соблюдения правил дорожного движения, иное специализированное оборудование. Мониторинг происходящего круглосуточно ведут операторы ситуационных центров субъектов Российской Федерации.

К обратившемуся в экстренной ситуации гражданину срочно направляется патрульная группа, в то же время оператор ситуационного центра выясняет все необходимые подробности и быстро выдает соответствующие указания дежурным нарядам полиции.

7.3. Средства охранные телевизионные

7.3.1. Общие требования к СОТ для контроля БУС

Общие вопросы, касающиеся выбора, применения компонентов и структур СОТ для различных категорий объектов, приведены в Рекомендациях Р 78.36.002-2010 МВД России [14].

Для видеонаблюдения в интересах обеспечения безопасности, контроля БУС и зон их размещения (зоны самообслуживания, сервисной зоны) должны применяться средства и системы охранные телевизионные, соответствующие требованиям ГОСТ Р 51558-2008.

В соответствии с рекомендациями Банка России [5] для контроля БУС следует применять СОТ, имеющие в своем составе, как минимум, две видеокамеры, со сроком хранения записей видеосъемки не менее 60 календарных дней. Кроме того, Банк России рекомендует использовать системы удаленного мониторинга, обеспечивающие контроль функционирования защитного оборудования и специального программного обеспечения.

В состав СОТ для контроля БУС должны входить:

- видеокамеры, размещаемые внутри и вне БУС;
- отдельный или совмещенный с управляющим компьютером БУС видеосервер (видеорегистратор), который обычно размещают внутри БУС или в контролируемой зоне с ограниченным доступом (в сервисной зоне, в специальном помещении);
- удаленные автоматизированные рабочие места (АРМ) операторов СОТ, которые могут находиться в

подразделении безопасности кредитной организации (платежного агента) – владельца БУС, мониторинговой компании или на ПЦО охранной организации (СПВО).

7.3.2. Особенности условий работы видеокамер СОТ, применяемых для контроля БУС

7.3.2.1. Особенности условий работы видеокамер, устанавливаемых внутри БУС

В большинстве БУС с функцией выдачи наличных денег устанавливают две внутренние видеокамеры: портретную и презентерную. Кроме того, в современных БУС с функцией приема наличных денег или многофункциональных БУС дополнительно устанавливают валидаторную видеокамеру. Эти три вида видеокамер, устанавливаемых внутри БУС, имеют различные задачи и различные условия работы, что определяет различные требования, предъявляемые к ним.

Целевой задачей портретной видеокамеры является получение четкого изображения лица клиента. Это накладывает дополнительные требования по разрешению видеокамеры, а также связано с размерами сцены по передней границе зоны самообслуживания БУС.

Сцена портретной видеокамеры часто оказывается подвергнута существенной засветке от естественных (солнечный свет) и искусственных источников (лампы освещения, фары транспортных средств). Кроме того, в сцене портретной видеокамеры БУС может наблюдаться значительный перепад уровней освещенностей.

Применительно к целевой задаче портретной видеокамеры, такая ситуация возникает, например, когда в солнечный день на очень светлом фоне на передний план перед видеокамерой выходит человек, находящийся в тени.

Портретная видеокамера может давать максимально информативное изображение ситуации вблизи БУС. В непосредственной близости от лицевой панели БУС (у передней границы зоны самообслуживания) собственной подсветки БУС может быть вполне достаточно. Однако, с отступлением от передней границы зоны самообслуживания недостаточная светочувствительность портретной видеокамеры все больше снижает качество видеозаписей, произведенных в темное время или при слабой освещенности, а также может негативно влиять на обеспечение необходимой глубины видеоархива (требуемого срока хранения видеозаписей).

Это может происходить в результате непродуктивного увеличения размера сжатого кадра, содержащего шумы матрицы видеокамеры, вызванные ее недостаточной светочувствительностью. Алгоритмы компрессии изображения воспринимают их как полезную составляющую, внося информацию о них в сжатый кадр, что не только негативно сказывается на качестве изображения, но и увеличивает размеры файлов.

Указанные особенности характерны для БУС групп ОУ и СУ, однако могут проявляться и в иных случаях.

На практике могут возникнуть случаи, когда портретную видеокамеру невозможно установить и

настроить так, чтобы исключить из ее сцены область набора ПИН-кода (либо в сцену видеокамеры попадает область набора ПИН-кода другого БУС). В таком случае, ПИН-код ИЭК клиента может быть скомпрометирован (стать известным посторонним лицам, например, работникам подрядной организации, занимающейся техническим обслуживанием СОТ БУС или сотрудникам кредитной организации).

Целевые задачи презенторной и валидаторной видеокамер не связаны с получением изображения лица человека. Основное назначение этих камер – контроль действий клиента в процессе сеанса самообслуживания с помощью БУС при проведении операций с наличными денежными средствами. При этом желательно иметь возможность по изображению определить номинал купюр. Сцены этих камер, как правило, чрезвычайно малы, поскольку наблюдаемые объекты (презенторы и валидаторы БУС) находятся в нескольких сантиметрах или десятках сантиметров от самих видеокамер в силу конструктивных особенностей БУС.

В некоторых случаях, в зависимости от конструкции БУС, места размещения презентора (валидатора) и, соответственно, презенторной (валидаторной) видеокамер, есть вероятность попадания в поля их зрения клавиатуры для ввода ПИН-кода этого (или другого) БУС, либо номера ИЭК клиента во время начала (окончания) сеанса самообслуживания. В связи с этим необходимо соблюдать рекомендации по установке и настройке таких видеокамер, изложенные в п.7.3.3.1.

7.3.2.2. Особенности работы видеокамер, устанавливаемых в зоне размещения БУС

Как показывает практика, применение для контроля только видеокамер, установленных внутри БУС или в специальных, представляющих собой конструктивно часть БУС, модулях, не дает возможности надежной видеофиксации и дальнейшего восстановления хода событий, в том числе при проведении оперативных мероприятия (проверок, исследований, экспертиз) в процессе расследования фактов криминальных посягательств на БУС (установки скиммеров и других несанкционированных устройств, взлома сейфа БУС, похищение БУС целиком). Это связано с естественными ограничениями, вызванными целевыми задачами видеокамер и условиями их размещения.

Для повышения эффективности применения СОТ для охраны БУС рекомендуется, в зависимости от способа установки, категории материальной ценности и места размещения конкретного БУС, применение дополнительных обзорных видеокамер.

При размещении в зонах повышенной (п.3.3) и высокой (п.3.4) степени риска существует вероятность саботажа (закрашивание или перекрытие оптической системы камеры, разворачивание, уничтожение) дополнительных обзорных видеокамер. Для защиты от таких видов криминальных угроз целесообразно применение специальных мер защиты, которые могут быть реализованы, как аппаратными, так программными средствами СОТ.

Обзорные видеокамеры являются важным источником информации о событиях, происходящих

в зонах размещения БУС и вблизи них. Как правило, эти зоны имеют освещенность, обеспечивающую комфортную работу клиентов в зоне самообслуживания, сотрудников кредитной организации – владельца БУС, подрядной организации, выполняющей работы в ее интересах. инкассаторов, обслуживающего персонала. Исключение составляют случаи умышленного ухудшения условий освещенности при криминальных посягательствах на БУС (вывод из строя источников освещения). Недостаточная светочувствительность обзорных видеокамер в этом случае может привести к потере существенной части важной информации.

В сценах обзорных видеокамер могут оказаться, как кратковременные, так и длительные фоновые источники яркого света (например, при контроле входа в помещение в дневное время, окна, ярко освещенные витрины, автомобильные фары при наружном размещении).

7.3.3. Технические требования к видеокамерам СОТ, применяемым для контроля БУС

7.3.3.1. Технические требования к видеокамерам, устанавливаемым внутри БУС

В связи с ограничением, налагаемым на габаритные размеры видеокамер устанавливаемых внутри БУС, для целевых задач, рассмотренных в п.7.3.2.1, используются, как правило, миниатюрные видеокамеры.

Для размещения внутри БУС рекомендуется применять цветные аналоговые или сетевые (IP) видеокамеры.

При выборе портретной видеокамеры рекомендуется придерживаться следующих требований:

- разрешение – высокое (HD): не ниже 500 ТВЛ при глубине модуляции не ниже 10% для аналоговой камеры, либо не менее 1,3 Мп (720p) для сетевой видеокамеры;

- управление диафрагмой – автоматическое;

- соотношение сигнал/шум с выключенной автоматической регулировкой уровня – не менее 48 дБ;

- минимальная освещенность на объективе камеры, без включения режима накопления заряда – не более 0,005 лк;

- наличие функции "день-ночь";

- наличие функции трехмерного цифрового шумоподавления (3DNR);

- наличие функции цифрового расширения динамического диапазона (D-WDR);

- наличие функции компенсации и подавления засветки (HSBLC);

- наличие функции назначения зон конфиденциальности сложной конфигурации.

При монтаже и настройке портретной видеокамеры БУС рекомендуется придерживаться следующих требований:

- верхняя граница сцены портретной видеокамеры по передней границе зоны самообслуживания БУС должна находиться не ниже 230 см от уровня пола;

- нижняя граница сцены портретной видеокамеры в передней границе зоны самообслуживания БУС должна находиться не выше 120 см от уровня пола;

- ширина поля зрения портретной видеокамеры в передней границе зоны самообслуживания БУС не должна превышать 200 см при использовании анало-

говой видеокамеры, либо 370 см при использовании сетевой видеокамеры с разрешением 1,3 Мп (или 720р);

- отклонение оптической оси объектива портретной видеокамеры от горизонтальной визирной линии по возможности не должно превышать 15 градусов;

- в сцену портретной видеокамеры не должна попадать клавиатура БУС для набора ПИН-кода.

При выборе презентерной (валидаторной) видеокамеры рекомендуется придерживаться выполнения следующих требований:

- разрешение – не ниже 400 ТВЛ при глубине модуляции не ниже 10% для аналоговой камеры, либо не менее 800×600 для сетевой видеокамеры;

- соотношение сигнал/шум с выключенной автоматической регулировкой уровня – не менее 48 дБ;

- минимальная освещенность на объективе камеры без включения режима накопления заряда – не более 0,01 лк;

- наличие функции "день-ночь".

При монтаже и настройке портретной, презентерной и валидаторной видеокамер рекомендуется придерживаться следующих требований:

- в сцену портретной видеокамеры не должна попадать клавиатура для набора ПИН-кода и номер ИЭК при ее установке или изъятии из БУС;

- сцены презентерной и валидаторной видеокамер должны занимать максимально большую площадь кадра.

7.3.3.2. Технические требования к видеокамерам, устанавливаемым в зоне размещения БУС

В качестве обзорных видеокамер, устанавливаемых в зоне размещения БУС (в помещении или на улице) рекомендуется применять, по возможности, купольные стационарные цветные аналоговые или сетевые (IP) видеокамеры, выполненные в антивандальном исполнении (для установки в помещении – не ниже IK08, для установки на улице – IK10, см. приложение Б), соответствующие следующим техническим параметрам:

- разрешение – высокое (HD): не ниже 600 ТВЛ при глубине модуляции не ниже 10% (для аналоговых видеокамер), либо не менее 1,3 Мп (720p) для сетевых видеокамер;
- управление диафрагмой – автоматическое;
- объектив вариофокальный;
- соотношение сигнал/шум – не менее 48 дБ;
- минимальная освещенность на объективе камеры без включения режима накопления заряда – не более 0,01 лк;
- наличие функции назначения "зон конфиденциальности" сложной конфигурации;
- наличие функции "день-ночь" со смещаемым инфракрасным фильтром;
- наличие функции цифрового расширения динамического диапазона (D-WDR).

При размещении видеокамер в местах высокой (п.3.4), повышенной (п.3.3) или средней (п.3.2) степени риска предпочтение рекомендуется отдавать моделям, имеющим антивандальное исполнение (IK10, см.

приложение Б) и встроенную инфракрасную (ИК) подсветку. Возможно также применение видеокамер, использующих ИК-технологию EXIR для видеонаблюдения в условиях плохой освещенности.

При невозможности исключения из сцены видеокамеры длительных или временных источников яркого света рекомендуется наличие функции компенсации и подавления засветки (HSBLC).

Видеокамеры уличного размещения должны иметь климатическое исполнение, соответствующее условиям У1 по ГОСТ 15150-69.

При проектировании, монтаже и настройке видеокамер СОТ рекомендуется придерживаться следующих требований:

- места размещения обзорных видеокамер рекомендуется выбирать таким образом, чтобы, по возможности, исключить или минимизировать постоянные (возникающие в результате ограничения поля зрения видеокамеры статичными преградами) или временные (возникающие, например, в результате загораживания одного человека другим) "мертвые зоны" в основных зонах контроля (зоне самообслуживания или сервисной зоне);

- обзорные видеокамеры следует размещать таким образом, чтобы избегать попадания в сцену камеры областей ввода ПИН-кода охраняемых БУС. В случае невозможности выполнения этого условия необходимо применять специальные меры для исключения компрометации ПИН-кода;

- при размещении одиночных БУС всех групп в местах высокой (п.3.4) или повышенной (п.3.3) сте-

пени риска рекомендуется устанавливать не менее двух обзорных видеокамер с целевой задачей различения (идентификации личности). Сцены видеокамер должны охватывать, как сервисную зону, так и зону самообслуживания БУС;

- при групповом размещении нескольких БУС в выделенном помещении в местах повышенной (п.3.3) степени риска (круглосуточные электронные офисы банковского самообслуживания клиентов, "зоны 24"), в помещении рекомендуется устанавливать не менее трех обзорных видеокамер. При этом, как минимум, одна видеокамера должна быть установлена так, чтобы в сцене этой видеокамеры находилась входная дверь. Данная видеокамера должна выполнять целевую задачу различения (фиксации лиц людей, входящих в помещение). При этом, объектив этой видеокамеры рекомендуется выбирать (настраивать) таким образом, чтобы при использовании аналоговой камеры ширина поля зрения на линии дверного проема не превышала 290 см, при использовании сетевой камеры с разрешением 1,3 Мп (720р) – 530 см, с разрешением 2 Мп – 670 см, с разрешением 1080р – 800 см;

- при размещении одиночных БУС в местах средней степени риска (п.3.2), в зависимости от категории материальной значимости БУС (п.2.3) рекомендуется устанавливать одну или несколько обзорных видеокамер с целевой задачей различения, в сцену которых должны входить сервисная зона. При групповом размещении нескольких БУС общее количество обзорных видеокамер рекомендуется выбирать, исходя из условия полного обзора сервисных зон БУС.

При организации охраны нескольких БУС, относящихся к группам СП, СВ и СУ, количество видеокамер, устанавливаемых в сервисном помещении, рекомендуется выбирать, исходя из условия достаточного обзора сервисных зон всех охраняемых БУС.

7.3.4. Особенности условий работы видеосерверов (видеорегистраторов) СОТ, применяемых для контроля БУС

7.3.4.1. Основные виды видеосерверов (видеорегистраторов), применяемых для контроля БУС

Видеосерверы (видеорегистраторы), применяемые в СОТ для контроля БУС, в зависимости от условий размещения и конструкции БУС, подразделяются на:

- совмещенные, реализованные непосредственно на управляющем компьютере БУС путем установки в него дополнительных специальных аппаратных и программных средств, предназначенных для организации видеонаблюдения;

- выделенные, представляющие собой отдельные, независимо работающие устройства, размещаемые внутри БУС или в специальных модулях, объединенных с БУС в единую конструкцию;

- вынесенные, представляющие собой отдельные, независимо работающие устройства, размещаемые вне БУС.

Совмещенные видеосерверы реализуются, как правило, установкой в управляющий компьютер БУС платы видеозахвата (если в БУС установлены аналоговые видеокамеры), увеличением объема накопителя для хранения видеоархива, а также установкой специализированного программного обеспечения. Для передачи дан-

ных совмещенный видеосервер может использовать тот же канал связи, что и управляющий компьютер БУС, в том числе, шифрованный, например, виртуальную частную сеть (VPN).

Необходимо отметить, что применение совмещенных видеосерверов имеет недостатки:

- существует вероятность взаимного влияния программных сбоев управляющего программного обеспечения БУС и специализированного программного обеспечения видеонаблюдения и их конкуренции в борьбе за вычислительные ресурсы;

- при проведении технического обслуживания и ремонта работники кредитной организации – владельца БУС (либо подрядных организаций, действующих в ее интересах) одновременно получают доступ как к программно-аппаратным средствам управления БУС, так и к программно-аппаратным средствам видеонаблюдения, что может быть крайне нежелательным;

- при взломе, похищении или уничтожении БУС видеоархив будет, скорее всего, потерян или уничтожен.

Выделенный видеосервер (видеорегистратор), представляющий собой отдельное независимое устройство, может вести необходимый информационный обмен с управляющим компьютером БУС через информационные стыки (USB, RS232, Ethernet). Размещение выделенного сервера внутри конструкций БУС накладывает ограничения на его предельные размеры и энергопотребление. Для передачи данных выделенный видеосервер может использовать либо тот же канал связи, что

и управляющий компьютер БУС, в том числе с шифрованием, либо отдельный канал связи.

Применение выделенных видеосерверов (видеорегистраторов) позволяет решить проблемы, связанные с разделением доступа к управляющему компьютеру (программному обеспечению) БУС и доступа к системе безопасности БУС. Выделенный видеосервер может размещаться в отдельном конструктивном элементе, доступ к которому ограничен с помощью инженерных и технических средств. Кроме того, при использовании выделенных видеосерверов (видеорегистраторов) существенно снижается вероятность взаимного влияния сбоев управляющего программного обеспечения БУС и СОТ. Вместе с тем, как и в случае совмещенных видеосерверов, при взломе, похищении или уничтожении БУС видеоархив СОТ может быть потерян или уничтожен.

Вынесенный видеосервер (видеорегистратор) также, как и выделенный, является отдельным, независимым устройством, осуществляющим необходимый информационный обмен с управляющим компьютером БУС через информационные стыки (USB, RS232, Ethernet). Вынесенные видеосерверы, как правило, не имеют жестких ограничений по габаритам и энергопотреблению, поскольку условия их размещения существенно проще. Особенно целесообразно применение вынесенных видеосерверов (видеорегистраторов) при групповом размещении БУС (например, в электронных офисах самообслуживания клиентов), когда к одному вынесенному видеосерверу могут быть подключены несколько БУС. Кроме того, при разме-

щении БУС на территории кредитной организации – владельца БУС, функции вынесенного видеосервера (видеорегистратора) может взять на себя видеосервер СОТ, функционирующий в составе интегрированной системы безопасности кредитной организации (п.3.6 Р 78.36.018-2011 МВД России [16]).

В отличие от случая применения совмещенного или выделенного видеосервера (видеорегистратора), разместить вынесенный видеосервер можно в труднодоступной для нарушителей, технически укрепленной зоне, и поэтому криминальные посягательства на БУС не смогут оказать негативного влияния на хранящийся на таком видеосервере видеоархив.

7.3.4.2. Особенности применения видеосерверов (видеорегистраторов) для контроля БУС

В случае криминального посягательства на БУС, объем работы представителей службы безопасности кредитной организации или специальных служб по просмотру видеоархива может быть весьма значительным. Особенно это касается случаев, когда нет информации о точном времени событий. В этом случае важной становится возможность привязать фрагмент видеозаписи к дополнительной информации. В качестве такой информации наиболее эффективно использование данных о срабатывании сигнализации, а также информации о номере ИЭК в виде, разрешенном для использования (с маскированием части символов).

Служба безопасности кредитной организации, имеющей разветвленную сеть БУС, при расследованиях, проводимых по претензиям клиентов, тратит существенные ресурсы на объезд мест размещения

видеосерверов (видеорегистраторов) СОТ БУС и копирование видеозаписей. В случаях, когда кредитная организация имеет разветвленную сеть БУС в отдаленных районах, ситуация еще более осложняется.

В повседневной деятельности кредитной организации – владельца БУС, а также при проведении оперативных мероприятий, может возникнуть необходимость либо изъятия существующего накопителя целиком и замены его новым, либо копирования необходимого фрагмента архива видеозаписей на переносной накопитель видеоинформации. Однако, в первом случае возникают проблемы, связанные, во первых, с возникающей "фрагментацией" видеозаписей (когда видеозаписи, находящиеся на уже изъятом накопителе, требуются для проведения другого расследования), а, во-вторых, сложностью организационно-технических процедур. Поэтому, изъятие накопителя следует рассматривать как исключительную меру, когда копирование хранящейся на накопителе информации по каким-либо причинам не может решить задачу.

Необходимо обратить внимание, что накопители видеосерверов (видеорегистраторов) БУС функционируют круглосуточно и непрерывно, обеспечивая кольцевую видеозапись всех подключенных видеокамер. При возникновении аппаратного сбоя или аварии накопителя, все или часть видеозаписей могут стать недоступными для использования.

7.3.5. Технические требования к видеосерверам (видеорегистраторам) СОТ, применяемым для контроля БУС

При выборе видеосервера (видеорегистратора) СОТ для контроля БУС, рекомендуется руководствоваться следующими требованиями:

- количество каналов оцифровки аналогового видеосигнала – не менее четырех (при использовании в БУС аналоговых видеокамер);

- размер кадра при оцифровке аналогового сигнала – не менее 704×576;

- разрядность аналого-цифрового преобразования – не менее 9 бит;

- размер кадра при использовании портретной сетевой видеокамеры – не менее 1280×720;

- размер кадра при использовании депозитарной (валидаторной) сетевой видеокамеры – не менее 800×600;

- скорость обновления кадров в видеозаписи – не менее 12 кадров в секунду для каждой камеры. Допустима скорость обновления кадров в видеозаписи – не менее 6 кадров в секунду, при условии увеличения скорости обновления кадров до 25 кадров в секунду в случае срабатывания детектора движения;

- длительность хранения видеозаписей в кольцевом хранилище для всех камер – не менее 60 суток;

- количество слаботочных входов для подключения внешних извещателей – не менее 4;

- количество релейных выходов – не менее 1;

- наличие функции настраиваемой длительности "предтревожной записи" для всех применяемых режимов записи;

- наличие функции назначения "зон конфиденциальности" сложной формы для любого количества доступных записываемых видеосигналов;

- наличие функции назначения временных зон реакции на обнаруженные события и извещения (например, включение или отключение реагирования в ночные часы);

- наличие функции архивации и экспортирования видеозаписей и отдельных кадров на внешние носители по запросу;

- наличие системы разделения прав пользователей.

Видеосервер (видеорегистратор), применяемый в СОТ для контроля БУС, должен иметь встроенную систему самодиагностики с функцией автоматической отправки извещений на пульт мониторинга кредитной организации – владельца БУС и на ПЦО. Рекомендуется наличие возможностей обнаружения:

- неисправностей накопителя для хранения видеозаписей;

- отключения или саботажа (заклеивание, закрашивание, отворачивание, уничтожение) видеокамер.

В случае применения в БУС специальных технических средств безопасности, позволяющих вести информационный обмен и передавать данные о своем состоянии (например, антискимминговые устройства, охранно-дымовые системы), рекомендуется также наличие функции обнаружения сбоев в работе этих технических средств или необходимости проведения технического обслуживания.

Для портретной и обзорных видеокамер рекомендуется применять режим запуска записи по обнаружению движения в сцене видеокамеры.

В случае подключения к видеосерверу (видеорегистратору) извещателей и (или) ППКОП, установ-

ленных в БУС, рекомендуется наличие функции видеозаписи по извещениям, поступившим от подключенных к слаботочным входам извещателей, и (или) от подключенного по информационному стыку ППКОП. Кроме того, в этом случае должна быть обеспечена возможность поиска фрагментов хронологически связанных видеозаписей по заданным извещениям.

В случае применения выделенного или вынесенного видеосервера для получения данных от управляющего компьютера БУС рекомендуется использовать доступные информационные стыки. При этом целесообразно предусмотреть функцию синхронизации системного времени видеосервера (видеорегистратора) с системным временем управляющего компьютера БУС.

Учитывая специфику задач, решаемых видеосервером (видеорегистратором), важным является наличие функций получения от управляющего компьютера БУС номера ИЭК в маскированном виде, дальнейшего хронологического увязывания полученных данных с видеозаписями всех подключенных видеокамер и автоматизированный поиск в видеозаписях фрагментов, с которыми хронологически связан заданный номер.

Для валидаторной и презенторной видеокамер допускается вместо записи по обнаружению движения применение режима записи по команде, например, при получении от управляющего компьютера БУС видеосервером номера ИЭК в маскированном виде.

Рекомендуется наличие функции наложения на изображение в видеозаписях, в заданных областях, следующей текстовой информации: текущие дата, время, номер БУС, идентификационная информация видеока-

меры (например, портретная, презентерная, валидаторная, обзорная), а также полученный от управляющего компьютера БУС номер ИЭК (во время сеанса самообслуживания) или информация об обнаруженном извещении (во время записи по срабатыванию извещателя и/или извещению от подключенного ППКОП).

При использовании видеосерверов (видеорегистраторов), соединенных с ПЦН (центрами мониторинга кредитных организаций – владельцев БУС) узкополосными и неустойчивыми каналами связи (например, каналами сотовой связи), рекомендуется наличие функции автоматической передачи сообщений об обнаруженных извещениях, полученных от подключенных извещателей и/или ППКОП и связанных фрагментов видеозаписи заданной камеры с определенной длительностью "предтревожной записи" или отдельных кадров в заданном количестве и определенной периодичностью для подтверждения актуальности тревоги.

При применении видеосерверов (видеорегистраторов) в составе СОТ для контроля БУС в разветвленной сети из большого количества БУС, рекомендуется наличие функции передачи заданных видеозаписей и отдельных кадров по запросам с АРМ оператора. При этом должна обеспечиваться возможность ограничения разрешенной пропускной способности канала связи с целью обеспечения требуемой полосы пропускания для выполнения БУС основных функций в случае, если управляющий компьютер БУС и видеосервер используют общий канал связи. Кроме того, должны обеспечиваться функции создания очередей передачи и восстановления процедуры передачи видеозаписей в случае разрыва соединения.

7.3.6. Особенности условий работы АРМ операторов СОТ, при осуществлении контроля БУС

При контроле разветвленной сети БУС возникает проблема одновременного представления информации от всех контролируемых устройств. Вместе с тем, возможности оператора СОТ и средств отображения ограничены. Таким образом, с увеличением количества контролируемых одним АРМ видеосерверов, растет вероятность потери сигнала "тревоги" или информации от системы диагностики об обнаруженном сбое.

Поскольку АРМ является средством контроля видеосерверов (видеорегистраторов) сети БУС, то сбой АРМ выводит из-под контроля все подключенные к нему видеосерверы (видеорегистраторы). При сбое или аварии АРМ локальные видеозаписи видеосерверов (видеорегистраторов) не страдают, однако сообщения об обнаруженных тревогах поступать не смогут.

При работе оператора СОТ, используемой для контроля БУС, наиболее часто возникают задачи двух типов: задача мониторинга событий, связанных с СОТ, в режиме реального времени, обеспечения своевременного реагирования на них и задача работы по запросам (поиск требуемых фрагментов видеозаписей) при проведении оперативных мероприятий, расследований по претензиям и специальным запросам.

7.3.7. Технические требования к автоматизированным рабочим местам операторов СОТ, осуществляющих контроль БУС

Для АРМ оператора СОТ, осуществляющего телевизионный контроль БУС, рекомендуется наличие следующих функций:

- просмотр списка БУС, к которым имеет доступ данный оператор, с возможностью поиска и фильтрации;

- создание и редактирование групп БУС;

- отображение извещений, полученных от видеосерверов (видеорегистраторов) БУС, в том числе, данных самодиагностики видеосерверов, состояние функционирования специального программного обеспечения и каналов связи;

- отображение кадров или фрагментов видеозаписи, полученных от видеосерверов (видеорегистраторов) БУС и предназначенных для ретроспективного просмотра при поступлении извещений о тревоге;

- поиск по видеозаписям с возможностью задавать различные критерии поиска (номер ИЭК, номер БУС, номер видеокамеры, дата и время записи, тип события, при котором была произведена запись и др.);

- одновременная загрузка с любого количества подключенных к данному АРМ видеосерверов (видеорегистраторов) заданных фрагментов видеозаписей с возможностью продолжения прерванной загрузки и создание расписания загрузок видеозаписей.

Аутентификация операторов и администраторов СОТ должна производиться посредством ввода логина (идентификационного кода оператора или администратора) и пароля, с последующим назначением оператору или администратору СОТ соответствующих прав доступа.

7.3.8. Перспективы развития СОТ для контроля БУС

Перспективы развития СОТ для контроля БУС определяются, во-первых, степенью полезности нового

оборудования для решения задач обеспечения безопасности БУС, во-вторых, соотношением стоимость/эффективность его внедрения.

Так, например, при условии эффективно установленных обзорных видеокамер перспективным может стать применение на видеосерверах функций видеоанализа. В этом случае применение специализированных видеоаналитических детекторов длительного нахождения в зоне размещения БУС может помочь в автоматическом режиме определять ситуации, в которых есть подозрение, что совершено криминальное посягательство на БУС.

Однако при использовании видеоаналитических функций следует помнить, что для их корректной работы необходимы условия достаточной освещенности с отсутствием контрастных длинных теней, а также требуется повышение кадровой скорости, что, в свою очередь, приводит к необходимости применения накопителей большей емкости. Учитывая эти обстоятельства, рекомендуется использовать функции видеоаналитики в первую очередь на вынесенных видеосерверах для обеспечения контроля групп БУС, размещенных в выделенных помещениях.

Перспективным является также направление взаимной интеграции всех технических средств охраны, устанавливаемых в БУС, не только с целью обеспечения мониторинга их работоспособности, но и в интересах получения целостной, комплексной картины события, на основе анализа данных от различных источников, а также создания специализированных сценариев оповещения или реагирования.

7.4. Охранно-поисковые средства

7.4.1. Классификация охранно-поисковых средств

Технические средства, предназначенные для позиционирования и поиска БУС, относящихся к группам ОП, ОВ и ОУ (в случае их хищения), можно классифицировать по типу используемых данных и ресурсов следующим образом:

- технические средства позиционирования и поиска БУС, использующие данные и ресурсы действующих спутниковых навигационных систем GPS (США) и ГЛОНАСС (Россия), а также в перспективе – развертываемых систем GALILEO (Европейский союз) и COMPASS (Китай);

- технические средства позиционирования и поиска БУС, использующие данные и ресурсы наземной сети операторов сотовой связи, предоставляющих соответствующую услугу (LBS)[27];

- комбинированные технические средства позиционирования и поиска БУС, использующие данные и ресурсы, как спутниковых навигационных систем, так и наземных сетей операторов сотовой связи;

- технические средства позиционирования и поиска БУС, использующие данные и ресурсы специально созданных (развернутых) на территории отдельного поселения (в отдельном регионе) радиоканальных систем определения координат контролируемых объектов.

---

[27] LBS (Location-based service) – услуга, предоставляемая операторами сотовой связи, для определение местоположения объекта (абонента) по базовым станциям этих операторов.

7.4.2. Охранно-поисковые средства, использующие данные и ресурсы спутниковых навигационных систем

Одним из наиболее распространенных способов определения текущего местоположения контролируемых объектов, в данном случае – отдельно установленных БУС (групп ОП, ОВ или ОУ), особенно находящихся в зонах высокой (п.3.4) или повышенной (п.3.3) степени риска быть подвергнутыми несанкционированному перемещению (хищению), является использование охранно-поисковых средств на базе так называемых GPS-трекеров – электронных устройств объединяющих в себе GPS/ГЛОНАСС-ресивер, предназначенный для приёма, передачи и обработки сигналов (данных) навигационных спутниковых систем, и GSM/GPRS[28]/EDGE[29] модуль, передающий данные с текущими координатами БУС, направлением движения БУС (в случае его несанкционированного перемещения) и временем на удалённый компьютер для просмотра информации о положении объекта и слежения за его перемещениям оператором подразделе-

---

[28] GPRS (General Packet Radio Service) – "пакетная радиосвязь общего пользования" – надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю сети сотовой связи производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе Интернет.

[29] EDGE (EGPRS) (Enhanced Data rates for GSM Evolution) – цифровая технология беспроводной передачи данных для мобильной связи, которая функционирует как надстройка над 2G и 2.5G (GPRS)-сетями. Эта технология работает в TDMA и GSM сетях.

ния безопасности кредитной организации (платежного агента) – владельца БУС, мониторинговой компании или дежурным ПЦО.

Информация о текущих координатах БУС, с установленным в нем GPS-трекере, могут передаваться посредством SMS сообщений, путём передачи данных в GPRS/EDGE протоколе или с использованием специального радиоканала.

Используемые в охранно-поисковых средствах GPS-трекеры подразделяются на три основные группы, исходя из способов передачи данных:

- GPS/ГЛОНАСС/GSM трекеры, которые передают информацию посредством SMS сообщений, используя GSM сети оператора сотовой связи. Они действуют в зоне покрытия GSM сети оператора сотовой связи, с которым заключен договор, или в роуминге;

- GPS/ГЛОНАСС/GSM/GPRS(EDGE) трекеры, которые передают информацию, используя GSM сети и GPRS технологию передачи данных. При отсутствии покрытия GSM сети, данные могут накапливаться во внутренней памяти трекера и затем пересылаться пакетом при появлении устойчивого приёма GSM сигнала;

- GPS/ГЛОНАСС/RF трекеры, которые передают информацию, используя специальный радиоканал, работающий в определённом диапазоне частот, не связанный с GSM сетями операторов сотовой связи. Действуют в любом месте, независимо от наличия GSM сети, но имеют локальное покрытие. Радиус удаления RF трекера от приёмника составляет, как правило, не более нескольких десятков километров. Ис-

пользуются в местах с нестабильным приёмом сотовой связи или в районах с её полным отсутствием.

Одним из недостатков работы охранно-поисковых средств на основе GPS/ГЛОНАСС технологии является большое время технической готовности навигационного приемника, необходимое для поиска и связи со спутниками и определения позиции после его включения ("холодный старт"). Для решения этой проблемы необходимо использовать охранно-поисковые средства, поддерживающие технологию A-GPS/ГЛОНАСС.

Для алгоритмов A-GPS/ГЛОНАСС необходим канал связи с удаленным сервером, который предоставляет вспомогательную информацию GPS-приемнику. Таким каналом чаще всего является наземная сеть базовых станций операторов сотовой связи. Для передачи информации, охранно-поисковое средство должно находиться в зоне действия базовой станции оператора сотовой связи и иметь доступ в Интернет.

Вспомогательная информация от ближайших базовых станций операторов сотовой связи позволяет определить приблизительное местоположение охранно-поискового средства. Точность зависит от плотности установки базовых станций. Наибольшая плотность станций – в центрах городов. Точность в таких местах составляет от 20 до 500 метров. При уменьшении плотности и при ухудшении условий приема точность снижается. На окраинах городов – до 1500 – 2000 метров.

Охранно-поисковые средства, использующие технологию A-GPS/ГЛОНАСС, обладают следующими преимуществами перед устройствами, использующими обычную технологию GPS/ГЛОНАСС:

- быстрое получение координат охраняемого объекта сразу после включения;

- повышение возможности приема слабых сигналов в так называемых "мёртвых зонах" (тоннелях, низинах, впадинах, на узких городских улицах, в помещениях, в лесу с плотным лиственным покровом).

Основным недостатком охранно-поисковых средств, использующих технологию A-GPS/ГЛОНАСС, является невозможность функционирования вне зоны покрытия сети операторов сотовой связи.

Кроме этого, общим недостатком охранно-поисковых систем на базе GPS/ГЛОНАСС технологий, ограничивающим возможности их применения в охранных целях, является слабая устойчивость к помехам от наземных источников, которые препятствуют нормальному приему радиосигналов от спутников и (или) базовых станций операторов сотовой связи. Такие помехи могут быть как случайными (от работающего вблизи оборудования, излучающего помехи на рабочей частоте охранно-поисковых средств), так и преднамеренно создаваемыми нарушителями при помощи подавителей радиосигналов (GPS/GSM-глушилок), а также других криминальных способов саботажа работы охранно-поисковых средств, описанных в п.7.4.5.

7.4.3. Охранно-поисковые средства, использующие данные и ресурсы наземной сети операторов сотовой связи

Средства позиционирования и поиска похищенных БУС, использующие данные и ресурсы наземной сети операторов сотовой связи (услугу LBS) не определяют фактическое местоположение контролируемого

объекта, а осуществляют условную "привязку" его местоположения к ориентирам, нанесённым на электронную карту LBS-системы оператором сотовой сети или поставщиком услуги.

В большинстве систем, предлагаемых сотовыми операторами в России, обязательным условием является получение от "искомого" объекта разрешения на "поиск", например, в соответствии с договором, заключаемым собственником БУС или охранной организацией с оператором сотовой связи.

Определение местоположения может осуществляться либо по запросу, либо по заданному пользователем расписанию.

В ответ на запрос местоположения обычно включается 3 координаты: пересечение улиц (координаты "x" и "y"), а также поясное время местоположения (координата "t"). В некоторых системах местоположение может быть отображено в виде окружности на карте, в пределах которой, по мнению системы, находится "искомый" или фрагмента карты, отправляемого "ищущему" по MMS. В городах федерального значения в качестве ориентира используются также станции метрополитена.

Точность определения координат по технологии LBS несколько ниже, чем по GPS/ГЛОНАСС (точность по технологии GPS/ГЛОНАСС составляет порядка 10 метров, по технологии LBS – 200-500 метров), но LBS является незаменимым средством поиска объекта в тех случаях, когда нет связи со спутниками GPS и ГЛОНАСС (например, при похищении БУС могут быть использованы подавители GPS/ГЛОНАСС

сигналов или автомобиль с похищенным БУС может находиться на подземной стоянке, в бетонном гараже, тоннеле и т.п.). Время определения координат при помощи GPS/ГЛОНАСС составляет примерно 5-15 минут, при помощи технологии LBS – несколько секунд.

Такая технология позиционирования и поиска БУС (в случае его хищение) используется, например, в системе активной защиты банкоматов "Алабай" (ЗАО "ПК Атлант").

7.4.4. Комбинированные охранно-поисковые средства

Для решения задачи позиционирования и поиска похищенных БУС могут быть также применены комбинированные охранно-поисковые средства, сочетающие в себе возможности устройств, использующих данные и ресурсы спутниковых навигационных систем GPS/ГЛОНАС (см. п.7.4.2), и устройств, использующих данные и ресурсы наземной сети сотовой связи по технологии LBS (см. п.7.4.3). В результате такой комбинации местоположение охраняемого БУС определяется либо по технологии GPS/ГЛОНАСС, либо (если нет связи со спутниками) по базовым станция операторов сотовой связи, а также (при наличии соответствующего модуля) посредством данных о расположении точек доступа Wi-Fi.

В случае определения положения БУС по базовым станциям оператора сотовой связи (по технологии LBS) точность определения координат контролируемого объекта, например, автомобиля с похищенным БУС резко падает, и его положение может хаотично "скакать" по карте на сотни метров, в зависимости от

плотности базовых станций оператора сотовой связи, но, тем не менее, в целом это дает подразделениям полиции (ГЗ СПВО, ППС, ДПС) необходимые ориентиры для реализации плана "Перехват" и других оперативно-розыскных мероприятий.

7.4.5. Методы защиты охранных-поисковых средств от саботажа

7.4.5.1. Защита от умышленного нарушения приема/передачи радиосигналов

Самым распространенным среди нарушителей методом деактивации охранно-поисковых средств, рассмотренных в пп.7.4.2–7.4.4, является умышленное нарушение приема/передачи радиосигналов, необходимых для определения текущего местоположения охраняемого БУС (связь со спутниками), передачи на ПЦО тревожных извещений и навигационной информации по GSM/3G каналам сотовой связи.

Для этих целей нарушители используют подавители радиосигналов. Проблема заключается в том, что такие устройства находятся в России в свободной продаже. Различаются они в основном своей функциональностью (в зависимости от модели могут подавлять сигналы GSM, CDMA, 3G, GPS, ГЛОННАС, Wi-Fi и др.), а также мощностью (от 3 до 30 Вт) и радиусом действия (от 10 до 150 м).

Для защиты охранно-поисковых средств от этого вида саботажа необходимо наличие в таких средствах функции контроля канала связи (Jamping Detection), которая в автоматическом режиме осуществляет проверку связи между специально организованным сер-

вером и охранно-поисковым средством. С установленной периодичностью охранно-поисковое средство, установленное в контролируемый БУС, должно связываться с сервером, например, пересылать данные по протоколу прикладного уровня HTTP (Hyper Text Transfer Protocol), основой которого является технология "клиент-сервер". Иными словами предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом. Если в течение N последних минут охранно-поисковое средство не свяжется с сервером, то это расценивается как вероятное подавление радиосигналов в зоне размещения контролируемого БУС и сервер высылает на ПЦО тревожное извещение.

7.4.5.2. Защита от умышленного повреждения GSM и GPS антенн

В криминальной практике используются в основном два метода поиска и повреждения GSM (3G) и GPS (ГЛОНАСС) антенн технических средств охраны.

Первым из них является банальный метод поиска и ликвидации выносных антенн GSM и GPS/ГЛОНАСС модулей охранно-поисковых средств, который чаще всего используют неквалифицированные или неподготовленные нарушители (см. п.4.2). Заключается он в физическом удалении антенны или повреждении ее соединительного кабеля. В первую очередь это касается антенн, устанавливаемых снаружи БУС (при помощи встроенного магнита) или под

пластиковыми деталями БУС (в верхнем кабинете банкомата).

Для защиты охранно-поисковых средств от этого вида саботажа обычно применяют так называемые "антенны-ловушки". Штатная GSM антенна охранно-поискового средств или ППКОП (УОО СПИ), работающего по GSM каналу связи, устанавливается скрытым образом под пластиковые детали БУС (внутри верхнего кабинета банкомата), а снаружи БУС устанавливается "антенна-ловушка" – внешне ничем не отличающаяся от обычной GSM антенны, но имеющая встроенный датчик отрыва. Соединительный кабель такой "антенны-ловушки" представляет собой контролируемый "на обрыв" шлейф сигнализации, подключенный к ППКОП (УОО СПИ).

Вторым (более изощренным) методом саботажа работы охранно-поисковых средств является метод поиска и устранения GSM и GPS антенн, в том числе скрыто установленных в охраняемом БУС. Для этого злоумышленники, как правило, используют специальные технические средства, так называемые детекторы или детекторы-частотомеры электромагнитного поля. Такой метод применяется, как правило, специально подготовленными и квалифицированными нарушителями.

Для защиты охранно-поисковых средств от такого вида саботажа рекомендуется скрытая установка в охраняемом БУС миниатюрного автономного поискового маяка, предназначенного для определения точных координат объекта, местоположение которого необходимо контролировать.

В дежурном режиме такой маяк большую часть времени находится в "спящем состоянии" и выходит на связь с сервером только по заданному расписанию. При выходе на связь маяк передает на сервер информацию о своем местоположении и состоянии. Если не включен режим поиска, устройство опять "засыпает". В режиме поиска, который может включить сам пользователь, маяк с заданной периодичностью, будет определять свои координаты и передавать их на сервер. Поскольку такой маяк значительную часть времени находится в "спящем" состоянии, его трудно обнаружить индикаторами (детекторами) радиосигналов.

Современные модели поисковых маяков, например, StarLine 17 (ООО "НПО "СтарЛайн") оснащаются встроенным датчиком движения, с помощью которого маяк может определять начало движения или переворот охраняемого БУС и сообщать в подразделение безопасности кредитной организации (платежного агента) – собственника БУС, мониторинговую компанию или на ПЦО об этих событиях SMS-сообщением.

Кроме того, такой маяк при возникновении тревожной ситуации с помощью универсального дополнительного канала может дистанционно управлять внешними устройствами, например, включить автономный звуковой оповещатель, установленный внутри БУС.

7.4.5.3. Защита от подмены базовой станции (ретранслятора) оператора сотовой связи

Подмена базовой станции (ретранслятора) оператора сотовой связи, с которой связывается охранно-поисковое средство или ППКОП (УОО СПИ), уста-

новленные в БУС, является наиболее интеллектуальным и технически сложным из приведённых методом саботажа охранно-поисковых средств и используется, как правило, квалифицированными нарушителями, обладающими специальными знаниями в области информационной безопасности.

Данный метод саботажа охранно-поисковых средств, а также ППКОП (УОО СПИ) и оборудования СОТ, осуществляющих передачу информации на ПЦО, используя GSM-каналы связи, заключается в том, что специальное портативное оборудование злоумышленника выдает себя за базовую станцию или ретранслятор оператора мобильной связи, с которой "ничего не подозревающий" GSM-модем охранно-поискового средства ППКОП (УОО СПИ) или оборудования СОТ осуществляет обмен информацией.

В результате применения такого противозаконного оборудования при возникновении тревожной ситуации на БУС реальной передачи данных на ПЦО или в подразделение безопасности кредитной организации не происходит.

Методом защиты от такого вида саботажа охранно-поисковых средств является наличие в них функции контроля канала связи (см. п.7.4.3.1).

7.4.5.4. Перспективы развития охранно-поисковых средств

Известной проблемой передачи данных по GSM и GPRS каналам является их существенная задержка, особенно при перегрузке сетей сотовой связи. Для передачи экстренной информации, в том числе о взломе

или несанкционированном перемещении (хищении) БУС такая ситуация не допустима.

С целью повышения оперативности реагирования по сигналу тревоги, поступающему на ПЦО от охранно-поисковых средств, используемых для контроля отдельно установленных БУС (особенно банкоматов высокой категории материальной значимости), целесообразно применение охранно-поисковых средств, интегрированных в создаваемую в Российской Федерации Государственную систему экстренного реагирования при авариях "ЭРА-ГЛОНАСС

Модемы, совместимые с системой "ЭРА-ГЛОНАСС", передают данные мгновенно, поскольку таким вызовам выделяется максимальный приоритет оператором мобильной связи, даже в случае перегрузки сотовой сети. Если сеть перегружена – то активные вызовы других абонентов разрываются, чтобы модемы, функционирующие в составе системы "ЭРА-ГЛОНАСС" могли связаться со службой 112.

Общие технические требования к навигационно-коммуникационным устройствам системы "ЭРА-ГЛОНАСС" установлены в ГОСТ Р 54620-2011.

7.5. Средства активной защиты и оповещения

7.5.1. Основные аспекты применения средств активной защиты и оповещения

Согласно теории анализа уязвимости и категорирования охраняемых объектов, основным критерием эффективности функционирования систем охранной сигнализации и противокриминальной защиты является

вероятность пресечения противоправных действий нарушителя[30], которая зависит от:

- вероятности обнаружения нарушителя техническими средствами охраны (охранными извещателями, детекторами движения видеокамер СОТ);

- вероятности удержания нарушителя (создания препятствий на пути проникновения в охраняемую зону) средствами ИТУ и СКУД (при ее наличии);

- вероятности нейтрализации нарушителя (вероятности того, что нарушитель по психофизическим причинам не сможет реализовать свой преступный замысел и будет вынужден покинуть охраняемую зону).

Вероятность быстрой нейтрализации нарушителя при установлении критериев и показателей эффективности систем охраны объектов, особенно объектов высоких категорий значимости, к которым относятся значительная часть БУС (банкоматы категории М1, М2), имеет такое же существенное значение, что и показатели удержания (средствами ИТУ) и обнаружения (при помощи ТСОС и СОТ) нарушителя.

Традиционные системы охранной сигнализации, которые применяются в том числе и для защиты БУС от преступных посягательств, относятся к категории так называемых пассивных систем, назначение которых заключается в обнаружении факта (или попытки) вторжения в охраняемую зону (зону размеще-

---

[30] Незаконное проникновение в зону размещения БУС (зону самообслуживания, сервисную зону), взлом сейфа БУС, кража наличных денег из БУС, установка устройств для незаконного доступа к конфиденциальной информации, несанкционированное перемещение (хищение) БУС, вандализм.

ния БУС), обнаружении попытки взлома или хищения БУС и формировании тревожного извещения для передачи на ПЦО СПВО и (или) в подразделение безопасности кредитной организации.

Специфика функционирования активных систем охраны, в дополнение к вышеуказанным функциям, выполняемых пассивными системами, предполагает еще и активное противодействие, затрудняющее совершение противоправных действий в отношении БУС.

В пассивных системах охраны нейтрализация нарушителей выполняется за счет действий сотрудников полиции (ГЗ СПВО), осуществляющих оперативное реагирование на сообщения о срабатывании средств охранной или тревожной сигнализации, установленных в охраняемом БУС (или в зоне его размещения). В данном случае вероятность успешной нейтрализации и задержания нарушителей зависит от многих факторов (численного состава, специальной подготовки, технического оснащения и вооружения нарушителей и сотрудников полиции, дистанционных и временных параметров прибытия ГЗ СПВО по сигналу тревоги).

При создании комплексной системы охраны БУС необходимо иметь в виду, что значительная часть преступлений в отношении БУС совершается специально подготовленными, техническими оснащенными и вооруженными преступными группами. При этом злоумышленники постоянно совершенствуют способы взлома БУС. В массовом порядке регистрируются преступления, связанные с хищением отдельно установленных и зачастую не прикрепленных к полу (фундаменту) БУС. Такие преступления совершаются,

как правило, при помощи транспортных средств и занимают по времени считанные минуты. Как показывает статистика преступлений в этой области, нарушителей не останавливает даже наличие физической охраны.

В связи с этим, наряду с применением традиционных охранных технологий, становится актуальным применение средств активного воздействия на нарушителей, функционирующих в едином комплексе средств охранной (тревожной) сигнализации и противокриминальной защиты БУС.

Применение средств активного воздействия на нарушителей значительно повышает вероятность успешной нейтрализации и задержания нарушителей на месте совершения ими противоправных действий, препятствует попыткам совершения преступлений, обеспечивает сохранение материальных ценностей.

Рассматриваемые в контексте обеспечения комплексной централизованной охраны БУС технические средства активной защиты (ТСАЗ) можно классифицировать по целевым функциям следующим образом:

- оказания психологического воздействия на нарушителей и привлечения внимания к охраняемому БУС.
- оказания психофизического (дезориентирующего) воздействия на нарушителей и создания условий для обеспечения безопасности граждан, находящихся в зоне размещения БУС (в случае ограбления отделения кредитной или иной организации, в которой установлены БУС или ведется работа с денежными средствами).

7.5.2. Средства оказания психологического воздействия на нарушителя (охранные оповещатели)

Для психологического воздействия на нарушителя, а также оповещения о несанкционированном проникновении в зону размещения БУС и (или) попытке взлома (хищения) БУС рекомендуется применять световые, звуковые или комбинированные охранные оповещатели, соответствующие требованиям ГОСТ Р 54126-2010, выбираемые с учетом рекомендаций по пп.6.3 – 6.8 и конкретных условий эксплуатации по ГОСТ Р 54455-2011 (в закрытом отапливаемом помещении, в помещении с нерегулируемой температурой, под навесом, вне помещений).

Целесообразно, чтобы охранные оповещатели, используемые в зоне размещения БУС (особенно, устанавливаемые вне помещений), были выполнены в антивандальном исполнении (имели степень защиты от механических ударов не ниже IK08, см. приложение Б).

Охранные оповещатели рекомендуется (по возможности) устанавливать в местах недоступных (труднодоступных) для посторонних лиц, в защищенных местах или за специальными защитными конструкциями, пропускающими звуковые и световые сигналы оповещения.

Для функционирования в закрытом помещении или под навесом может быть использован, например, комбинированный оповещатель "Призма-202" (НПО "Сибирский арсенал"), а для функционирования вне помещений – комбинированный оповещатель "Гром-12К исп. 3" (ООО УК "Арсенал безопасности").

В верхнем кабинете банкомата или внутри корпуса платежного терминала группы ОП, ОВ или ОУ, независимо от наличия средств оповещения в зоне

размещения БУС, рекомендуется устанавливать отдельный звуковой оповещатель, например, "Маяк-12-3М1" (ООО "Электротехника и автоматика"), при условии обеспечения ему резервируемого электропитания.

7.5.3. Средства оказания психофизического (отпугивающего или дезориентирующего) воздействия на нарушителей

В качестве технических средств оказания психофизического (отпугивающего или дезориентирующего) воздействия на нарушителей в настоящих Рекомендациях рассматриваются специальные дымовые, газовые или парогенерирующие устройства, заполняющие охраняемое помещение (зону размещения БУС) густым непрозрачным паром (дымом), а также устройства, содержащие вещества слезоточивого или раздражающего действия.

7.5.3.1. В отдельных случаях, например, для охраны БУС группы ОВ, установленных в больших помещения общего доступа могут быть использованы распылительные устройства слезоточиво-раздражающего действия, которое заключается во временном выведении нарушителя из строя за счет раздражения слизистой оболочки глаз порошковой взвесью со специальными маркирующими добавками, выбрасываемой в пространство электромеханическим устройством при подаче на него управляющего сигнала при срабатывании ТСОС или КТС.

Устройства такого принципа действия используется, например, в системе активной защиты банкоматов "Алабай" (ЗАО "ПК Атлант"), в которую входит

комплект устройств звукового, дымового и слезоточивого воздействия на нарушителя.

Недостатком таких устройств, ограничивающим их применение для охраны БУС, является то, что подготовленный нарушитель, имеющий информацию о наличии такого устройства в системе охраны БУС, может, например, механически заблокировать выход дыма (газа) или защитить себя простыми известными способами, начиная от защитных строительных очков или очков для плавания, плотно прилегающих к лицу, и заканчивая противогазовым респиратором.

Кроме того при использовании средств активной защиты на основе пиропатронов, например, управляемых генераторов окрашенного дыма, есть опасность возникновения пожара, повреждения БУС или зоны его размещения, а также опасность нанесения вреда здоровью и имуществу клиентов и обслуживающего персонала в случае срабатывания системы из-за какого-либо внешнего фактора, случайного (неумышленного) воздействия на БУС или ошибки действий инкассаторов, например, при несвоевременном снятии БУС с охраны. Такие случайные срабатывания охранной сигнализации, согласно статистике кредитных организаций, происходят регулярно (примерно один случай из десяти).

7.5.3.2. Как показали испытания, наиболее эффективными и безопасными для организации централизованной охраны БУС являются технические средства активной защиты, принцип действия которых основан на генерации непрозрачного тумана и заполнении им охраняемого помещения (зоны размещения БУС), так называемые охранно-дымовые системы.

Такие системы должны соответствовать требованиям МЭК 62642-8:2011, а также требованиям электромагнитной совместимости по ГОСТ Р 50009-2000, ГОСТ Р 51317.3.2-2006, ГОСТ Р 51317.3.3-2008 и требованиям безопасности по ГОСТ IEC 60065-2011, иметь встроенный датчик вскрытия корпуса и необходимые степени его защиты: не ниже IP30 по ГОСТ 14254-96 и не ниже IK08 (см. приложение Б).

Для подтверждения безопасности генерируемого дыма (тумана) для людей и животных системы должны иметь соответствующее санитарно-эпидемиологическое заключение Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека.

Принцип действия данных средств активной защиты БУС заключается в следующем.

Получив управляющий сигнал от ТСОС, КТС или ППКОП (УОО СПИ), установленных в БУС или зоне его размещения (зоне самообслуживания, сервисной зоне), охранно-дымовая система начинает вырабатывать густой белый туман, за несколько секунд полностью заполняющий помещение (зону размещения БУС).

Задымляющий помещение эффект достигается за счет специальной жидкости[31], испаряемой при постоянно поддерживаемой в нагревательном блоке температуре, которая затем конденсируется в воздушном пространстве помещения, превращаясь в стойкий мелкодисперсный аэрозоль, создавая види-

[31] Обычно это гликоль или глицерин, смешанный с подготовленной водой.

мый эффект дыма, точнее тумана (что более верно по физико-химическому процессу).

Диаметр образуемых частиц такого дыма или тумана в среднем у разных производителей составляет от 0,2 до 3 мкм.

Чем меньше размер частиц, тем более "сухой" туман будет образовываться, который будет оседать медленнее и, следовательно, будет оказывать более длительное воздействие на нарушителя. Кроме того, при минимальном размере частиц появление осадков, загрязнений и нанесение какого-либо ущерба имуществу исключается, такой туман рассеивается практически бесследно.

Психофизическое (дезориентирующее) воздействие, оказываемое на нарушителя данными техническими средств активной защиты БУС заключается в следующем.

В распространившемся по помещению тумане нарушитель теряет возможность видеть что-либо на расстоянии примерно 20–30 см от глаз. При этом нарушитель (если он психически адекватен) понимает, что у него есть всего лишь несколько минут до приезда полиции (ГЗ СПВО). Вслепую же осуществлять какие-либо криминальные воздействия, например, вскрывать сейф банкомата затруднительно и требует больше времени, чем было запланировано. Как показывает статистика применения охранно-дымовых систем в различных странах, в таких неблагоприятных и неожиданных условиях нарушители предпочитают спешно покинуть место задуманного преступления и больше на него не возвращаться.

В качестве таких средств активной защиты БУС (кроме БУС группы ОУ) могут быть использованы, например, охранно-дымовые системы серии "Protect" производства компании "Protect" или охранно-дымовые системы "Sentinel" производства компании "Concept Smoke Screen".

Следует отметить, что эффективность системы активной защиты зоны размещения БУС туманом значительно повышается при включении в ее состав стробоскопа, яркий прерывистый свет которого, рассеиваясь в тумане, практически полностью лишает нарушителя возможности видеть что-либо, кроме ослепляющих вспышек света, неприятно бьющих в глаза. Для усиления психологического эффекта возможно применение данной системы совместно с мощным звуковым оповещателем, установленным в помещении.

Системы активной защиты туманом рекомендуется устанавливать скрытно (маскировать), например, за фальш-потолком, стеной, перегородкой, оставляя небольшое отверстие для выхода пара, которое также может быть замаскировано, например, под пожарный извещатель. При отсутствии такой возможности, систему рекомендуется устанавливать на потолке над БУС (группой БУС), заблокировав возможность несанкционированного приближения к системе, например, с помощью ИК извещателя с поверхностной зоной обнаружения (см. п.7.1.4), направленной вдоль потолка.

Необходимо учитывать, что срабатывание охранно-дымовых систем может привести к срабатыванию технических средств пожарной сигнализации (если они установлены). Это обстоятельство может по-

требовать принятия специальных технических решений, обычно на аппаратно-программном уровне конфигурирования охранно-пожарной или интегрированной системы безопасности объекта при использовании охранно-дымовых систем в помещениях оснащенных пожарными извещателями по ГОСТ Р 53325-2009 и (или) автоматическими установками пожаротушения [21].

У всех входов в здание, либо помещение, в котором установлена охранно-дымовая система, рекомендуется расположить предупреждающий знак, образец которого приведен в МЭК 62642-8:2011.

7.6. Средства защиты кассет с деньгами

В некоторых случаях, например, при большой удаленности охраняемого банкомата от СПВО, могут быть использованы специальные устройства активной защиты кассет с наличными деньгами от несанкционированного доступа (спецкассеты), основанные на технологии окрашивания купюр при срабатывании ТСОС, например, извещателей, защищающих банкомат от взлома и криминального открывания сейфа, а также от несанкционированного перемещения банкомата с целью взлома его сейфа в удаленном скрытом месте.

Для обеспечения такой защиты в каждую кассету банкомата могут быть вмонтированы элементы, позволяющие установить систему по защите наличных денег, хранящихся в кассетах, с применением технологии окрашивания купюр.

В состав комплекта защиты, как правило, входят:

- модули активной защиты со специальными несмываемыми чернилами,
- элементы управления для активации защиты.

Для каждого типа кассет существует свой комплект средств защиты, который может работать либо автономно, осуществляя контроль статуса кассет при их работе в банкомате, либо быть интегрированным в комплекс мер по защите денежных средств вне кассового центра при инкассации и хранении.

Основным условием применения технических средств защиты кассет с наличными деньгами, использующих технологию окрашивания купюр при попытке вскрытия или кражи кассет, является обеспечение этими техническими средствами закрашивания всех машиночитаемых признаков (соответствующих зон) на банкнотах, используемых банкоматами с функцией приема наличных денег и платежными терминалами для идентификации подлинности денежных купюр.

7.7. Средства защиты от скимминга

В соответствии с рекомендациям Банка России [5] все БУС должны быть оснащены антискимминговым оборудованием, обеспечивающим защиту банкоматов и платежных терминалов, а также клиентов кредитных (платежных) организаций от мошенничества, связанного с незаконным считыванием конфиденциальной информации ИЭК с целью дальнейшей подделки ИЭК и незаконного снятия средств со счетов граждан. На рынке представлен широкий спектр устройств, предназначенных для защиты БУС от скимминга.

Технические средства защиты от скимминга можно разделить на две основные группы:

- антискимминговые средства пассивной защиты;
- средства активного противодействия скимингу.

Антискимминговые средства пассивной защиты представляют собой специальные накладки, препятствующие установке посторонних устройств на картридер БУС.

Конструкция антискимминговых устройств пассивной защиты должна соответствовать следующим требованиям:

- рабочее положение антискимминговых устройства на картридере БУС должно контролироваться электроконтактным либо магнитоконтактным датчиком, чувствительным к снятию антискимминговых устройства с картридера;

- при удалении (попытке удаления) антискимминговых устройства картридер БУС должен блокироваться (отключаться);

- конструкция антискимминговых устройства должна обеспечивать необходимую прочность (приложение Г) и устойчивость к воздействию различных внешних факторов;

- корпус антискимминговых устройства должен быть прозрачным, чтобы визуально можно быть определить наличие скимминговых устройства

Необходимо отметить, что эффективность пассивной защиты увеличивается при размещении на экране банкомата изображения правильного вида картридера.

Антискимминговые технические средства пассивной защиты имеют следующие недостатки:

- не подходят для блокирования миниатюрных скиммеров;

- злоумышленники способны изготавливать скиммеры в корпусах, внешне практически не отличимых от пассивных антискимминговых устройств или предназначенные для установки незаметно на популярные пассивные антискимминговые устройства;

- не формируют извещение об обнаружении скиммингового устройства, поэтому они не могут быть включены в общую систему комплексной охраны БУС;

- довольно часто уничтожаются просто из хулиганских побуждений.

Таким образом, пассивные антискимминговые средства не обеспечивают необходимый уровень защиты от скимминга и поэтому не рекомендуются для использования в комплексе технических средств централизованной охраны БУС.

Принцип действия средств активного противодействия скимммингу основан на создании электромагнитного поля в зоне картридера БУС, блокирующий скимминговые устройства.

Средства активного противодействия скимммингу должны предусматривать:

- возможность интеграции в централизованную систему мониторинга функционирования БУС;

- отсутствие возможности у злоумышленника обнаружить устройство визуально;

- наличие датчика проверки наличия "защитного поля", позволяющее обнаружить выведение из строя трансмиттера или атаку на него (например, путем излучения в противофазе);

- блокирование функционирования или отключение БУС при неисправности антискимминговой защиты, блокировка картридера;

- чувствительность к установке скиммингового оборудования, при обнаружении которого должно формироваться тревожное извещение;

- выдача уведомления о потенциальной угрозе по линии связи БУС с кредитной (платежной организацией);

- выход для формирования тревожного сообщения на ППКОП (УОО СПИ) для последующей передачи информации на ПЦО;

- хранение информации о тревогах в энергонезависимой памяти;

- световая индикация состояния.

В качестве технического средства активного противодействия скимминг может быть использован, например, комплект оборудования "Cerber" (ООО "АНСЕР ПРО").

Недостатком технических средств активного противодействия скимминг является то, что на части устройств БУС близкое расположение считывающего устройства к входу картридера может привести к невозможности установки подобных систем без создания помех работе БУС.

7.8. Средства контроля и передачи извещений

Для контроля состояния технических средств обнаружения проникновения (п.7.1) и тревожной сигнализации (7.2), в том числе средств активного противодействия скимминг (п.7.7), а также для управления средствами активной защиты БУС (п.7.5), оповещения и передачи извещений на ПЦО, в большинстве случаев

используется объектовое оборудование[32] систем передачи извещений (СПИ), включенных в "Список ТСО".

Общие рекомендации по выбору и применению подразделениями вневедомственной охраны объектового оборудования проводных СПИ, устойчивых к несанкционированному обходу. приведены в Р 78.36.020-2012 МВД России [15].

Для организации централизованной охраны БУС и зон их размещения может быть использовано, например, следующее объектовое оборудование: контроллер "Приток-А-КОП-02" (СПИ "Приток-А"), ППКОП "Тандем-1" (СПИ "Атлас-20"), ППКОП "Юпитер" 4 (8, 16) IP/GPRS (СПИ "Юпитер"), ППКОП "Заря-УО-IP-GPRS" (СПИ "Заря"), УОО "6EG" (СПИ "Ахтуба"), использующее для информационного обмена (контроля и передачи извещений) сетевые каналы связи (TCP/IP) или каналы сотовой связи (GSM, GPRS).

Вместе с тем, при использовании объектового оборудования СПИ с GSM-каналом передачи извещений, не рекомендуется устанавливать антенну GSM-канала внутри БУС, где установлены другие ТСОС, поскольку это может привести к сбоям в работе ТСОС, средств управления и безопасности БУС.

При расположении антенны GSM-канала передачи извещений объектового оборудования СПИ снаружи БУС необходимо принять дополнительные меры защиты, изложенные в п.7.4.5.2.

---

[32] Контроллеры, устройства объектовые оконечные (УОО), приборы приемно-контрольные (ППК) охранные или охранно-пожарные и т.п.

При использовании СПИ с GSM, GPRS, TCP/IP каналами передачи извещений следует иметь в виду, что надежность охраны БУС в этом случае будет зависеть от организаций-посредников (операторов сотовой связи, Интернет-провайдеров), которые не несут ответственность за безопасность объекта и не могут гарантировать стабильность канала связи и его работоспособность. В некоторых случаях, как например, согласно п.5 "Правил оказания услуг подвижной связи" [18], утвержденных Правительством Российской Федерации, при чрезвычайных ситуациях природного и техногенного характера оператор связи вправе временно прекращать или ограничивать абоненту оказание услуг подвижной связи. Не исключено, что нарушители могут воспользоваться этим, создавая ситуации со стороны, напоминающие чрезвычайные, что может привести к временному отключению канала связи и даст возможность нарушителям получить доступ к оборудованию, находящемуся на охране в течение длительного времени, без сигнализации об этом на ПЦО.

Кроме того, необходимо иметь в виду, что обычные РСПИ, использующие общедоступный радиоканал или GSM-канал связи могут быть выведены из строя квалифицированными нарушителями при помощи средств подавления радиосигналов. При этом антенны РСПИ (в случае их размещения снаружи БУС) могут быть умышленно выведены из строя (см. п.7.4.5).

В связи с этим для организации охраны БУС, в особенности групп ОП, ОВ и ОУ высокой категории материальной значимости (категории М1, М2), размещенных в местах средней (п.3.2), повышенной (п.3.3) и высокой степени риска (п.3.4), целесообразно

применение РСПИ повышенной надежности и устойчивости к саботажу, которые должны обеспечивать:

- устойчивую связь на необходимых для оперативного реагирования ГЗ СПВО расстояниях.
- регулярный автоматический контроль канала связи;
- устойчивость к подавлению радиосигналов;
- защиту от подмены;
- возможность скрытой установки объектового оборудования и антенны внутри БУС (в т.ч. в сейфе банкомата).

7.9. Средства контроля и управления доступом

Средства контроля и управления доступом (СКУД) в отдельно выделенную зону круглосуточного банковского самообслуживания ("зону 24") предназначены для:

- организации санкционированного доступа клиентов и персонала кредитных (платежных, сервисных) организаций, обслуживающих БУС, в помещение "зоны 24";
- ограничения проникновения в "зону 24" случайных лиц, в том числе имеющих криминальные цели;
- предотвращения умышленного повреждения БУС и осуществления других незаконных действий;
- повышения безопасности клиентов при совершении ими банковских (платежных) операций;
- повышения безопасности инкассаторов и технических специалистов кредитных (платежных, сервисных) организаций при загрузке или выгрузке наличных денег и техническом обслуживании БУС.

На двери круглосуточной зоны самообслуживания "зоны 24", закрывающей доступ к банкомату, должен быть установлен электромеханический замок,

управляемый контроллером СКУД при получении разрешающего сигнала со считывателя ИЭК.

Обзор запирающих устройств, представленных на российском рынке, приведен в РМ 78.36.002-2012 МВД России [19], методические рекомендации по эффективному применению запирающих устройств при организации охраны имущества граждан и организаций – в Р 78.36.017-2012 МВД России [20].

У входа в помещение "зоны 24" должен быть размещен считыватель ИЭК, который должен иметь защищенный от внешних воздействий корпус, обеспечивающий следующие степени защиты:

- от механических ударов – IK10 (приложение Б);
- от попадания твердых предметов и влаги не ниже IP54 по ГОСТ 14254-96;
- защиту от установки на считыватель ИЭК скиммера.

В качестве карт доступа в помещение "зоны 24" считывателем СКУД должны приниматься ИЭК любых платежных систем, обслуживаемые БУС, установленными в "зоне 24", причем как ИЭК с магнитной полосой, так и с микропроцессором.

Считыватель ИЭК должен обеспечивать проверку подлинности, срока действия и регистрацию ИЭК, предъявляемой клиентом для прохода в "зону 24".

Для выхода из "зоны 24" внутри ее помещения возле входной двери должна быть установлена кнопка "Выход".

Если в помещении "зоны 24" установлено одно БУС, то до тех пор, пока клиент не завершит необходимые банковские (платежные) операции и не покинет помещение, входная дверь должна быть заблокирована "на вход" для других лиц, кроме сотрудников подразде-

ления безопасности кредитной (платежной) организации и сотрудников СПВО, обеспечивающих охрану данного объекта[33]. Снаружи такого помещения возле входной двери в удобном для визуального прочтения месте должно быть размещено информационное табло, сообщающее о томе, что помещение "зоны 24" занято или свободно.

В помещении "зоны 24" рекомендуется установить охранные извещатели, формирующие извещение о тревоге в случаях открывания входной двери без регистрации ИЭК в считывателе (см. п.7.1.1), разбития стекла во входной (остекленной) двери или оконных конструкциях помещения (см. п.7.1.2), несанкционированном проникновении с последующем перемещением в помещении "зоны 24" (см. пп.7.1.4, 7.1.5), а также при слишком длительном нахождения человека в "зоне 24" (возле охраняемых БУС)[34]. Кроме того, охранные извещатели, реагирующие на перемещение человека внутри небольшой "зоны 24", в которой установлено одно БУС, могут быть задействованы для выполнения сервисных функций, например отслеживания ситуации, при которой клиент предъявил ИЭК,

---

[33] Указанные сотрудники должны быть обеспечены так называемыми "мастер-картами" – специальными (служебными) ИЭК, обеспечивающими возможность беспрепятственного входа в помещение "зоны 24" при выполнении своих функций, независимо от нахождения кого-либо в "зоне 24".

[34] Извещение о превышении времени нахождения человека возле БУС, санкционированно вошедшего в помещение "зоны 24", может передаваться в мониторинговый центр кредитной организации, а также служить управляющим сигналом для оператора СОТ, контролирующего данную "зону 24".

открыл дверь, но передумал входить в "зону 24" и захлопнул дверь. В таких случаях блокировка замка входной двери должна быть снята, и должен быть разрешен доступ к БУС следующего посетителя.

7.10. Шлюзовые кабины безопасности

Для повышения инженерно-технической укрепленности и противокриминальной защиты БУС групп ОВ, ОУ, СВ, СУ рекомендуется применение специальных остекленных защитных барьеров вокруг БУС в виде полукруглой шлюзовой кабины, которые специально разрабатываются и поставляются различными организациями для повышения безопасности банкоматов и платежных терминалов, установленных или выходящих лицевой панелью в зоны свободного, в том числе круглосуточного доступа, а также на открытые участки территории.

Такие шлюзовые кабины, часто называемые кабинами безопасности, обеспечивают защиту БУС и их клиентов от:

- кражи наличных денег у клиентов;
- кражи ИЭК;
- подсматривания номера ИЭК и ПИН-кода;
- возможных нападений, ограблений, мошенничества в отношении клиентов;
- умышленного повреждения или уничтожения БУС, вандализма,
- взлома БУС с целью хищения наличных денег или несанкционированного доступа к программно-аппаратной части БУС;
- хищения отдельно установленного БУС.

Шлюзовые кабины безопасности БУС должны иметь защитное остекление класса защиты не ниже 3 (см. приложение Е) и быть оборудованы электронной СКУД, соответствующей рекомендациям, приведенным в п.7.9.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Уголовный кодекс Российской Федерации (УК РФ) от 13 июня 1996 г. № 63-ФЗ (ред. от 01 ноября 2013 г.).

2. Федеральный закон от 02 декабря 1990 г. № 395-1 (ред. от 30 сентября 2013 г.) "О банках и банковской деятельности".

3. Федеральный закон Российской Федерации от 03 июня 2009 г. № 103-ФЗ (ред. от 27 июня 2011 г.) "О деятельности по приему платежей физических лиц, осуществляемой платежными агентами".

4. Федеральный закон Российской Федерации от 22 мая 2003 г. № 54-ФЗ (ред. от 25 ноября 2013 г.) "О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт".

5. "Рекомендации по повышению уровня безопасности при использовании банкоматов и платежных терминалов" (приложение к письму Банка России от 01 марта 2013 г. № 34-Т).

6. "Перечень объектов, подлежащих обязательной охране полицией", утв. Распоряжением Правительства Российской Федерации от 02 ноября 2009 г. № 1629-р (ред. от 10 декабря 2013 г.).

7. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ (ред. от 23 июля 2013 г.) "О персональных данных".

8. Положение Банка России от 19 августа 2004 г. № 262-П "Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях

противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".

9. "Памятка "О мерах безопасного использования банковских карт" (приложение к письму Банка России от 02 октября 2009 г. № 120-Т).

10. СанПиН 2.2.1/2.1.1.1278-03 "Проектирование, строительство, реконструкция и эксплуатация предприятий, планировка и застройка населенных пунктов. Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий. Санитарные правила и нормы" (ред. от 15 марта 2010 г.).

11. РД 78.36.003-2002 МВД России "Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств".

12. "Положение о порядке ведения кассовых операций и правилах хранения, перевозки и инкассации банкнот и монеты Банка России в кредитных организациях на территории Российской Федерации", утв. Банком России 24 апреля 2008 г. № 318-П (ред. от 07 февраля 2012 г.).

13. "Список технических средств безопасности, удовлетворяющих "Единым требованиям к системам передачи извещений и системам мониторинга подвижных объектов, предназначенным для применения в подразделениях вневедомственной охраны" и "Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны".

14. Р 78.36.028-2012 МВД России "Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов".

15. Р 78.36.002-2010 МВД России "Выбор и применение систем охранных телевизионных".

16. Р 78.36.018-2011 МВД России. "Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности".

17. Р 78.36.020-2012 МВД России "Рекомендации по выбору и применению объектового оборудования проводных систем передачи извещений, устойчивых к несанкционированному обходу".

18. "Правила оказания услуг подвижной связи", утв. Постановлением Правительства Российской Федерации от 25 мая 2005 г. № 328 (ред. от 01 декабря 2013г.).

19. РМ 78.36.002-2012 МВД России "Обзор запирающих устройств на отечественном рынке".

20. Р 78.36.017-2012 МВД России "Об эффективном применении запирающих устройств, имеющихся на отечественном рынке, при организации охраны имущества граждан и организаций".

21. СП 5.13130.2009 "Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования".

22. СНиП 3.03.01-87 "Несущие и ограждающие конструкции".

23. Указание Министерства внутренних дел Российской Федерации от 17 ноября 2011 г. №1/9940 "О защите банкоматов".

24. "Инструкция по защите банкоматов в учреждениях Сбербанка России" от 03 декабря 1998 г. № 465-р (с изменениями №1 от 22 марта 2004 г.).

25. "Инструкция по защите устройств самообслуживания подразделений Сбербанка России" от 24 января 2006 г. № 1412-р.

26. ГОСТ 530-2012 Кирпич и камень керамические. Общие технические условия.

27. ГОСТ 379-95 Кирпич и камни силикатные. Технические условия .

28. ГОСТ 9272-81 Блоки стеклянные пустотелые. Технические условия.

29. ГОСТ 9561-91 Плиты перекрытий железобетонные многопустотные для зданий и сооружений. Технические условия.

30. ГОСТ 11024-2012 Панели стеновые наружные бетонные и железобетонные для жилых и общественных зданий. Общие технические условия.

31. ГОСТ 12504-80 Панели стеновые внутренние бетонные и железобетонные для жилых и общественных зданий. Общие технические условия.

32. ГОСТ 12767-94 Плиты перекрытий железобетонные сплошные для крупнопанельных зданий. Общие технические условия.

33. ГОСТ 14254-96 Степени защиты, обеспечиваемые оболочками (код IP).

34. ГОСТ 21992-83 Стекло строительное профильное. Технические условия.

35. ГОСТ 23279-2012 Сетки арматурные сварные для железобетонных конструкций и изделий. Общие технические условия.

36. ГОСТ 24698-81 Двери деревянные наружные для жилых и общественных зданий. Типы, конструкция и размеры.

37. ГОСТ 25192-2012 Бетоны. Классификация и общие технические требования

38. ГОСТ 31173-2003 Блоки дверные стальные. Технические условия.

39. ГОСТ 31462-2011 Блоки оконные защитные. Общие технические условия.

40. ГОСТ 31817.1.1-2012 Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения.

41. ГОСТ Р 50009-2000 Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний.

42. ГОСТ Р 50658-94 Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений

43. ГОСТ Р 50659-2012 Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний

44. ГОСТ Р 50777-95 Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 6. Пассивные оптико-электронные инфракрасные извещатели для закрытых помещений и открытых площадок

45. ГОСТ Р 50862-2012 Сейфы, сейфовые комнаты и хранилища ценностей. Требования и методы

испытаний на устойчивость к взлому и огнестойкость.

46. ГОСТ Р 50941-96 Кабина защитная. Общие технические требования и методы испытаний.

47. ГОСТ Р 51053-97 Замки сейфовые. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому.

48. ГОСТ Р 51072-2005 Двери защитные. Общие технические требования и методы испытаний на устойчивость к взлому, пулестойкость и огнестойкость.

49. ГОСТ Р 51113-97 Средства защитные банковские. Требования по устойчивости к взлому и методы испытаний (с изменениями №1, №2).

50. ГОСТ Р 51186-98 Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний.

51. ГОСТ Р 51221-98 Средства защитные банковские. Термины и определения.

52. ГОСТ Р 51317.3.3-2008 Совместимость технических средств электромагнитная. Ограничение изменений напряжения, колебаний напряжения и фликера в низковольтных системах электроснабжения общего назначения. Технические средства с потребляемым током не более 16 А (в одной фазе), подключаемые к электрической сети при несоблюдении определенных условий подключения. Нормы и методы испытаний.

53. ГОСТ Р 51558-2008 Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний.

54. ГОСТ Р 52435-2005 Технические средства

охранной сигнализации. Классификация. Общие технические требования и методы испытаний.

55. ГОСТ Р 52502-2012 Жалюзи-роллеты металлические. Технические условия.

56. ГОСТ Р 52551-2006 Системы охраны и безопасности. Термины и определения.

57. ГОСТ Р 52582-2006 Замки для защитных конструкций. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому.

58. ГОСТ Р 52650-2006 Извещатели охранные комбинированные радиоволновые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний.

59. ГОСТ Р 53325-2009 Техника пожарная. Технические средства пожарной автоматики. Общие технические требования. Методы испытаний.

60. ГОСТ Р 53702-2009 Извещатели охранные поверхностные вибрационные для блокировки строительных конструкций закрытых помещений и сейфов. Общие технические требования и методы испытаний.

61. ГОСТ Р 54126-2010 Оповещатели охранные. Классификация. Общие технические требования и методы испытаний.

62. ГОСТ Р 54162-2010 Стекло закаленное. Технические условия.

63. ГОСТ Р 54169-2010 Стекло листовое, окрашенное в массе. Общие технические условия.

64. ГОСТ Р 54170-2010 Стекло листовое бесцветное. Технические условия.

65. ГОСТ Р 54171-2010 Стекло многослойное. Технические условия.

66. ГОСТ Р 54175-2010 Стеклопакеты клееные.

Технические условия.

67. ГОСТ Р 54176-2010 Стекло с низкоэмиссионным мягким покрытием. Технические условия.

68. ГОСТ Р 54177-2010 Стекло с низкоэмиссионным твердым покрытием. Технические условия.

69. ГОСТ Р 54178-2010 Стекло с солнцезащитным или декоративным мягким покрытием. Технические условия.

70. ГОСТ Р 54179-2010 Стекло с солнцезащитным или декоративным твердым покрытием. Технические условия.

71. ГОСТ Р 54180-2010 Стекло термоупрочненное. Технические условия.

72. ГОСТ Р 54455-2011 Системы охранной сигнализации. Методы испытаний на устойчивость к внешним воздействующим факторам.

73. ГОСТ Р 54620-2011 Глобальная навигационная спутниковая система. Система экстренного реагирования при авариях. Автомобильная система вызова экстренных оперативных служб. Общие технические требования

74. ГОСТ Р 54832-2011 Извещатели охранные точечные магнитоконтактные. Общие технические требования и методы испытаний.

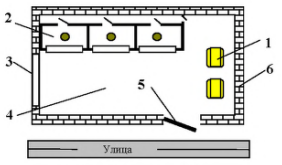
75. ГОСТ IEC 60065-2011 Аудио-, видео- и аналогичная электронная аппаратура. Требования безопасности.

76. МЭК 62642-8:2011 Системы тревожной сигнализации. Системы сигнализации о вторжении и захвате. Часть 8: Системы (устройства) безопасности, обеспечивающие защиту с помощью дыма или тумана.

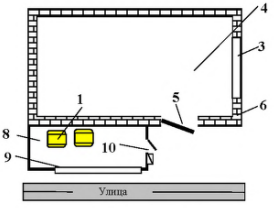
77. EN 1143-1:2005 + A1:2009 Устройства для безопасного хранения. Требования, классификация и методы испытания на устойчивость к взлому. Часть 1. Сейфы, сейфы для банкоматов, двери для сейфовых хранилищ и сейфовые хранилища.

78. EN 50102:1995 Степени защиты, обеспечиваемые оболочками для электрооборудования от внешних механических ударов (код IK).

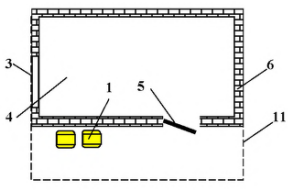
Приложение А
(справочное)
Основные варианты размещения банковских устройств самообслуживания



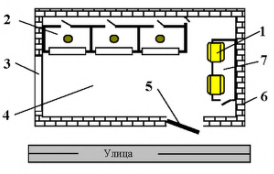
а) БУС группы ОП



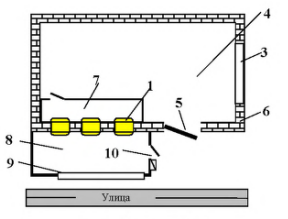
б) БУС группы ОВ



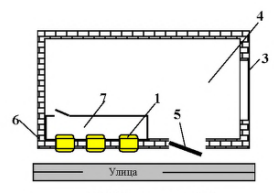
в) БУС группы ОУ



г) БУС группы СП



д) БУС группы СВ



е) БУС группы СУ

Условные обозначения:

1 – БУС;

2 – рабочие места персонала организации;

3 – остекление операционного зала (офиса),

4 – операционный или торговый зал (офис, зал ожидания),

5 – вход в организацию,

6 – наружные стены здания организации,

7 – сервисная зона,

8 – зона самообслуживания ("зона 24"),

9 – остекление зоны самообслуживания,

10 – вход в зону самообслуживания ("зону 24"),

11 – ограждение территории, закрывающее свободный въезд (подъезд к БУС) автотранспорта.

Приложение Б
(справочное)

Классификация сейфов банковских устройств самообслуживания по устойчивости к взлому

Классификация сейфов БУС по устойчивости к взлому по ГОСТ Р 50862-2012 и EN 1143-1:2005+A1: 2009 приведена в таблице Б.1.

Таблица Б.1 – Классификация сейфов БУС по устойчивости к взлому

Класс устойчивости сейфа БУС к взлому		Сопротивление взлому, в условных единицах сопротивления, не менее			Сила отрыва, кН, не менее	Сопротивление разрушению элементов крепления, в единицах сопротивления, не	Замки	
		Частичный доступ		Полный доступ			Количество, не менее	Класс устойчивости к криминальному открыванию и взлому по ГОСТ
		Кроме доступа через отверстия	Доступ через отверстия[35]					
L	Корпус	20	20	30	50	50	1	A
	Дверь	30	30	50				

[35] Применимо только к фактически используемым отверстиям; заделанные и неиспользуемые отверстия должны удовлетворять общим значениям

Класс устойчивости сейфа БУС к взлому	Сопротивление взлому, в условных единицах сопротивления, не менее			Сила отрыва, кН, не менее	Сопротивление разрушению элементов крепления, в единицах сопротивления, не	Замки	
	Частичный доступ		Полный доступ			Количество, не менее	Класс устойчивости к криминальному открыванию и взлому по ГОСТ
	Кроме доступа через отверстия	Доступ через отверстия[35]					
I	30	30	50	50	50	1	A
II	50	35	80	50	50	1	A
III	80	65	120	50	50	1	B
IV	120	100	180	100	50	2	B
V	180	145	270	100	50	2	B
VI	270	220	400	100	70	2	C
VII	400	350	600	100	120	2	C
VIII	550	500	825	100	160	2	C

Сейфы БУС, имеющие класс устойчивости к взлому не ниже II и имеющие маркировку "EX", обладают также некоторой степенью устойчивости к взлому после взрыва по EN 1143-1:2005+A1:2009, приведенную в таблице Б.2.

Таблица Б.2 – Классификация сейфов БУС по устойчивости к взлому после взрыва

Класс устойчивости сейфа БУС к взлому по ГОСТ Р 50862-2012 (EN 1143-1:2005+A1:2009)	Дополнительные требования к сейфу БУС для обозначения "EX" по EN 1143-1:2005+A1:2009. Значение устойчивости к взлому после взрыва, в условных единицах сопротивления, не менее
II	4
III	6
IV	9
V	14
VI	20
VII	30
VIII	41

Приложение В
(справочное)
Классификация строительных конструкций зон размещения банковских устройств самообслуживания по устойчивости к криминальному разрушению

В.1. Строительная конструкция 1 класса защиты (минимально необходимая степень защиты объекта от проникновения):

а) гипсолитовая, гипсобетонная толщиной не менее 75 мм;

б) щитовая деревянная конструкция толщиной не менее 45 мм;

в) конструкция из бревен или бруса толщиной не менее 100 мм;

г) каркасная перегородка толщиной не менее 20 мм с обшивкой металлическими (в том числе профилированными) листами толщиной не менее 0,55 мм;

д) перегородка из кирпича керамического по ГОСТ 530-2012 или силикатного по ГОСТ 379-95 толщиной не менее 120 мм, выполненная по СНиП 3.03.01-87;

е) перегородка из легкого теплоизоляционного бетона толщиной менее 200 мм;

ж) внутренняя стеновая панель толщиной 100 мм по ГОСТ 12504-80;

з) многопустотная железобетонная конструкция толщиной 160 мм по ГОСТ 9561-91;

и) перегородки из профильного строительного стекла по ГОСТ 21992-83 или стеклянных пустотелых блоков по ГОСТ 9272-81.

В.2. Строительная конструкция 2 класса защиты (средняя степень защиты объекта от проникновения):

а) конструкция из бревен или бруса толщиной не менее 200 мм;

б) кирпичная стена толщиной 250 мм по СНиП 3.03.01-87;

в) пустотная железобетонная плита толщиной 220, 260 и 300 мм по ГОСТ 9561-91 из легкого бетона и толщиной 160 мм из тяжелого бетона;

г) сплошное железобетонное перекрытие толщиной 120, 160 мм по ГОСТ 12767-94 из легкого бетона;

д) стеновая панель наружная по ГОСТ 11024-2012, внутренняя по ГОСТ 12504-80 и блок стеновой по ГОСТ 19010-82 из легкого бетона толщиной от 100 до 300 мм;

е) стена из монолитного железобетона по СНиП 3.03.01-87, изготовленная из тяжелого бетона, толщиной до 100 мм;

ж) строительная конструкция, относящаяся к 1 классу защиты, усиленная стальной сеткой по ГОСТ 23279-2012 с толщиной прутка 8 мм и с ячейкой размерами 100×100 мм.

В.3. Строительная конструкция 3 класса защиты (высокая степень защиты объекта от проникновения):

а) кирпичная стена толщиной более 380 мм по СНиП 3.03.01-87;

б) пустотное железобетонное перекрытие толщиной 220, 260 и 300 мм по ГОСТ 9561-91 из тяжелого бетона;

в) сплошное железобетонное перекрытие толщиной 120 и 160 мм по ГОСТ 12767-94 из тяжелого бетона;

г) стеновая панель наружная по ГОСТ 11024-2012 и блок стеновой по ГОСТ 19010-82 из легкого бетона толщиной более 300 мм;

д) стеновая панель наружная по ГОСТ 11024-2012, внутренняя по ГОСТ 12504-80, блок стеновой по ГОСТ 19010-82 и стена из монолитного железобетона по СНиП 3.03.01-87 толщиной от 100 до 300 мм из тяжелого бетона;

е) строительная конструкция 1 класса защиты, дополнительно усиленная стальной решеткой, выполненной из прутьев толщиной не менее 10 мм, образующих (путем сварных соединений) ячейки размером не более 150×150 мм;

ж) строительная конструкция 2 класса защиты, усиленная стальной сеткой по ГОСТ 23279-2012 с толщиной прутка 8 мм и с ячейкой размерами 100×100 мм.

В.4. Строительная конструкция 4 класса защиты (специальная степень защиты объекта от проникновения) – конструкция, соответствующая 5-му и выше классу устойчивости к взлому по ГОСТ Р 50862-2012.

Приложение Г
(справочное)
Классификация антивандальной защиты банковских устройств самообслуживания и технических средств охраны

Классификация антивандальной защиты БУС и технических средств охраны, установленных в зонах размещения БУС, по ГОСТ Р 54455-2011 (МЭК 62599-1:2010) и EN 50102-1995 приведена в таблице Г.1.

Таблица Г.1 – Классификация антивандальной защиты БУС и технических средств охраны

Степень защиты (код IK)	*Энергия удара, Дж*	*Уровень антивандальной защиты*	*Примечание*
01	0,15	Низкий уровень	Не обеспечивает минимально необходимой защиты БУС и ТСО от механических ударов
02	0,20		
03	0,35		
04	0,50	Пониженный уровень	Не обеспечивает достаточной для эксплуатации в реальных условиях зашиты БУС и ТСО от механических ударов
05	0,70		
06	1,00		
07	2,00	Средний уро-	Обеспечивает

		вень	минимально необходимую защиту БУС и ТСО, устанавливаемых в помещении, от случайных механических ударов
08	5,00	Повышенный уровень	Обеспечивает защиту БУС и ТСО, устанавливаемых в помещении, снаружи здания или на открытой территории от случайных механических ударов
09	10,00		
10	20,00	Высокий уровень	Обеспечивает устойчивость БУС и ТСО, устанавливаемых в помещении, снаружи здания или на открытой территории к случайным механическим ударам и попыткам умышленного повреждения (из хулиганских побуждений или с целью вывода из строя)

Приложение Д
(справочное)
Классификация дверных конструкций зон размещения банковских устройств самообслуживания по устойчивости к взлому

Д.1. Дверные конструкции 1 класса защиты (минимально необходимая степень защиты объекта от проникновения):

а) защитные двери, соответствующие I классу устойчивости к взлому по ГОСТ Р 51072-2005;

б) взломоустойчивые защитные дверные блоки, соответствующие классу устойчивости к взлому ПВ2 и выше по ГОСТ 31462-2011;

в) двери деревянные типа Н (входные, тамбурные) или С (служебные) по ГОСТ 24698-81;

г) остекленные дверные конструкции, изготовленные с применением листовых стекол по ГОСТ Р 54170-2010, ГОСТ Р 54169-2010, стекол с различными видами низкоэмиссионных, солнцезащитных, декоративных мягких и твердых покрытий по ГОСТ Р 54176-2010, ГОСТ Р 54177-2010, ГОСТ Р 54178-2010, ГОСТ Р 54179-2010, закаленных стекол по ГОСТ Р 54162-2010, термоупрочненных стекол по ГОСТ Р 54180-2010, многослойных ударостойких стекол класса РА1 и выше по ГОСТ Р 54171-2010, а также стеклопакетов по ГОСТ Р 54175-2010, выполненных с применением указанных видов стекол;

д) металлические решетчатые двери произвольной конструкции, изготовленные из стальных прутьев диаметром не менее 9 мм (площадью сечения не менее 80 мм^2), образующих ячейки площадью не более 230 см^2 и скрепленных между собой сварным соединением в каждом пересечении;

е) жалюзи-роллеты металлические, соответствующие классу устойчивости к взлому Р2 и выше по ГОСТ Р 52502-2012.

Д.2. Дверные конструкции 2 класса защиты (средняя степень защиты объекта от проникновения):

а) защитные двери, соответствующие II классу устойчивости к взлому по ГОСТ Р 51072-2005;

б) взломоустойчивые защитные дверные блоки, соответствующие классу устойчивости к взлому ПВ3 и выше по ГОСТ 31462-2011;

в) обычные дверные конструкции, соответствующие категории и классу устойчивости О-II и выше по ГОСТ Р 51242-98;

г) остекленные дверные конструкции, изготовленные с применением многослойных ударостойких стекол класса РА2 и выше по ГОСТ Р 54171-2010, а также стеклопакетов по ГОСТ Р 54175-2010, выполненных с применением указанных видов стекол;

д) металлические решетчатые двери, изготовленные из стальных прутьев диаметром не менее 16 мм, образующих ячейку не более 150×150 мм и скрепленных между собой сварным соединением в каждом пересечении. По периметру решетчатая дверь

должна быть обрамлена стальным уголком размером не менее 35×35×4 мм;

е) стальные решетчатые раздвижные двери, изготовленные из полосы сечением не менее 30×4 мм с ячейкой не более 150×150 мм;

ж) стальные защитные дверные блоки с прочностными характеристиками класса М1 и выше по ГОСТ 31173-2003;

з) жалюзи-роллеты металлические, соответствующие классу устойчивости к взлому Р4 и выше по ГОСТ Р 52502-2012.

Д.3. Дверные конструкции 3 класса защиты (высокая степень защиты объекта от проникновения):

а) защитные двери, соответствующие III классу устойчивости к взлому по ГОСТ Р 51072-2005;

б) взломоустойчивые защитные дверные блоки, соответствующие классу устойчивости к взлому ПВ4 и выше по ГОСТ 31462-2011;

в) усиленные дверные конструкции, соответствующие категории и классу устойчивости У-I и выше по ГОСТ Р 51242-98;

г) остекленные дверные конструкции, изготовленные с применением многослойных ударостойких стекол класса РА3 и выше по ГОСТ Р 54171-2010, а также стеклопакетов по ГОСТ Р 54175-2010, выполненных с применением указанных видов стекол;

д) стальные защитные дверные блоки с прочностными характеристиками класса М2 и выше по ГОСТ 31173-2003;

е) жалюзи-роллеты металлические, соответствующие классу устойчивости к взлому Р6 и выше по ГОСТ Р 52502-2012.

Д.4. Дверные конструкции 4 класса защиты (специальная степень защиты объекта от проникновения):

а) защитные двери, соответствующие IV классу устойчивости к взлому по ГОСТ Р 51072-2005;

б) взломоустойчивые защитные дверные блоки, соответствующие классу устойчивости к взлому ПВ5 и выше по ГОСТ 31462-2011;

в) специальные дверные конструкции, соответствующие категории и классу устойчивости С-II и выше по ГОСТ Р 51242-98;

г) остекленные дверные конструкции, изготовленные с применением многослойных ударостойких стекол класса РА4 и выше по ГОСТ Р 54171-2010, взломостойких стекол класса Р8В и выше по ГОСТ Р 54171-2010, а также стеклопакетов по ГОСТ Р 54175-2010, выполненных с применением указанных видов стекол;

д) двери сейфовых комнат и хранилищ ценностей по ГОСТ Р 50862-2012;

е) двери защитных кабин по ГОСТ Р 50941-96.

Приложение Е
(справочное)
Классификация оконных конструкций зон размещения банковских устройств самообслуживания по устойчивости к криминальному разрушению

Е.1. Оконные конструкции 1 класса защиты (минимально необходимая степень защиты объекта от проникновения):

а) взломоустойчивые защитные оконные блоки, соответствующие классу устойчивости к взлому ПВ2 и выше по ГОСТ 31462-2011;

б) остекленные конструкции зданий и помещений (окна, витрины, остекленные фасады или крыши, внутренние остекленные перегородки между помещениями и т.п.), изготовленные с применением листовых стекол по ГОСТ Р 54170-2010, ГОСТ Р 54169-2010, стекол с различными видами низкоэмиссионных, солнцезащитных, декоративных мягких и твердых покрытий по ГОСТ Р 54176-2010, ГОСТ Р 54177-2010, ГОСТ Р 54178-2010, ГОСТ Р 54179-2010, закаленных стекол по ГОСТ Р 54162-2010, термоупрочненных стекол по ГОСТ Р 54180-2010, многослойных ударостойких стекол класса РА1 и выше по ГОСТ Р 54171-2010, а также стеклопакетов по ГОСТ Р 54175-2010, выполненных с применением указанных видов стекол.

Е.2. Оконные конструкции 2 класса защиты (средняя степень защиты объекта от проникновения):

а) взломоустойчивые защитные оконные блоки, соответствующие классу устойчивости к взлому ПВ3 и выше по ГОСТ 31462-2011;

б) остекленные конструкции зданий и помещений, изготовленные с применением многослойных ударостойких стекол класса РА2 и выше по ГОСТ Р 54171-2010, взломостойких стекол класса Р6В и выше по ГОСТ Р 54171-2010, а также стеклопакетов по ГОСТ Р 54175-2010, выполненных с применением указанных видов стекол;

в) защитные оконные блоки и другие остекленные конструкции зданий и помещений 1 класса защиты, оборудованные дополнительными средствами инженерно-технической укрепленности, в качестве которых могут быть использованы, например, жалюзи-роллеты металлические, соответствующие классу устойчивости к взлому Р2 и выше по ГОСТ Р 52502-2012.

Е.3. Оконные конструкции 3 класса защиты (высокая степень защиты объекта от проникновения):

а) взломоустойчивые защитные оконные блоки, соответствующие классу устойчивости к взлому ПВ4 и выше по ГОСТ 31462-2011;

б) остекленные конструкции зданий и помещений, изготовленные с применением многослойных ударостойких стекол класса РА3 и выше по ГОСТ Р 54171-2010, взломостойких стекол класса Р7В и выше по ГОСТ Р 54171-2010, а также стеклопакетов

по ГОСТ Р 54175-2010, выполненных с применением указанных видов стекол;

в) защитные оконные блоки и другие остекленные конструкции зданий и помещений 2 класса защиты, оборудованные дополнительными средствами инженерно-технической укрепленности, в качестве которых могут быть использованы, например, жалюзи-роллеты металлические, соответствующие классу устойчивости к взлому Р4 и выше по ГОСТ Р 52502-2012, другие защитные конструкции, соответствующие категории и классу устойчивости О-II и выше по ГОСТ Р 51242-98.

Е.4. Оконные конструкции 4 класса защиты (специальная степень защиты объекта от проникновения):

а) взломоустойчивые защитные оконные блоки, соответствующие классу устойчивости к взлому ПВ5 и выше по ГОСТ 31462-2011;

б) остекленные конструкции зданий и помещений, изготовленные с применением многослойных ударостойких стекол класса РА4 и выше по ГОСТ Р 54171-2010, взломостойких стекол класса Р8В и выше по ГОСТ Р 54171-2010, а также стеклопакетов по ГОСТ Р 54175-2010, выполненных с применением указанных видов стекол;

в) защитные оконные блоки и другие остекленные конструкции зданий и помещений 3 класса защиты, оборудованные дополнительными средствами инженерно-технической укрепленности, в качестве которых могут быть использованы, например, жалю-

зи-роллеты металлические, соответствующие классу устойчивости к взлому Р6 и выше по ГОСТ Р 52502-2012, другие защитные конструкции, соответствующие категории и классу устойчивости С-II и выше по ГОСТ Р 51242-98.