ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.53

DOI: 10.21822/2073-6185-2026-53-1-139-150 Оригинальная статья/ Original article

Модернизация системы обеспечения информационной безопасности ситуационного центра, являющегося объектом критической информационной инфраструктуры

И.А. Лоскутов[1,2,3], В.А. Репенко[4]

[1]Научно-производственная корпорация «Космические системы мониторинга, информационно-управляющие и электромеханические комплексы имени А.Г. Иосифьяна» (АО Корпорация «ВНИИЭМ»),
[1]107078, г. Москва, ул. Вольная, 30, стр. 10, Россия,
[2]Колледж экономики, права и информационных технологий,
[2]109029, г. Москва, ул. Нижегородская, 32, стр.16, Россия,
[3]МИРЭА - Российский технологический университет,
[3]119454, г. Москва, проспект Вернадского, 78, стр.4, Россия,
[4]Национальный исследовательский ядерный университет «МИФИ»,
[4]115409, г. Москва, Каширское шоссе, 31, Россия

Резюме. Цель. Целью исследования является повышение защищенности ситуационного центра, являющегося объектом критической информационной инфраструктуры. **Метод**. Методы научного познания, использованные при написании работы: систематизация, анализ, описание. **Результат**. Определена модель ситуационного центра, сформирована модель угроз. Предложены четыре подхода по определению значимости защиты от разных видов кибератак, сформированы рекомендации по защите. **Вывод**. Полученные в работе результаты не только структурируют информацию по вопросам обеспечения информационной безопасности ситуационного центра, но и пытаются математически описать закономерности ее модернизации, что может стать базисом для дальнейших исследований, как по направлению исследования, так и в смежных областях.

Ключевые слова: беспилотные летательные аппараты, информационная безопасность, ситуационный центр, критическая информационная инфраструктура, система защиты информации, угрозы

Для цитирования: И.А. Лоскутов, В.А. Репенко. Модернизация системы обеспечения информационной безопасности ситуационного центра, являющегося объектом критической информационной инфраструктуры. Вестник Дагестанского государственного технического университета. Технические науки. 2026;53(1):139-150. DOI:10.21822/2073-6185-2026-53-1-139-150.

Modernization of the information security system of the situational center, which is a critical information infrastructure facility

I.A. Loskutov[1,2,3], V. A. Repenko[4]

[1]A.G. Iosifian' Joint Company 'Research and Production Corporation "Space Monitoring Systems, information management and electromechanical complexes",
[1]30 Volnaya St., p. 10, Moscow 107078, Russia,
[2]College of Economics, Law and Information Technology,
[2]32 Nizhegorodskaya St., build.16, Moscow 109029, Russia,
[3]MIREA - Russian Technological University,
[3]78, Vernadsky Ave., build.4, Moscow 119454, Russia,
[4] National Research Nuclear University MEPhI,
[4]31 Kashirskoe highway, Moscow 115409, Russia

Abstract. Objective. The purpose of this study is to improve the security of a situation center, which is part of critical information infrastructure. **Method.** The research methods used in

writing this paper include systematization, analysis, and description. **Result.** A situation center model has been defined, and a threat model has been developed. Four approaches to determining the importance of protection against various types of cyberattacks are proposed, and recommendations for protection are developed. **Conclusion.** The results obtained in the work not only structure information on issues of ensuring information security of the situation center, but also attempt to mathematically describe the patterns of its modernization, which can become the basis for further research, both in the direction of the study and in related fields.

Keywords: unmanned aerial vehicles, information security, situation center, critical information infrastructure, information security system, threats

For citation: I.A. Loskutov, V.A. Repenko. Modernization of the information security system of the situational center, which is a critical information infrastructure facility. Herald of Daghestan State Technical University. Technical Sciences. 2026;53(1):139-150. (In Russ) DOI:10.21822/2073-6185-2026-53-1-139-150.

Введение. XXI век породил множество киберугроз, а также способов их доставки до атакуемого объекта. Кроме того, в последние десятилетия постоянно растет количество и виды кибернападений на предприятия [1] с целью получения несанкционированного доступа (НСД) к их коммерческой тайне и иных важных сведений о персонале [2]. Особенно данная выкладка важна для относящихся к категории критической информационной инфраструктуры (КИИ). Для осуществления планов злоумышленников, в последнее время начало набирать популярность использование беспилотных летательных аппаратов (БПЛА) [3]. Именно их массовое производство и относительно низкая цена [4] позволили приспособить с виду безобидные устройства для атак на автоматизированные информационные системы (АИС). Преимущества данного вида механизмов для злоумышленников очевидны – вследствие их относительно малого размера, появляется возможность незаметно проникнуть в контролируемую зону и начать проводить компьютерную атаку (КА). Именно поэтому, вопрос об обеспечении информационной безопасности (ИБ) объектов КИИ от малых летательных аппаратов (ЛА), несущих злонамеренное воздействие все более стал волновать специалистов по защите информации (ЗИ) [5].

Важно отметить, что, как и в случае с обычными КА, применение БПЛА в редких случаях проводится спонтанно [6], нарушители ИБ достаточно хорошо знают территорию объекта, а также примерное расположение наиболее значимых мест скопления важной информации и принятия решения (серверные, зоны управления и т.п.).

Постановка задачи. На предприятии значимую роль играет ситуационный центр (СЦ) [7]. Именно он становится одной из приоритетных целей КА, вследствие особенностей обрабатываемой там информации. Исследование вопросов по ЗИ для данного объекта априори становится актуальным. Поскольку редко используется определение ситуационного центра, предварительно покажем в общих чертах основные характеристики. В соответствии с [8] под СЦ следует понимать объединение технических средств и программных продуктов (ПП), направленное на подержание стабильности бизнес-процессов предприятия, а также обеспечение лаконичного внутреннего взаимодействия связанных с ним элементов предприятия. Однако в данном определении плохо раскрыты некоторые аспекты работы СЦ. Для уточнения информации обратимся к работе [9]. Именно в ней конкретизируется вариативность исполнений, которая условно делится на три группы, рис. 1.

Рис. 1 – Виды ситуационных центров
Fig. 1 – Types of situation centers

Отмеченная вариативность сделана с учетом влияния информационных технологий на внутренние процессы предприятия и СЦ, т.е. на степень их взаимодействия с АИС. В целом же, архитектурная модель СЦ будет усреднённо похожа на рассмотренное в работе [9] для МЧС России, рис. 2. Именно ее и будем принимать в качестве объекта ЗИ.

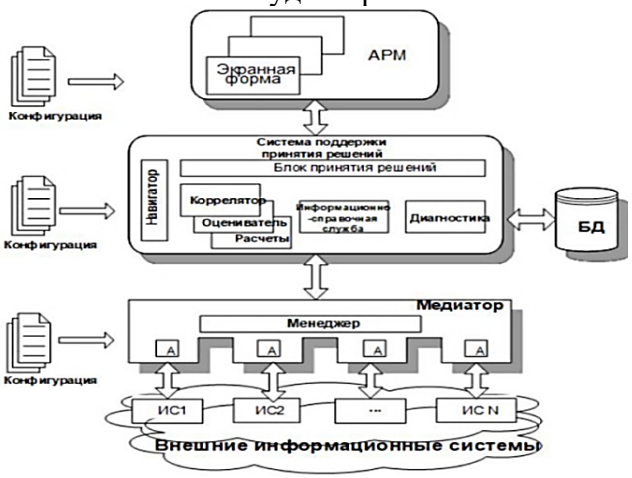

Рис. 2 – Обобщенная архитектурная модель ситуационного центра
Fig. 2 – Generalized architectural model of the situation center

На рис. 2 под АРМ понимается автоматизированное рабочее место, под БД – база данных, под ИС – информационная система. С точки зрения необходимых элементов, на основании показанной схемы, рис. 2 и сведений из [10], компонентный состав будет соответствовать рис. 3.

Рис. 3 – Компонентный состав ситуационного центра
Fig. 3 – Component composition of the situation center

Организация СЦ будет сегментирована по частям, рис.4.

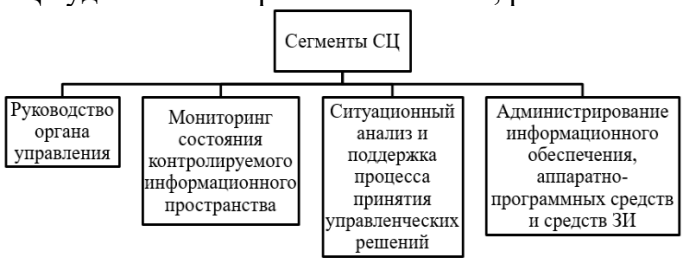

Рис. 4 – Сегментация ситуационного центра
Fig. 4 – Segmentation of the situation center

Наибольший интерес для данной работы представляет последний элемент, т.к. в нем упоминаются средства ЗИ (СЗИ), априори необходимые для обеспечения должного уровня ИБ.

Методы исследования. Проанализируем применяемую систему обеспечения информационной безопасности (СОИБ). Обратимся к научной работе [10], т.к. в ней показана интересная схема взаимодействия компонентов с СЗИ, рис. 5. На рис. 5 показаны элементы, необходимые для обеспечения должного уровня ИБ – определены модель нарушителя, модель угроз, политика. Примем данную логику взаимодействия за основу. Далее опишем необходимы требования для СОИБ [11]: использовать передовые технологии; не выходить за рамки, оговоренные законодательными актами России; архитектура построения – иерархическая; применение наиболее эффективных средств борьбы с кибернарушителями. Поскольку логика построения безопасных информационных сред в целом известна,

примем, что в СЦ изначально установлены наиболее актуальные ПП, обеспечивающие должный уровень ЗИ.

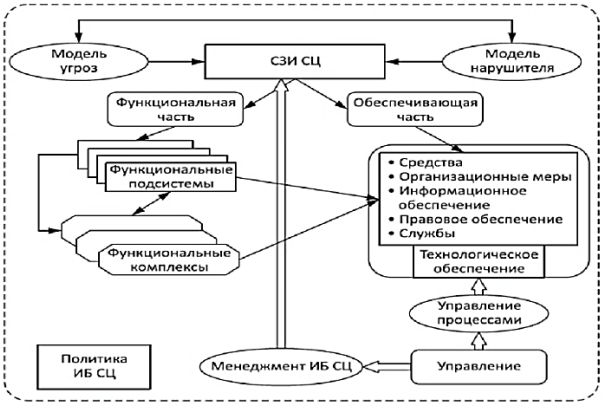

Рис. 5 – Схема взаимодействия СЗИ
Fig. 5 – Scheme of interaction of information security system

Отметим, что в системе установлена не отечественная операционная система (ОС) Windows Server, что вызывает рациональное пожелание о замене на одну из перечисленные в работе [12]. В аппаратной части необходимо отметить современные тенденции по переходу на отечественное оборудование, вследствие прекращения поставок иностранными компаниями [13], да и в целом политики ФСТЭК России, направленной на прекращение их лицензирования [14].

Имеется явная потребность в обновлении аппаратной части СОИБ. В части обеспечения ЗИ, как показывает практика, наиболее актуальной угрозой становится применение малых ЛА. Поскольку вопрос об ИБ в данном ключе актуален и мало предприятий на данный момент времени обладают системой защиты от них – примем, что ее у рассматриваемого СЦ нет. Соответственно, необходимо оценить способы получения информации при помощи БПЛА, которые в дальнейшем и будут парироваться СОИБ.

1) Расположение СЦ. Как показывает практика, многие СЦ предприятия мало заботятся о физической защите информации, о чем свидетельствует, например, работа [15]. И, если даже исключить вариант непосредственного подключения со стороны улицы, то все равно представляется возможность считать информацию с того же БПЛА, непосредственно находящегося вблизи коммуникаций.

2) Верхняя полусфера. О защите данной территории стали активно говорить в последнее время, как и о способах борьбы, пример – работа [16].

3) Для обеспечения должного уровня защиты необходимо использовать специальные комплексы аппаратно-программных средств, которые не установлены около помещения СЦ и на периметре предприятия.

4) Перехват данных, передаваемых по беспроводным технологиям. В данном случае уже имеются прецеденты, когда БПЛА подключался извне к внутренней WiFi системе и начинал перехват данных [17]. Таким образом, необходимо учитывать особенности распространения беспроводного сигнала на территории производства.

5) Злонамеренное падение. На данный момент времени не было найдено упоминания подобного применения БПЛА, хотя, безусловно, она уже была использована. Суть – активация встроенных функций аварийной посадки. Логика будет во многом похожа на отмеченные в патентной разработке [18]. В данном случае понимается медленный спуск на территорию предприятия даже при условии прерывания управления с помощью спецсредств. Ключевой особенностью станет тот факт, что после приземления, устройство все также может начать в автономном режиме подключаться к сети предприятия, а далее уже к СЦ и передавать наружу необходимые для злоумышленника сведения. Для защиты от угрозы, необходимо применять специальные технологии, не допускающие подобных планирований (что сложно реализовать) или использовать системы активной защиты

и шумогенераторы на крышах и иных возвышенностях в постоянно включенном режиме (что вполне реализуемо).

6) Подрезка информационного кабеля. Нередко инфокоммуникационное оборудование находится на верхних этажах, в которое БПЛА может залететь и осуществить непосредственное физическое подключение. Необходимо обеспечить защиту подобных помещений от стороннего проникновения, особенно извне здания.

7) Использование дрона как доставщика скаченной из АИС информации. В данном случае необходимо обеспечить невозможность физической передачи флешкарт и т.п. накопителей информации, как и проводить анализ поведения сотрудников с целью выявления потенциальных угроз, исходящих из них, особенно администраторов.

Можно констатировать о выявлении проблем СЦ, которые необходимо решить.

Составим подробную модель угроз для ситуационного центра предприятия, на котором он располагается. Модель угроз формируется на основании нормативно-правовых актов России и органа власти – ФСТЭК России. Наиболее подробно указана в Методическом документе от 2021 года [19], на него и будем далее опираться при моделировании потенциальных угроз СЦ. Первое на что следует обратить внимание – определение возможного нарушителя ИБ и его разделение по месту атаки (изнутри предприятия или снаружи). Деление нарушителей ИБ на внешних и внутренних показано на рис. 6. Следующим этапом станет их разграничение по уровням возможностей. Из [20] следует, что они подразделяются на $H_1 \ldots H_4$.

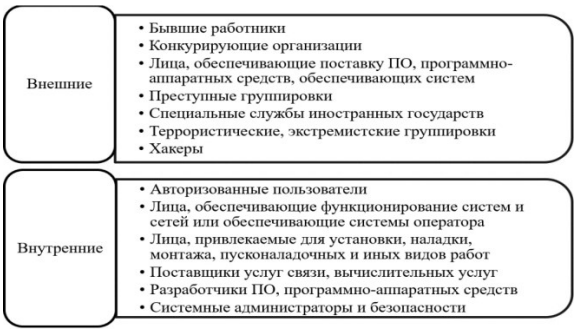

Рис. 6 – Возможные нарушители ИБ
Fig. 6 – Potential information security violators

Бывшие работники, безусловно, могут оказать негативные действия против АИС. Их знания расположения оборудования, основных узлов и точек подключения будут играть значительную роль при автономном подключении к СЦ. Уровень H_1.

Конкурирующие организации – поскольку СЦ принадлежит предприятию и обрабатывает значимые информационное ресурсы, нанимателями операторов дронов или же пилотами могут в большей вероятности стать сотрудники данных компаний. Уровень H_1.

Лица, поставляющие ПП, маловероятно станут атакующими, тем более с применением БПЛА. Причина первая – вредоносную программу можно установить непосредственно в код поставляемого ПО, применение малых ЛА в данном случае скорее станет редким исключением, его применение будет только в виде получателя информации, достаточно смутная перспектива. Причина вторая – выбор устанавливающих ПП на СЦ предприятиях. Выбор иметь СЦ будет ограничен только зарекомендовавшими себя фирмами, репутация которых будет многократно выше выигрыша от продажи полученной информации. Уровень не имеет значения.

Преступные группировки – возможные нарушители ИБ СЦ предприятия. Причин для их атак предостаточно – как самореализация и утверждение в обществе, так и получение материальной выгоды, например, при исполнении заказа от конкурирующей организации. Уровень H_2.

Специальные службы иностранных государств. Крайне маловероятная угроза, т.к. рассматриваемый СЦ не обрабатывает информацию типа «гостайна». Уровень не имеет значения.

Террористы. Аналогично предыдущему. Частные компании крайне редко подвергаются атакам террористов, кроме того целенаправленность их потенциальной КА мало связана с бизнес-процессами и т.п. информацией, обрабатываемой в СЦ. Сущность их действий хорошо показана в работе [21]. Уровень не имеет значения.

Хакеры, безусловно, будут являться потенциальными злоумышленниками. Как верно подмечено в базе данных ФСТЭК России, их основная цель это самореализация и финансовая выгода. Применение БПЛА для КА достаточно необычный способ киберпроникновения в серверное пространство, связанное с СЦ. Уровень $Н_1$.

Пользователи внутренней АИС не рационально причислять к потенциальным атакующим, т.к. применение БПЛА для них абсолютно нерациональное действие, исключение – использование его как контейнера, однако вероятность быть раскрытым слишком велика. Уровень не имеет значения.

Лица, обеспечивающие функционирование АИС аналогично предыдущему, не будут отнесены к категории потенциальных нарушителей. Уровень не имеет значения.

Установщики ПП и наладчики маловероятно будут атаковать АИС с применением БПЛА, т.к. существует много других более рациональных способов получить доступ изнутри. Уровень не имеет значения.

Поставщики услуг связи. Данные лица нерационально считать злоумышленниками, т.к. обычно соискатели на подобные должности проходят достаточно жесткий контроль, нередко применяются даже полиграф. Кроме того, применение БПЛА для потенциальной атаки данными сотрудниками также неоправданно. Уровень не имеет значения.

Разработчики ПО и программных средств – аналогично предыдущему. Уровень не имеет значения.

Системные администраторы и безопасности. Данные индивиды будут являться потенциальными нарушителями. Причина кроется в их возможности работать напрямую с системами ЗИ, применяемыми внутри АИС. Поведение атаки с их участием можно смоделировать следующим образом: партнер снаружи запускает дрон и подводит максимально близко к слепой зоне систем ИБ СЦ предприятия. Системные администраторы отключает частично защиту, отправляя ее на «штатную перезагрузку». В этот момент по полученной от него схеме – оператор дрона подсоединяется к серверным компонентам, скачивает информацию и улетает. Уровень $Н_2$. Сведем в табл. 1 полученные сведения.

Таблица 1. Характеристика нарушителей ИБ
Table 1. Characteristics of information security violators

Проникновение Penetration	Нарушитель Intruder	Уровень Level
Внешнее External	Бывшие работники Former employees	$Н_1$
	Конкурирующие организации Competing organizations	
	Хакеры Hackers	
	Преступные группировки Criminal groups	$Н_2$
Внутренние Internal	Системные администраторы и безопасности System administrators and security administrators	

Из табл. 1 следует, что максимальный уровень возможностей у потенциальных нарушителей $Н_2$, и останется таким же даже в случае сговора нескольких из представленных. Следующим этапом следует оценить потенциальный ущерб АИС и СЦ. В данном случае это будут $У_1$, $У_2$ и $У_3$. Т.е. ущерб физическим лицам из-за утечки их конфиденциальных и персональных данных; проблемы у юридического лица, повлекшие дополнительные материальные затраты; а также нарушение законов. Вне зависимости от способа подключения к АИС СЦ предприятия, способы в целом, останутся одинаковыми.

На рис. 7 представлены способы реализации угроз ИБ. Остановимся на определении угроз, свойственных АИС СЦ предприятия. В первом случае важно показать их характер: непреднамеренные / преднамеренные; неатропогенные; утечка по техническим каналам. Во втором случае, соотнесение шифра.

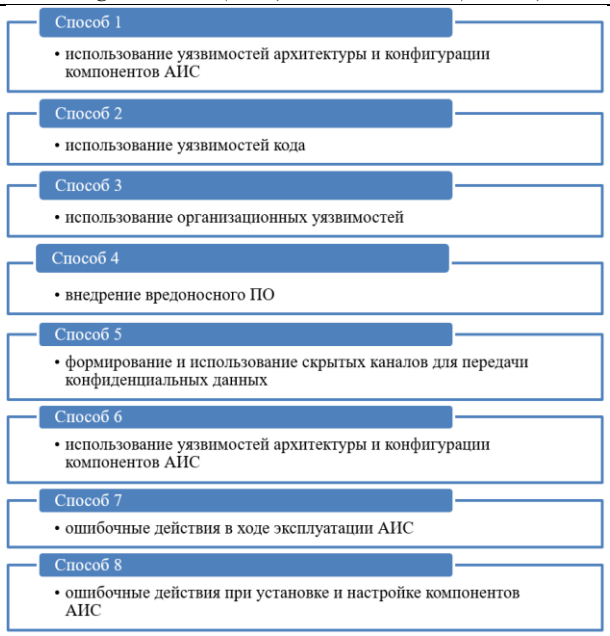

Рис. 7 – Способы реализации угроз ИБ
Fig. 7 – Methods of implementing information security threats

Применительно к рассматриваемому объекту это будут:

У.II.1, 3-6; У.III.1.2-1.9; У.III.2.1-2.13; У.III.3.1-3.7, 3.9; У.III.4.1-4.9; У.III.5.1-5.6.

Более подробно о вариациях угроз показано на уже упомянутом портале базы данных угроз ФСТЭК России, а также на [22], который дублирует информацию, так и обеспечивает более удобный способ навигации по базе, которая на данный момент плохо реализована на головном сайте.

Обсуждение результатов. В целом, были описаны все самые значимые элементы, свойственные модели угроз и можно однозначно сказать о ее завершенности. Отдельным моментом следует указать возможности математической реализации определенных частей модели угроз, особенно с учетом применимости БПЛА. В данном случае из-за отсутствия явной статистики по КА на СЦ и иные элементы предприятий можно вывести предварительную математическую формулу, которую в дальнейшем можно будет реализовать при создании модели угроз. Наиболее оправданным в данном случае следует считать:

1) Подход по определению вероятности возникновения КА на СЦ предприятии в целом посредством применения БПЛА. Как известно, среди КА наиболее распространено порядка сотни видов, в некоторых источниках пытаются указать более конкретную цифру. Так, например, в статье [23] говорится о 54 наиболее часто встречающихся. Однако, в любом случае, зависимость в первом приближении будет следующей:

$$P_{КА\_БПЛА} = 1 / N$$

где: $P_{КА\_БПЛА}$ – вероятность возникновения КА посредством БПЛА; N – количество известных КА.

Важно отметить, что подобный подход крайне грубый и принимает равнозначность видов атак, что, разумеется есть частный случай. Другое дело, ели провести видоизменение матаппарата. В данном случае зависимость приобретет следующий вид:

$$P_{КА\_БПЛА} = 1 - \sum_{k=1}^{N-1} P_i.$$

где: P_i– вероятность возникновения КА.

Рассчитать вероятность подобным образом намного проще, т.к. достаточно много компаний публикуют количественные показатели КА. Более того, именно такой путь на данный момент представляет возможным хоть как-то определить число проведенных атак с малых ЛА.

2) Подход поиска вероятности успешности КА. Для поиска вероятности успешности атаки следует проанализировать возможные способы проникновения. В частности, для атак с БПЛА они будут: подключение к беспроводной сети цели, использование технических

каналов, удаленная подрезка к сетевому кабелю и т.п. Уравнение в данном случае будет вида:

$$Р_{УСП\_КА\_БПЛА} = 1 / L \times S_j$$

где: $Р_{УСП\_КА\_БПЛА}$ – вероятность успешности определенного способа КА; L – количество вариаций КА; S_j – вероятность состояний.

Под вероятностью состояний понимается один из сценариев. Как пример, можно рассматривать все виды защитных действий, а можно учитывать вероятностный характер, так как уравнение верхнего уровня, внутренние множители могут быть коррелированы, что создаст дополнительный стимул развития направления.

3) Подход поиска усредненной вероятности возникновения КА на конкретном СЦ предприятии. Данный подход будет основан на определении вероятности КА при учете его характеристических особенностей, которые могут заинтересовать потенциальных злоумышленников. В простом случае это будет соотношение выявленных КА за период. Т.е. уравнение станет вида:

$$Р_{ШАНС\_КА} = M / C$$

где: $Р_{ШАНС\_КА}$ – вероятность возникновения КА на производстве; M – количество выявленных КА на СЦ предприятии за период времени; C – количество КА за период.

4) Подход определения среднеквадратичной суммы потерь СЦ предприятий посредством КА с БПЛА. Для оценки среднеквадратичных потерь следует вывести зависимость, связанную с общей стоимостью утраченных финансов, т.е.:

$$Pr = 1 / N_П \times Pr_{ПОТЕРЬ}$$

где: $N_П$ – количество предприятий за исследуемый период; $Pr_{ПОТЕРЬ}$ – общее количество финансовых потерь.

Данное уравнение наиболее полезно также и при определении суммы страхования, т.к. она может применяться как показатель для распределения потерь

С целью обеспечения должного уровня безопасности СЦ необходимо учесть вышеозвученные проблемы и найти оптимальные на них решения. Более того, с учетом отсутствия в чистом виде регулирующих нормативно-правовых актов по направлению, примененные подходы можно будет использовать при разработке соответствующих документов. Предварительно важно учесть финансовую составляющую, играющую немаловажную роль при учете потенциальных потерь. Для этого проведем оценку стоимости СЦ. В целом, стоимость СЦ будет напрямую зависеть от количества и значимости информации, поступающей в нее. Так как при расчете бралась концептуальная модель предприятия, можно принять ее как долю от общей выручки компании. Так как имеется деление на принадлежность к компании к малому / среднему / крупному бизнесу [24], то посчитаем что стоимость фирмы будет составлять 1,4 млрд. руб. Так как общесуммарный доход будет превышать потери от разрушения СЦ, примем что максимальное пагубное влияние выльется в 40%, по причине автономной работы на низких оборотах предприятия, что следует из правил расчета критических значений, свойственных организации производства. Максимальная потеря составить 1,4 млрд руб. x 0.4 = 0,56 млрд. руб.

Покажем предложения по улучшению СОИБ и рассчитаем уже выигрыш от применения защитных мер. Первое на что следует обратить внимание – предустановленное программное обеспечение. Как уже было сказано ранее, в СЦ применяются иностранные ПП. Соответственно и изменения должны их касаться. Среди ОС оправдан выбор между UNIX – системами. Хорошим примером можно считать ATSRA LINUX, разработанную НПО «РУСБИТЕХ» [25]. Об оправданности выбора также говорит и распространяемая информация на отмеченном сайте производителя, рис. 8. В поддержку данного ПП выступает и банк угроз ФСТЭК России, который ясно дает понять о практически полном отсутствии угроз от КА, в отличие от всех известных систем компании Microsoft, которая даже на последней версии насчитывает свыше десятка.

Рис. 8 – Оборудование для установки отечественной ОС ASTRA LINUX
Fig. 8 – Equipment for installing the domestic ASTRA LINUX OS

Следующая проблема – необходимость перехода на отечественные аппаратные средства. Как известно, наиболее распространенными элементами информационной системы является межсетевые экраны, коммутаторы и маршрутизаторы. Среди отечественных производителей коммутаторов достаточно активно развивается компания ELTEX, имеющая сертификацию ФСТЭК России на свою продукцию. Соответственно ее и будем предлагать в качестве импортозамещения. Среди маршрутизаторов кроме уже озвученной ELTEX, часто фигурирует компания DIONIS, как, например, вариант [26]. У межсетевых экранов разброс фирм еще больше чем у предыдущих устройств. Как вариант замены рекомендуем присмотреться к фирме ALTELL [27]. В части предустановленных защитных ПП считаем, что проблем не обнаружено (логика обновления их до последней версии само собой актуальна), потому далее дадим комментарии относительно не хватающих элементов физической (пассивной / активной) защиты.

1) Проблема плохо расположенных коммуникаций. С целью достижения максимизации защиты извне рекомендуется убрать весь электромонтаж из стен, прилегающих к оконной зоне (внешней стороны) помещений, установить на стекла системы активных помех, с целью недопущения утечки речевой и технической информации.

2) Установить купольную защиту периметра. В данном случае имеется ввиду средства, которые будут принудительно отключать беспилотные устройства посредством электромагнитных импульсов. Важно отметить, что система должна не только отключать электронику БПЛА, но и также, по возможности вызывать перегрузку устройств, с целью недопущения возобновления передачи информации как КА, так и ретрансляции украденной за пределы периметра предприятия с установленным СЦ. Кроме того, в данной системе должно присутствовать понятие «ведения» устройства, т.е. не просто бессмысленное циклическое распространение электромагнитных волн в пространство над зданиями и сооружениями, но и также анализ в какое место приземлился / упал БПЛА, а также направление его удаления при неэффективности изначальных мер электромагнитной борьбы.

3) Как рациональное предложение следует ввести применение газовых растворов, которые будут выпускаться по всему периметру верхней полусферы. Тем самым кроме блокирования возможности визуального управления малым ЛА, в случае использование механизмов с двигательной установкой не электрического характера, проводить засорение воздушных входов и нарушения законов Карно, действующих для двигателей внутреннего сгорания. Данная мера пусть и в меньшей степени, но все же будет эффективна также при воздействии на винты БПЛА, т.к. будет засорять контакты коннекта движителя с лопастями и по возможности стопорить их.

4) Решение проблемы передачи данных по беспроводным технологиям. С целью недопущения воровства сведений из СЦ по беспроводным каналам, логично по всему периметру установить системы активного глушения, тем самым, не допуская распространения WIFI, Bluetooth или иного сигнала за потребную рабочую зону.

5) Злонамерное падение. О противостоянии данной угроз уже говорилось выше. Единственное замечание, которое следует сделать – это программное недопущение отключения систем активной борьбы с БПЛА. Т.е. минимизация возможности помощи злоумышленникам, управляющим малым ЛА изнутри.

6) Установка пассивных защитных систем от попадания внутрь защищаемого объекта БПЛА. Рекомендуется кроме сеток, применять датчики звукового анализа (оценка нападавшего, чтобы не перепутать с птицей, крысой, белкой и т.п.). Датчики приближения также рационально разместить, хотя, они будут скорее дублирующим контуром.

7) Закрытие всех пустых портов серверной составляющей, а также устройств распространения данных заглушками. В данном случае будет не допущено даже при попадании БПЛА внутрь СЦ его физического подключения. Более того, при наличии специальных замков не будет возможности использовать малый ЛА как транспорт для доставки данных, скопированных на флеш-карту.

Проведем оценку вновь примененных защитных мер.

1) Программное обеспечение. Общие затраты на него составят порядка 1 млн. руб., с учетом установки как на ПО внутри СЦ, так и на связанные элементы.

2) Применение отечественных аппаратных средств. На маршрутизирующее устройства средняя стоимость будет составлять 190000 руб. (Крафтвэй)

На коммутирующее устройство – 520000 руб. (DIONIS)

На межсетевой экран – 3100000 руб. (IDECO)

3) Переоборудование коммуникаций – стоимость: 3500000 руб.

4) Средства принудительной посадки – 12500000 руб.

5) Применение газовый систем – 8000000 руб.

6) Системы активной блокировки – минимум 50 штук, по цене – 110000 руб. / шт.

7) Системы активного зашумления эфира – 4600000 руб.

8) Заглушки – 100000 руб.

Итого, суммарно: 1000000 + 190000 + 5200000 + 3100000 + 3500000 + 12500000 + 8000000 + 5500000 + 4600000 + 10000 = 43600 000 руб.

Как можно заметить, 560000000 руб. >> 43600000 руб.

Таким образом, применение данных рекомендаций позволит добиться большего успеха при защите информации СЦ.

Вывод. Результаты исследования могут быть полезны для специалистов отрасли ИБ, т.к. отражают мало освещённый материал зашиты СЦ; позволяет заострить внимание на необходимости реализации должной системы защиты. Особо следует уделить внимание описанию четырех обобщенных вариантов проведения атак, а также плохой защищенности от БПЛА. Содержащиеся в работе рационализаторские предложения позволят сотрудникам службы ИБ провести их реализацию на конкретном объекте.

Библиографический список:

1. Шулаева Е.А., Маринич А.А. Разработка системы мониторинга безопасности информационной среды предприятия//Электротехнические и информационные комплексы и системы. – 2023. – №1. – С.144-155.
2. Липатов Ю.В. К вопросу об информационных угрозах безопасности в органах государственной власти Российской Федерации // Тенденции развития науки и образования. – 2022. – № 83-2. – С.59-63.
3. Басан Е.С., Басан А.С., Некрасов А.В. [и др.]. База знаний об атаках на беспилотные летательные аппараты//Системный синтез и прикладная синергетика:сборник научных работ X Всероссийской научной конференции, пос. Нижний Архыз, 28 сентября 2021 года. Ростов-на-Дону, Таганрог: Южный федеральный университет, 2021. – С.170-178.
4. Шестаков Н.В. Исследование радиолокационных отражений от беспилотных летательных аппаратов с малой эффективной поверхностью рассеяния//Известия ТулГУ. Технические науки. – 2022. – №2. – С.402-407.
5. В РФ растёт количество атак на информационные системы и физическую инфраструктуру предприятий, согласно данным от «Лаборатории Касперского». https://www.ixbt.com/news/2022/12/12/v-rf-rastjot-kolichestvo-atak-na-informacionnye-sistemy-i-fizicheskuju-infrastrukturu-predprijatij-soglasno-laboratorii.html (дата обращения 24.03.2024).
6. Клебанов Л.Р., Полубинская С.В. Компьютерные технологии в совершении преступлений диверсионной и террористической направленности // Вестник РУДН. Серия: Юридические науки. – 2020. – № 3. – С.717-734.
7. Котенко И.В., Саенко И.Б., Авраменко В.С. Концептуальный подход к обеспечению информационной безопасности системы распределенных ситуационных центров//Информатизация и связь. – 2019. – № 3. – С.37-43.
8. Райков А.Н. Целостный дискурс ситуационного центра // Межотраслевая информационная служба. – 2012. – № 3. – С.47-54.
9. Казаков Е.А. Ситуационный центр как современный инструмент обеспечения непрерывности деятельности на предприятии // Развитие науки и практики в глобально меняющемся мире в условиях рисков:Сб. материалов IV Международной научно-практической конференции, Москва, 10 мая 2021 года. –Махачкала. ООО "Институт развития образования и консалтинга", 2021. – С.195-198.

10. Жаныбек Ж.А., Попова Г.В. Информационная безопасность ситуационного центра//Вестник Восточно-Казахстанского государственного технического университета им. Д. Серикбаева. – 2017. – № 3. – С. 181-186.
11. Цели и задачи информационной безопасности системы распределенных ситуационных центров (СРСЦ) определяются «Концепцией информационной безопасности системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия».
12. Титов К.А., Водяницкая С.И. Концептуальные подходы к сравнению российских операционных систем с открытым кодом // Научные исследования 2023: актуальные теории и концепции: сборник материалов XXIX-ой международной очно-заочной научно-практической конференции, Москва, 24 мая 2023 года. Том 1. – Москва: Научно-издательский центр "Империя", 2023. – С. 39-43.
13. Евдокимова А.А. Рынок информационной безопасности РФ//Актуальные проблемы развития экономики России в условиях новых вызовов:сборник научных трудов по итогам научной конференции, Москва, 08–09 ноября 2022г. Москва:ИТК «Дашков и К», 2022. – С.83-87.
14. ФСТЭК оставит иностранные компании без сертификатов. – URL: https://www.securitylab.ru/news/530814.php?r=1 (дата обращения: 16.10.2024).
15. Юдин А.П. Проблемы обеспечения информационной безопасности телекоммуникационных технологий предприятия // Вестник науки. – 2023. – №5(62). – С.437-443
16. Грехов А.С., Поликанин А.Н., Титов Д.Н. Исследование средств противодействия оптическим каналам утечки информации с использованием беспилотных летательных аппаратов // интерэкспо геосибирь. – 2022. – С.39-46.
17. Финансовая компания обнаружила, что ее пытаются взломать с помощью дрона с WiFi Pineapple на борту. - URL: https://xakep.ru/2022/10/13/drone-hacking/ (дата обращения 20.03.2024)
18. Патент № 2729905 C1 Российская Федерация, МПК G05D 1/10, B64C 39/00. Способ управления беспилотным летательным аппаратом : № 2019126994 : заявл. 26.08.2019 : опубл. 13.08.2020 / С.Ю. Бибиков, А.И. Поляков, М.Л. Тучинский [и др.] ; заявитель Российская Федерация, от имени которой выступает Министерство обороны Российской Федерации.
19. Приказ ФСТЭК России от 11.02.2013г.№ 17«Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
20. Уровни возможностей нарушителя. https/bdu.fstec.ru/threat-ction/potential?ysclid=lpei6ta63f793896869 (дата обращения 05.11.2024)
21. Шондиров Р.Х. Киберпространство: новая платформа для терроризма // Право и управление. – 2023. – № 2. – С.141-145.
22. БДУ ФСТЭК - Реестр. https://service.securitm.ru/bduthreats? ysclid=lpfulb2kh2553360154 (дата обращения: 12.11.2024).
23. 54 вида кибератак, о которых следует знать в 2024 году. https://dzen.ru/a/ZUYNJUusBWYBYvzz (дата обращения: 20.11.2024).
24. Среднее предприятие:критерии отнесения в 2024 году. https://www.rnk.ru/article/217538-srednee-predpriyatie-kriterii-otneseniya-v-2024-godu?ysclid=lry2qded9s484735943(дата обращения: 25.01.2024).
25. Операционные системы. https://rusbitech.ru/products/os/?ysclid= lqihyyvmd7425699666 (дата обращения: 10.12.2024).
26. Маршрутизатор Dionis DPS-3006. https://dzen.ru/a/XvTr27cM-1f_ZXSb (дата обращения: 10.12.2024).
27. Аппаратный межсетевой экран ALTELL NEO — защита корпоративной, локальной сети. - URL: https://altell.ru/products/neo/?ysclid= lqijluoqi1592987623 (дата обращения: 10.12.2024).

References:

1. Shulaeva E.A., Marinich A.A. Development of an enterprise information environment security monitoring system. *Electrotechnical and information complexes and systems.* 2023;1:144-155.
2. Lipatov Yu.V. On the issue of information security threats in public authorities of the Russian Federation. *Trends in the development of science and education*. 2022;83-2:59-63.
3. Basan E.S., Basan A.S., Nekrasov A.V. [and]. Knowledge base on attacks on unmanned aerial vehicles. System synthesis and applied synergetics :coll. of Scientific papers of the X All-Russian Scientific Conference, Nizhny Arkhyz, 28 09 2021. Rostov-on-Don, Taganrog: Southern Federal University, 2021;70-178.
4. Shestakov N.V. Investigation of radar reflections from unmanned aerial vehicles with a small effective scattering surface. *News of TulSU. Technical sciences*. 2022; 2:402-407.
5. The number of attacks on information systems and physical infrastructure of enterprises is growing in the Russian Federation, according to data from Kaspersky Lab. https://www.ixbt.com/news/2022/12/12/v-rf-rastjot-kolichestvo-atak-na-informacionnye-sistemy-i-fizicheskuju-infrastrukturu-predprijatij-soglasno-laboratorii.html (accessed 03/24/2024).
6. Klebanov L.R., Polubinskaya S.V. Computer technologies in the commission of subversive and terrorist crimes. *Bulletin of the RUDN University. Series: Legal Sciences*. 2020;3:717-734.
7. Kotenko I.V., Saenko I.B., Avramenko V.S. A conceptual approach to ensuring information security of a system of distributed situational centers. Informatization and communication, 2019;3:37-43.

8. Raikov A.N. Holistic discourse of a situational center. *An intersectoral information service*. 2012;3:47-54.
9. Kazakov E.A. Situational center as a modern tool for ensuring business continuity at an enterprise. Development of science and practice in a globally changing world under conditions of risks : Proceedings of the IV International Scientific and Practical Conference, Moscow, May 10, 2021. – Makhachkala: Limited Liability Company "Institute for the Development of Education and Consulting", 2021, pp.195-198.
10. Zhanybek Zh.A., Popova G.V. Information security of the situational center. *Bulletin of the D. Serikbayev East Kazakhstan State Technical University*. 2017; 3:181-186.
11. The goals and objectives of information security of the system of distributed situational centers (SRSC) are defined by the "Concept of information security of the system of distributed situational centers operating according to a single regulation of interaction."
12. Titov K.A., Vodianitskaya S.I. Conceptual approaches to comparing Russian open source operating systems. Scientific Research 2023:current theories and concepts:proceedings of the XXIX TH International Correspondence Scientific and Practical Conference, Moscow, May 24, 2023;1:39-43. Moscow: Empire Scientific Publishing Center.
13. Evdokimova A.A. The information security market of the Russian Federation. Actual problems of the development of the Russian economy in the context of new challenges :a collection of scientific papers based on the results of a scientific conference, Moscow, November 08-09, 2022:83-87. Moscow, November 08-09, 2022. Moscow: Dashkov & Co. 2022:83-87 (In Russ)
14. The FSTEC will leave foreign companies without certificates. – URL: https://www.securitylab.ru/news/530814.php?r=1 (date of reference: 16.10.2024).
15. Yudin A.P. Problems of ensuring information security of telecommunication technologies of the enterprise *Bulletin of Science*. 2023;5(62):437-443.
16. Grekhov A.S., Polikanin A.N., Titov D.N. Investigation of means of countering optical channels of information leakage using unmanned aerial vehicles. *Interexpo geo-siberia*. 2022;39-46.
17. A financial company discovered that they were trying to hack it using a drone with a WiFi Pineapple on board. - URL: https://xakep.ru/2022/10/13/drone-hacking / (accessed 20.03.2024).
18. Patent No. 2729905 C1 Russian Federation, IPC G05D 1/10, B64C 39/00. Method of controlling an unmanned aerial vehicle : No. 2019126994 : application. 26.08.2019 : published 13.08.2020 / S.Y. Bibikov, A.I. Polyakov, M.L. Tuchinsky [et al.] ; applicant is the Russian Federation, on behalf of which the Ministry of Defense of the Russian Federation acts.
19. FSTEC of Russia Order No. 17 February 11, 2013 "On Approval of Requirements for the Protection of Information Not Constituting a State Secret Contained in State Information Systems.
20. Levels of intruder's capabilities. - URL: https://bdu.fstec.ru/threat-section/potential?ysclid=lpei6ta63f793896869 (accessed 05.11.2024).
21. Shondirov R.H. Cyberspace: a new platform for terrorism. *Law and Governance*. 2023; 2:C.141-145.
22. FSTEC Database Registry. - URL: https://service.securitm.ru/bduthreats?ysclid= lpfulb2kh2553360154 (date of request: 12.11.2024).
23. 54 types of cyber attacks that you should be aware of in 2024. https://dzen.ru/a/ZUYNJUusBWYBYvzz (date of request: 11/20/2023).
24. Medium-sized enterprises: criteria for assignment in 2024 https://www.rnk.ru/ article/217538-srednee-predpriyatie-kriterii-otneseniya-v-2024-godu?ysclid=lry2qded9s484735943 (accessed: 25.01.2024).
25. Operating systems. https://rusbitech.ru/products/os/?ysclid=lqihyyvmd7425699666 (date of request: 10.12.2024).
26. Dionis DPS-3006 router. - URL: https://dzen.ru/a/XvTr27cM-1f_ZXSb (date of request: 10.12.2024).
27. ALTELL NEO hardware Firewall - corporate, local network protection. https://altell.ru/products/neo/?ysclid= lqijluoqi1592987623 (date of request: 10.12.2024). (In Russ)

Сведения об авторах:

Лоскутов Иван Андреевич, инженер – конструктор, отдел 55; преподаватель; доцент кафедры индустриального программирования Института перспективных технологий и индустриального программирования; faxvex@ya.ru

Репенко Виктор Андреевич, магистрант; ekspert6@ya.ru

Information about the authors:

Ivan A. Loskutov, Engineer-constructor, Department 55, Teacher; Assoc.Prof., Department of Industrial Programming at the Institute of Advanced Technologies and Industrial Programming; faxvex@ya.ru

Viktor A. Repenko, Master's student; ekspert6@ya.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 20.10.2025.

Одобрена после рецензирования/Reviced 28.11.2025.

Принята в печать/Accepted for publication 20.01.2026.